

**IN THE MATTER OF THE ROYAL COMMISSION  
INTO FAMILY VIOLENCE**

**ATTACHMENT DW-2 TO STATEMENT OF DAVID WATTS**

Date of document: 31 July 2015  
Filed on behalf of: the Applicant  
Prepared by:  
Victorian Government Solicitor's Office  
Level 33  
80 Collins Street  
Melbourne VIC 3000



This is the attachment marked '**DW-2**' produced and shown to **DAVID WATTS** at the time of signing his Statement on 31 July 2015.

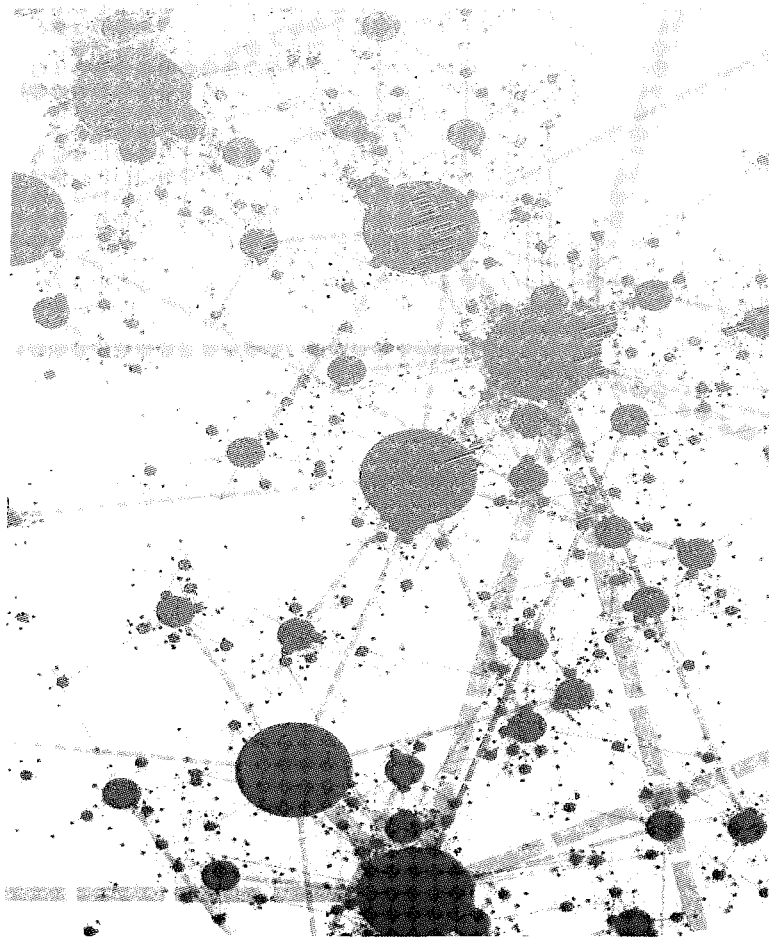
Before me: ..... ..



An Australian legal practitioner  
within the meaning of the  
Legal Profession Uniform Law (Victoria)

Attachment DW-2

# THE OECD PRIVACY FRAMEWORK



2013

## ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

© OECD 2013

Cover image: © kentoh - Fotolia.com

---

No reproduction, copy, transmission or translation of this document may be made without written permission. Applications should be sent to OECD Publishing:

[rights@oecd.org](mailto:rights@oecd.org)

---

## Foreword

Over many decades the OECD has played an important role in promoting respect for privacy as a fundamental value and a condition for the free flow of personal data across borders.

On 11 July 2013 the OECD Council adopted a revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (“Privacy Guidelines”). This revision is the first since the original 1980 release of the Guidelines and arises out of a call by Ministers in the 2008 *Seoul Declaration for the Future of the Internet Economy* to assess the Guidelines in light of “changing technologies, markets and user behaviour, and the growing importance of digital identities”.

The OECD Working Party on Information Security and Privacy (WPISP) agreed on Terms of Reference for the review in 2011. The Terms of Reference highlighted that, as compared with the situation 30 years ago, there has been a profound change of scale in terms of the role of personal data in our economies, societies, and daily lives. The environment in which the traditional privacy principles are now implemented has undergone significant changes, for example, in:

- The **volume** of personal data being collected, used and stored;
- The **range of analytics** involving personal data, providing insights into individual and group trends, movements, interests, and activities;
- The **value** of the societal and economic benefits enabled by new technologies and responsible uses of personal data;
- The extent of **threats** to privacy;
- The **number and variety of actors** capable of either putting privacy at risk or protecting privacy;
- The **frequency and complexity of interactions** involving personal data that individuals are expected to understand and negotiate;

- The *global availability* of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.

In accordance with the Terms of Reference, the WPISP convened a multi-stakeholder group of experts from governments, privacy enforcement authorities, academia, business, civil society and the Internet technical community (“Expert Group”). This Expert Group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada. Omer Tene, consultant to the OECD, served as rapporteur. On the basis of the work by the Expert Group, proposed revisions were developed by the WPISP, approved by the Committee for Information, Computer and Communications Policy (ICCP), before final adoption by the OECD Council.

Two themes run through the updated Guidelines. First is a focus on the practical implementation of privacy protection through an approach grounded in risk management. Second is the need for greater efforts to address the global dimension of privacy through improved interoperability. A number of new concepts are introduced, including:

- *National privacy strategies* – While effective laws are essential, the strategic importance of privacy today also requires a multifaceted national strategy co-ordinated at the highest levels of government.
- *Privacy management programmes* – These serve as the core operational mechanism through which organisations implement privacy protection.
- *Data security breach notification* – This provision covers both notice to an authority and notice to an individual affected by a security breach affecting personal data.

Other revisions modernise the OECD approach to transborder data flows, detail the key elements of what it means to be an accountable organisation, and strengthen privacy enforcement. As a step in a continuing process, this revision leaves intact the original “Basic Principles” in Part Two of the Guidelines. On-going work by the OECD on privacy protection in a data-driven economy will provide further opportunities to ensure that its privacy framework is well adapted to current challenges.

This booklet brings together the key components of the OECD privacy framework, along with the supplementary documentation to provide context and explanation. The cornerstone of that framework is the revised Privacy Guidelines, which form Chapter 1.

Chapter 2 contains a new supplementary explanatory memorandum that was prepared to provide context and rationale for the revisions to the Guidelines. It was approved for public release by the OECD Council when it adopted the revised Guidelines. It is intended to supplement – not replace – the original explanatory memorandum, which remains relevant to interpreting the aspects of the Guidelines that remain unchanged from 1980 and is reproduced as Chapter 3.

Preparations for the review were conducted during 2010-11 in the context of the 30<sup>th</sup> anniversary of the Privacy Guidelines, during which the OECD organised a series of events and produced a report on “The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines.” That report documents the tremendous changes evident in privacy landscape which motivated many of the revisions to the Guidelines and is reproduced as Chapter 4.

The second part of this booklet focuses on a key dimension of effective privacy protection in a global context: cross-border enforcement co-operation. In 2007 the OECD Council adopted a Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, reproduced as Chapter 5. Chapter 6 is the 2011 OECD report on the implementation of this Recommendation, three years after its adoption. The revised Privacy Guidelines integrate and build on a number of elements from the 2007 Recommendation, and the two instruments are mutually reinforcing in helping improve the cross-border dimensions of what is fundamentally a global issue.

## *Table of contents*

<b>PART I. THE OECD PRIVACY GUIDELINES.....</b>	<b>9</b>
<b>Chapter 1. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).....</b>	<b>11</b>
Part One. General.....	13
Part Two. Basic principles of national application .....	14
Part Three. Implementing accountability.....	16
Part Four. Basic principles of international application: Free flow and legitimate restrictions.....	16
Part Five. National implementation .....	17
Part Six. International co-operation and interoperability.....	17
<b>Chapter 2. Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013) .....</b>	<b>19</b>
<b>Introduction.....</b>	<b>19</b>
Context of the review.....	19
Process of the review .....	21
<b>Revisions to the Guidelines .....</b>	<b>23</b>
Privacy management programmes.....	23
Data security breach notification .....	26
Privacy enforcement authorities .....	28
Transborder flows of personal data.....	29
National implementation.....	31
International co-operation and interoperability.....	33
Improving the evidence base for policy making.....	34
Other updates.....	34
Notes .....	36
References.....	37

<b>Chapter 3. Original Explanatory Memorandum to the OECD Privacy Guidelines (1980)</b> .....	<b>39</b>
Introduction.....	39
I. General background.....	40
II. The guidelines.....	47
<b>Chapter 4. The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011)</b> .....	<b>65</b>
Main points.....	66
The development and influence of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.....	69
Current trends in the processing of personal data.....	81
Privacy risks in the evolving environment.....	90
Considerations and challenges to existing privacy approaches.....	96
Evolution and innovation in privacy governance.....	102
Conclusion.....	114
<b>PART II. CROSS-BORDER PRIVACY LAW ENFORCEMENT CO-OPERATION</b> .....	<b>127</b>
<b>Chapter 5. Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007)</b> .....	<b>129</b>
I. Definitions.....	131
II. Objectives and scope.....	131
III. Domestic measures to enable co-operation.....	132
IV. International co-operation.....	133
<b>Chapter 6. Report on the Implementation of the 2007 OECD Recommendation on Privacy Law Enforcement Co-operation (2011)</b> ..	<b>137</b>
Main points.....	137
Background.....	139
Implementation activities supported by OECD.....	140
Improving domestic measures to enable co-operation.....	144
Examples of cross-border co-operation.....	147
Other international initiatives.....	149
Conclusion.....	151



*PART I.*  
*THE OECD PRIVACY GUIDELINES*

## Chapter 1.

### Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)

[C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79]

#### 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 *Ministerial Declaration on the Protection of Privacy on Global Networks* [Annex 1 to C(98)177]; the *Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks* [C(2002)131/FINAL], the *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* [C(2007)67], the *Declaration for the Future of the Internet Economy (The Seoul Declaration)* [C(2008)99], the *Recommendation of the Council on Principles for Internet Policy Making* [C(2011)154], the *Recommendation of the Council on the Protection of Children Online* [C(2011)155] and the *Recommendation of the Council on Regulatory Policy and Governance* [C(2012)37];

**RECOGNISING** that Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information;

**RECOGNISING** that more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks;

**RECOGNISING** that the continuous flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border co-operation among privacy enforcement authorities;

**12** – I. OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

**RECOGNISING** the importance of risk assessment in the development of policies and safeguards to protect privacy;

**RECOGNISING** the challenges to the security of personal data in an open, interconnected environment in which personal data is increasingly a valuable asset;

**DETERMINED** to further 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 them;

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

- I. **RECOMMENDS** that Member countries:
  - Demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest levels of government;
  - Implement the Guidelines contained in the Annex to this Recommendation, and of which they form an integral part, through processes that include all relevant stakeholders;
  - Disseminate this Recommendation throughout the public and private sectors;
- II. **INVITES** non-Members to adhere to this Recommendation and to collaborate with Member countries in its implementation across borders.
- III. **INSTRUCTS** the Committee for Information, Computer and Communication Policy to monitor the implementation of this Recommendation, review that information, and report to the Council within five years of its adoption and thereafter as appropriate.

This Recommendation revises 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].

## 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 national 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) “Laws protecting privacy” means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines.
  - d) “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.
  - e) “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 risk to privacy and individual liberties.
3. The principles in these Guidelines are complementary and should be read as a whole. They should not be interpreted:
  - a) as preventing the application of different protective measures to different categories of personal data, depending upon their nature and the context in which they are collected, stored, processed or disseminated; or

**14**– 1. OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

- b) in a manner which unduly limits the freedom of expression.
- 4. Exceptions to 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 can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data.

**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. Individuals 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 them;
  - b) to have communicated to them, data relating to them
    - 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 them;
  - 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 them 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. IMPLEMENTING ACCOUNTABILITY**

15. A data controller should:
- a) Have in place a privacy management programme that:
    - i. gives effect to these Guidelines for all personal data under its control;
    - ii. is tailored to the structure, scale, volume and sensitivity of its operations;
    - iii. provides for appropriate safeguards based on privacy risk assessment;
    - iv. is integrated into its governance structure and establishes internal oversight mechanisms;
    - v. includes plans for responding to inquiries and incidents;
    - vi. is updated in light of ongoing monitoring and periodic assessment;
  - b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and
  - c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

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

16. A data controller remains accountable for personal data under its control without regard to the location of the data.
17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.
18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

**PART FIVE. NATIONAL IMPLEMENTATION**

19. In implementing these Guidelines, Member countries should:
- a) develop national privacy strategies that reflect a co-ordinated approach across governmental bodies;
  - b) adopt laws protecting privacy;
  - c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;
  - d) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
  - e) provide for reasonable means for individuals to exercise their rights;
  - f) provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;
  - g) consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy;
  - h) consider the role of actors other than data controllers, in a manner appropriate to their individual role; and
  - i) ensure that there is no unfair discrimination against data subjects.

**PART SIX. INTERNATIONAL CO-OPERATION AND INTEROPERABILITY**

20. Member countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.
21. Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.
22. Member countries should encourage the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.
23. Member countries should make public the details of their observance of these Guidelines.



## *Chapter 2.*

### **Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)**

#### **Introduction**

In 1980, the OECD adopted the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (“1980 Guidelines”) to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. The 1980 Guidelines, which contained the first internationally agreed-upon set of privacy principles, have influenced legislation and policy in OECD Member countries and beyond. Framed in concise, technology-neutral language, they have proven remarkably adaptable to technological and societal changes. Nevertheless, changes in personal data usage, as well as new approaches to privacy protection, have left the 1980 Guidelines in need of updating in a number of important respects. The Honourable Michael Kirby chaired the original OECD expert group that drafted the Guidelines. In reflecting on that achievement on the occasion of the Guideline’s 30th anniversary Justice Kirby observed: “In the field of information policy, the technology is such that no international expression of principles can be immune from the forces of change.”<sup>1</sup>

#### **Context of the review**

Over the last three decades, personal data have come to play an increasingly important role in our economies, societies and everyday lives. Innovations, particularly in information and communication technologies, have impacted business operation, government administration, and the personal activities of individuals. New technologies and responsible data uses are yielding great societal and economic benefits. The volume of

personal data being collected, used and stored is vast and continues to grow. Modern communications networks support global accessibility and continuous, multipoint data flows. The potential uses of personal data have increased tremendously as a result of the wide range of analytics that can provide comprehensive insights into individuals' movements, interests, and activities.

At the same time, the abundance and persistence of personal data have elevated the risks to individuals' privacy. Personal data is increasingly used in ways not anticipated at the time of collection. Almost every human activity leaves behind some form of digital data trail, rendering it increasingly easy to monitor individuals' behaviour. Personal data security breaches are common. These increased risks signal the need for more effective safeguards in order to protect privacy.

In recent years, several initiatives have been undertaken to address new and elevated privacy risks, particularly in the context of transborder data flows. The work is ongoing and examples include the European Union's system of Binding Corporate Rules (BCRs)<sup>2</sup>; the global discussion on the commonly accepted elements of privacy accountability<sup>3</sup>; and the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules System (APEC CBPR).<sup>4</sup> At the OECD, cross-border co-operation among privacy enforcement authorities has been a priority, resulting in the adoption of the 2007 Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (the "2007 Recommendation", [OECD, 2007]).

The *Seoul Declaration for the Future of the Internet Economy* (2008) recommended that the OECD assess the application of certain OECD instruments, including the 1980 Guidelines, in light of "changing technologies, markets and user behaviour and the growing importance of digital identities." This Declaration triggered the launch of a formal review of the 1980 Guidelines.

The OECD Recommendation on Principles for Internet Policy Making (OECD, 2011a) called for a strengthening of consistency and effectiveness in privacy protection at a global level. While the OECD Privacy Guidelines have a broader scope than Internet policies, the 2011 Recommendation is nevertheless instructive. The Communiqué attached to the 2011 Recommendation for information purposes explains that current privacy challenges are likely to become more acute "as the economy and society depends more heavily on broadened and innovative uses of personal information that can be more easily gathered, stored, and analysed" (OECD, 2011b).

Privacy frameworks around the world are being examined and refined. Three of the primary frameworks with an international dimension (OECD, European Union, and Council of Europe) have been under review simultaneously, and a fourth (APEC) is implementing new cross-border arrangements. Work on domestic privacy frameworks is likewise underway across the globe, from Australia to Brazil to China to the United States. In light of all of these developments, the OECD concluded that it was an appropriate time to engage in a substantive review of the 1980 Guidelines.

### **Process of the review**

Preparations for the review began in 2010, in the context of the 30<sup>th</sup> anniversary of the 1980 Guidelines. As part of the process, the OECD organised three thematic events. These events addressed (1) the impact of the 1980 Guidelines; (2) the evolving role of the individual; and (3) the economic dimensions of personal data and privacy. It also produced two reports, “The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines” (OECD, 2011c), and “Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation” (OECD, 2011d).

Building on this preparatory work, the Working Party for Information Security and Privacy (WPISP) developed Terms of Reference (OECD, 2011e) to serve as a roadmap for the review. The Terms of Reference articulated a shared view of current issues and approaches, and provided the rationale for further work. In addition to highlighting the changes in the environment, the Terms of Reference identified those elements which Member countries considered essential to improving the effectiveness of privacy protections.

A Volunteer Group of Privacy Experts (“Expert Group”) was formed to assist the WPISP in the review process. This group included experts from governments, privacy enforcement authorities, academics, business, civil society, and the Internet technical community. Participants also included representatives of the Council of Europe and the European Union, as well as experts active in APEC. This multi-stakeholder group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada. Omer Tene served as the Rapporteur to the group. The Expert Group collaborated through a series of meetings and a virtual workspace during 2011 and 2012. During these meetings, the Expert Group focused on three main themes identified by the Terms of Reference, namely: (1) the roles and responsibilities of key actors; (2) geographic restrictions on transborder data flows; and (3) proactive implementation and enforcement.

The approach that emerged from the work of the Expert Group suggested that, although the environment for privacy and transborder data flows has changed significantly, an update to the 1980 Guidelines was preferred rather than a fundamental rethinking of its core principles. The Expert Group took the view that the balance reflected in the eight basic principles of Part Two of the 1980 Guidelines remains generally sound and should be maintained. The Expert Group introduced a number of new concepts to the OECD privacy framework, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other aspects of the 1980 Guidelines were expanded or updated, such as accountability, transborder data flows and privacy enforcement.

The 1980 Guidelines were accompanied by an Explanatory Memorandum, which described the environment that led to their development, as well as their underlying rationale. The Explanatory Memorandum provides insight into the competing priorities of the time, as well as a detailed interpretation of various provisions in the 1980 Guidelines, some of which have not been modified (in particular those of Part Two). These insights remain relevant today. This Supplementary Explanatory Memorandum has been prepared as part of the review process to complement the revised Guidelines. It is intended to supplement – not replace – the original Explanatory Memorandum. Where there have been changes to the 1980 Guidelines, this Supplementary Explanatory Memorandum sheds light on the rationale and context of these changes to help understand and interpret them.

## Revisions to the Guidelines

### Privacy management programmes

Part Two of the 1980 Guidelines sets forth the principle of accountability, which places the onus on the data controller to comply “with measures that give effect to the rest of the principles”. Recognition of the importance of the accountability principle has increased over time. Domestic privacy laws have come to introduce a variety of mechanisms designed to promote the accountability of both public and private data controllers. Obligations of transparency towards individuals and privacy enforcement authorities are clear examples of such mechanisms.

In recent years, the principle of accountability received renewed attention as a means to promote and define organisational responsibility for privacy protection. Building on this experience, the new Part Three of the Guidelines (“Implementing Accountability”) introduces the concept of a privacy management programme and articulates its essential elements.

Paragraph 15(a)(i) specifies that a data controller’s privacy management programme should give effect to the Guidelines “for all personal data under its control”. The term “control” refers back to the definition of a “data controller”, as defined in paragraph 1(a). This formulation emphasises that a privacy management programme should not only address the data controller’s own operations, but all operations for which it may be accountable - regardless of to whom data is transferred. For example, a privacy management programme should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf. Safeguards may also be necessary in relationships with other data controllers, particularly where the responsibility for giving effect to the Guidelines is shared. Appropriate safeguards may include: provisions in contracts that address compliance with the data controller’s privacy policies and practices; protocols for notifying the data controller in the event of a security breach; employee training and education; provisions for sub-contracting; and a process for conducting audits.

Paragraph 15(a)(i) refers only to the Guidelines as a source of rules or principles to be implemented through a privacy management programme. In practice, privacy management programmes may need to reflect other sources as well; including domestic law, international obligations, self-regulatory programmes, or contractual provisions.

Paragraph 15(a)(ii) underlines the need for flexibility when putting in place a privacy management programme. For example, large data controllers with locations in multiple jurisdictions may need to consider different internal oversight mechanisms than small or medium sized data controllers with a single establishment. At the same time, paragraph 15(a)(ii) also provides that privacy management programmes should be adapted to the volume and sensitivity of the controller's operations. Programmes for data controllers that deal with large volumes of personal data will need to be more comprehensive than those of data controllers who handle only limited amounts of personal data. The sensitivity of the data controller's operations may also impact the nature of a privacy management programme, as even a very small data controller may handle extremely sensitive personal data.

A recurring element in the discussions about privacy management programmes was the need for such programmes to develop appropriate safeguards based on privacy risk assessment. Paragraph 15(a)(iii) contemplates that the determination of the necessary safeguards should be made through a process of identifying, analysing and evaluating the risks to individuals' privacy. This process is sometimes accomplished by conducting a "privacy impact assessment" before a new programme or service is introduced or where the context of the data use changes significantly. "Risk" is intended to be a broad concept, taking into account a wide range of possible harms to individuals. A privacy management programme can also assist in the practical implementation of concepts such as "privacy by design", whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an afterthought.

Paragraph 15(a)(iv) indicates that privacy management programmes should be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms. Obtaining support and commitment from senior management is a key factor in ensuring the successful implementation of a privacy management programme. Ensuring the availability of sufficient resources and staff, as well as training programmes, may also improve the effectiveness of the programme. Privacy officers may play an important role in designing and implementing a privacy management programme.

Paragraph 15(a)(v) provides that a privacy management programme should also include plans for responding to incidents and inquiries. The increasing frequency of security breaches affecting personal data demonstrates the importance of developing an incident response plan, which includes breach notification (see below). To support the “Individual Participation Principle” in Part Two, data controllers should also be able to provide timely response to inquiries (either in the form of complaints or requests for information) by data subjects. Finally, paragraph 15(a)(vi) stipulates that privacy management programmes should be routinely reviewed and updated to ensure that they remain appropriate to the current risk environment.

Paragraph 15(b) provides that a data controller should be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines. Establishing the capacity and effectiveness of a privacy management programme, even in the absence of a personal data security breach or allegation of non-compliance, enhances the accountability of data controllers. The assessment of the programme may be carried out directly by the privacy enforcement authority or by an agent on its behalf.

Paragraph 15(b) includes the terms “appropriate” and “competent” to highlight that data controllers should be prepared to demonstrate their privacy management programmes at the request of a privacy enforcement authority provided that this authority has jurisdiction over the data controller. The Guidelines do not address legal issues related to jurisdiction, competence and conflicts of law.

A privacy management programme may also be demonstrated to an entity which is responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to Guidelines. Such arrangements may involve seal programmes or certification schemes, and may also concern transborder flows of personal data. In this regard it can be noted that paragraph 21 encourages the development of international arrangements that give practical effect to the Guidelines. The European Union’s Binding Corporate Rules (BCRs) and the APEC Cross-border Privacy Rules System provide two models for developing such an arrangement.

### **Data security breach notification**

The “Security Safeguards Principle” of Part Two states that “Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.” Numerous high-profile data breaches have demonstrated that personal data security continues to be a challenge.

Data breaches can result, for example, from actions by careless employees who fail to follow proper procedures; hackers who gain access to inadequately protected databases; or opportunistic thieves who steal unsecured portable devices. However, the underlying causes – lack of employee training and awareness, out-of-date security safeguards, inadequate rules governing access to personal data, over-collection of data and undefined retention periods, or a lack of adequate oversight – can often be attributed to the data controller.

The potential harm to individuals from the misuse of their personal data, whether accidentally lost or purposefully stolen, may be significant. Organisations experiencing a breach often incur significant costs responding to it, determining its cause, and implementing measures to prevent recurrence. The reputational impact can also be significant. A loss of trust or confidence can have serious consequences for organisations. As a result, the security of personal data has become an issue of great concern to governments, businesses and individuals.

Breach notification laws requiring data controllers to inform individuals and/or authorities when a security breach has occurred have been passed or proposed in many countries. These laws are usually justified on the grounds that data controllers have little incentive to disclose breaches voluntarily, given the possible harm this can cause to their reputation. Requiring notification may enable individuals to take measures to protect themselves against the consequences of identity theft or other harms. Notification requirements may also provide privacy enforcement authorities or other authorities with information to determine whether to investigate the incident or take other action. Ideally, breach notification laws also help to create an incentive for data controllers to adopt appropriate security safeguards for the personal data they hold.

In addition to contributing to data security, data breach notification enhances other basic principles set forth in Part Two of the Guidelines, including accountability, individual participation and openness. Furthermore, mandatory security breach notification may improve the evidence base for privacy and information security policies by generating information about the number, severity and causes of security breaches.



Security breaches not only raise privacy concerns, but also intersect with other issues, including criminal law enforcement and cybersecurity. When an organisation suffers a security breach, particularly one resulting from an external attack, notification of the breach to authorities other than privacy enforcement authorities (e.g. computer incident response teams, criminal law enforcement entities, other entities responsible for cybersecurity oversight) may be appropriate or required.

Requiring notification for every data security breach, no matter how minor, may impose an undue burden on data controllers and enforcement authorities, for limited corresponding benefit. Additionally, excessive notification to data subjects may cause them to disregard notices. Accordingly, the new provision that has been added to the Guidelines [paragraph 15(c)] reflects a risk-based approach to notification. Notice to an authority is called for where there is a “significant security breach affecting personal data”, a concept intended to capture a breach that puts privacy and individual liberties at risk. Where such a breach is also likely to adversely affect individuals, notification to individuals would be appropriate as well. To determine whether individuals are likely to be “adversely affected” by a breach, the term “adverse effect” should be interpreted broadly to include factors other than just financial loss. Notification requirements should be flexible to allow for prevention and mitigation of further damage. There may be circumstances where notification to data subjects would be inappropriate, for example when it would increase the risk to data subjects or impede a law enforcement investigation.

Existing breach notification laws differ in terms of the thresholds for notification, the parties to be notified, the timing of the notification, as well as the role of privacy enforcement and other authorities. Further experience may be needed to determine which modalities of breach notification are most effective in practice.

Security breaches may affect the personal data of individuals residing in different jurisdictions. When designing, implementing or revising breach notification requirements, special consideration may be given to the interests of affected individuals who may live outside their jurisdiction. In particular, the notification of privacy enforcement authorities in other jurisdictions where a significant number of individuals are known or likely to have been affected, can be beneficial. Cross-border enforcement cooperation mechanisms are one way to foster arrangements that might support or disseminate breach notifications of importance to multiple jurisdictions. Such arrangements may also help to address issues arising from conflicting legal requirements.

### **Privacy enforcement authorities**

Neither the 1980 Guidelines nor the 2007 Recommendation explicitly call for the establishment of privacy enforcement authorities, although the latter instrument assumes their existence and recommends their endowment with effective powers and authority. The revised Guidelines define and make explicit the need to establish and maintain “privacy enforcement authorities”. They also incorporate a definition of “laws protecting privacy”, to refer to “national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines”. Both definitions mirror those agreed in the 2007 Recommendation.

The definitions of “laws protecting privacy” and “privacy enforcement authorities” allow for flexibility in application. “Laws protecting privacy” can refer not only to horizontal privacy laws that are common in Member countries, but also to sectoral privacy legislation (e.g. credit reporting or telecommunications laws) or other types of legislation that contain provisions which protect personal data so as to give effect to the Guidelines in practice (e.g. consumer protection laws). Likewise, a “privacy enforcement authority” refers not only to those public sector entities whose primary mission is the enforcement of national privacy laws, but may for example also extend to regulators with a consumer protection mission, provided they have the powers to conduct investigations or bring proceedings in the context of enforcing “laws protecting privacy”.

A new provision in Part Five (“National Implementation”) calls on Member countries to establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an “objective, impartial and consistent basis” [paragraph 19(c)]. This formulation has been adapted from the 2012 OECD Recommendation on Regulatory Policy and Governance (OECD, 2012a). In the context of the Guidelines, it refers to the need for privacy enforcement authorities to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy. There exist a variety of mechanisms across Member countries for ensuring the necessary impartiality of privacy enforcement authorities in the exercise of their privacy protection functions. Paragraph 19(c) focuses on the practical impact of such mechanisms, which should ensure that these authorities can take decisions free from influences that could compromise their professional judgment, objectivity or integrity.

In some countries, the term “privacy enforcement authority” can also refer to a group of bodies that collectively enforce laws protecting privacy. For example, oversight of public sector data controllers may involve multiple bodies from different branches of government, who may also have the authority to issue guidelines or other data usage requirements. The “governance, resources, and technical expertise” called for in paragraph 19(c) may not, in such a case, be embodied in a single entity, but rather be found in the enforcement system as a whole.

The 2007 Recommendation underlined the need for privacy enforcement authorities to be endowed with the resources and authority necessary 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; and (c) permit corrective action to be taken against data controllers engaged in violations of laws protecting privacy. The resources of privacy enforcement authorities should be commensurate with the scale and complexity of data processing operations subject to their oversight. The new provision also calls for empowering privacy enforcement authorities with sufficient technical expertise, which has become crucial in light of the increasing complexity of data uses. This reinforces the emerging trend within privacy enforcement authorities to retain staff with a technical background.

### **Transborder flows of personal data**

When the 1980 Guidelines were drafted, data flows largely constituted discrete point-to-point transmissions between businesses or governments. Today, data can be processed simultaneously in multiple locations; dispersed for storage around the globe; re-combined instantaneously; and moved across borders by individuals carrying mobile devices. Services, such as “cloud computing”, allow organisations and individuals to access data that may be stored anywhere in the world.

The 1980 Guidelines presumed that data flows should generally be allowed, but recognised the ability of governments to restrict them in certain circumstances, namely where the receiving country “does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation.” Since then, Member countries have instituted a range of mechanisms to ensure the protection of individuals in the context of transborder data flows. Some of these mechanisms include a country-specific assessment, such as the “adequacy model” adopted within the European Union. Other mechanisms are not based on a country-specific assessment, but are instead based on the safeguards put in place by data controllers. Such mechanisms include, for example, Binding Corporate Rules, model contracts, and Cross-Border Privacy Rules.

The revisions reflected in Part Four attempt to simplify and consolidate the OECD approach to transborder flows of personal data. It begins by recalling that a data controller remains accountable for personal data under its control without regard to the location of the data [paragraph 16]. This paragraph restates the basic principle of accountability contained in Part Two in the context of transborder data flows. Transborder flows of personal data, to Member countries or non-Member countries, present risks, which data controllers must address. Some data flows may require close attention because of the sensitivity of the data or because the receiving jurisdiction may lack either the willingness or capacity to enforce privacy safeguards.

Without precluding the application of paragraph 6, paragraph 17 specifies two circumstances in which a Member country should refrain from imposing restrictions on transborder flows of personal data. Paragraph 17(a) retains the general approach from the 1980 Guidelines, by providing that Member countries should refrain from restricting transborder data flows between itself and another country where the other country substantially observes these Guidelines. Paragraph 17(b) discourages restrictions where sufficient safeguards exist to ensure a continuing level of protection consistent with these Guidelines. It gives recognition to the measures which a data controller can put in place to ensure a continuing level of protection, which may result from a combination of measures, such as technical and organisational security safeguards, contracts, complaint handling processes, audits, etc. However, the measures provided by the data controller need to be sufficient and supplemented by mechanisms that can ensure effective enforcement in the event these measures prove ineffective. Paragraph 17(b) therefore includes as a consideration the availability of effective enforcement mechanisms which support measures adopted by the data controller. Such enforcement mechanisms may take a variety of forms, including for example, administrative and judicial oversight, as well as cross-border co-operation among privacy enforcement authorities.

Paragraphs 16 and 17 operate independently. The existence or absence of country restrictions on data flows adopted pursuant to paragraph 17 does not, as such, affect the operation of the principle embodied by paragraph 16, namely that data controllers remain accountable for personal data under their control, including in the context of transborder flows.

Paragraph 18 updates the language in the 1980 Guidelines to refer to “risk” and “proportionality”, indicating that any restrictions upon transborder data flows imposed by Member countries should be proportionate to the risks presented (i.e. not exceed the requirements necessary for the protection of personal data), taking into account the sensitivity of the data, the purpose and context the processing. In doing so, the text has been made more coherent with other provisions of the Guidelines, which implement a risk-based approach.

Paragraph 6 of the Guidelines acknowledges that Member countries have the ability to supplement the standards set forth by the Guidelines with additional measures necessary for the protection of privacy and individual liberties, which may impact transborder flows of personal data. Such measures should be implemented in a manner that least impacts the free flow of personal data.

### **National implementation**

Regarding national implementation, the 1980 Guidelines focused on the need for “legal, administrative and other procedures or institutions”. Although the 1980 Guidelines also highlighted non-regulatory measures, including self-regulation, it was recognised that there is a need for additional measures to help to protect privacy.

Paragraph 19(a) recommends that Member countries develop national privacy strategies that reflect a co-ordinated approach across governmental bodies. Elevating the importance of privacy protection to the highest levels within government helps improve the effectiveness of privacy protection. A further element of national privacy strategies concerns intra-governmental co-ordination. As highlighted in the OECD Recommendation on Regulatory Policy and Governance, Member countries should promote regulatory coherence between various levels of government. Where governments act as a policy maker for private sector activity, ensuring co-ordination across governmental departments is a necessary part of a national strategy. In addition, with many government departments making use of personal data, another dimension of co-ordination is to ensure a consistent level of protection across governmental bodies. Finally, national privacy strategies also offer a vehicle to ensure compatibility of policy development in related areas (e.g. national cybersecurity strategies).

Paragraph 19(g) calls upon Member countries to consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy. While existing initiatives attempt to raise awareness, there is broad recognition that more needs to be done. The Terms of Reference for the review of the Guidelines called for the creation of a culture of privacy among organisations and individuals through implementation of privacy literacy initiatives. Recent OECD instruments in related areas include measures for education and awareness as part of their policy frameworks.<sup>5</sup> Such initiatives should involve a wide range of stakeholders, including governments, privacy enforcement authorities, self-regulatory bodies, civil society organisations, and educators. As children are a particularly vulnerable category of data subjects, Member countries are specifically

encouraged to consider privacy literacy initiatives which seek to equip children with the knowledge and skills necessary to stay safe online and use the Internet to their benefit.

Privacy professionals play an increasingly important role in the implementation and administration of privacy management programmes. Several Member countries have already undertaken initiatives to define the competencies of privacy professionals. Credential programmes in data protection and privacy, as well as specialised education and professional development services may contribute to the development of the necessary skills. Paragraph 19(g) explicitly encourages Member countries to consider the adoption of measures to support such skills development.

Technical measures also play an increasingly important role in complementing laws protecting privacy. Paragraph 19(g) encourages measures to foster the development and deployment of privacy-respecting and privacy-enhancing technologies (PETs). For example, Member countries may choose to support the development of technical standards which advance privacy principles. International standardisation initiatives may also advance technical interoperability among PETs, which may in turn help promote wider adoption of these technologies. Accreditation and seal programmes may further foster the adoption of technologies beneficial to privacy. Other measures include the promotion of research and development, exchange of best practices, and the issuance of regulatory guidance.

Paragraph 19(h) invites Member countries to consider the role of actors other than data controllers, “in a manner appropriate to their individual role”. When discussing the need for complementary measures, it was recognised that other actors who, while not covered by the concept of data controller, nevertheless play an important role in determining the level of protection of personal data. Over the past few years, individuals have transcended the role of passive “data subjects” to become actively involved in creating, posting and sharing personal data about themselves, friends, relatives and others, over a vast array of information outlets including social networking services, rating systems and geo-location based applications. When discussing this change, it was recognised that not every actor should necessarily be regulated in the same way. For example, individuals acting in the context of their private lives are generally perceived to fall outside the remit of the Guidelines, as relationships among individuals are usually fundamentally different from those between individuals and organisations. Non-legislative measures, including education and awareness raising, were considered more appropriate to address the privacy risks associated with the activities of individuals. Where an individual does cause damage to the privacy interests of others, tort or civil law may offer a possible remedy, but other measures may need to be considered as well.

### **International co-operation and interoperability**

The OECD Recommendation on Internet Policy Making calls for a strengthening of consistency and effectiveness in privacy protection at a global level. The Communiqué which is annexed to it for information purposes further recognises the objective of governments to pursue global interoperability in this area. The Terms of Reference similarly identified the value of globally interoperable privacy frameworks that ensure effective protection of privacy and support the free flow of personal information around the world. However, as outlined by the G8 Deauville Declaration, we still “face considerable challenges in promoting interoperability and convergence among our public policies on issues such as the protection of personal data” (G8, 2011).

Paragraph 21 expresses the general objective of Member countries to improve global interoperability of privacy frameworks through international arrangements that give practical effect to the Guidelines. There exists a range of approaches to interoperability among privacy frameworks. The US-EU Safe Harbour Framework<sup>6</sup>, which was adopted under the EU adequacy regime and implemented in 2000, was an early example. Since then, several initiatives have been undertaken to bring together different approaches and systems of protection, including work by the privacy enforcement authorities within the framework of the EU Binding Corporate Rules and the APEC Cross-Border Privacy Rules System within the Asia-Pacific region. At the time of publication of these revised Guidelines, the Council of Europe continues its deliberations on the modernisation of Convention 108 on the Automated Processing of Personal Data. Further work is needed at the policy level towards a more seamless approach to global privacy governance.

A strong global network of privacy enforcement authorities working together is a first important step towards global interoperability. In 2005, the OECD revisited the issue of global cooperation among privacy enforcement authorities, resulting in the adoption of a new framework for cross-border co-operation in the form of the 2007 Recommendation. The three-year implementation report for the 2007 Recommendation highlighted the need for further efforts to ensure that privacy enforcement authorities have sufficient powers to administer effective sanctions and resources to accomplish their mission.<sup>7</sup> The Terms of Reference for the review of the Guidelines called for a redoubling of efforts to develop a globally active network of privacy enforcement authorities. Paragraph 20 reiterates the commitment expressed by Member countries in the 2007 Recommendation to enhance co-operation between privacy enforcement authorities. In particular, Member countries are encouraged to address obstacles – be they

legal or practical – towards information sharing among privacy enforcement authorities to facilitate coordinated and effective enforcement. Reducing the barriers to information sharing has been a particular concern in this respect.

Improving the global interoperability of privacy frameworks raises challenges but has benefits beyond facilitating transborder data flows. Global interoperability can help simplify compliance by organisations and ensure that privacy requirements are maintained. It can also enhance individuals' awareness and understanding of their rights in a global environment.

### **Improving the evidence base for policy making**

The OECD Recommendation on Internet Policy Making calls for the development of capacities to bring publicly available, reliable data into the policy-making process. The Communiqué, annexed to it for information, specifically notes the value of internationally comparable metrics.

The evidence base which is currently available for policymaking in the area of privacy is uneven. Household surveys by national statistical agencies provide some insight into privacy issues on the basis of internationally comparable metrics. However, the scope of these surveys, which focus primarily on awareness issues among individuals, is limited. There are gaps, for example, related to the technical or economic dimensions of privacy, as well as the implementation of prevention measures. Privacy enforcement authorities gather considerable data that are made public through annual reports, but not in a format well-suited to international comparisons. For example, progress in understanding complaint data, data breach statistics, and how fines and other sanctions influence data controllers' behaviour could be a potentially rich source of insight for policy makers. The addition of paragraph 22 in Part Six identifies the need for Member countries' support for initiatives to improve the evidence base in this area.

### **Other updates**

In addition to the substantive changes discussed in the previous section, the revised Guidelines reflect several minor changes which were made either to enhance readability or otherwise update the language of the 1980 Guidelines.

As a general matter, all references to specific parts of the Guidelines, have been replaced by a more generic phrasing ("these Guidelines").



Paragraph 2, which specifies the scope of the Guidelines, now refers to a “risk” rather than “danger” to privacy and individual liberties, reflecting the increased emphasis on risk within the revised Guidelines. This change should not be construed as preventing Member countries from extending the scope of laws protecting privacy or other privacy regimes to all forms of processing of personal data.

Former paragraph 3(b) has been deleted, as the ability for Member countries to exclude from the application of the Guidelines “personal data which do not pose any risk to privacy and individual liberties” is already reflected in paragraph 2.

Former paragraph 3(c) has been deleted, as Member countries have generally extended the scope of their domestic privacy laws to include the processing of personal data in general.

A new paragraph 3(b) has been added, to recognise the potential conflict between the protection of privacy and other fundamental rights arising from the now ubiquitous nature of personal data processing. It is also in line with the Communiqué on Principles for Internet Policy Making (OECD, 2011g) which underlines that “[p]rivacy rules should also consider the fundamental rights of others in society including rights to freedom of speech, freedom of the press, and an open and transparent government”.

Former paragraphs 15 and 16 of the 1980 Guidelines were removed in the interests of clarity and to avoid repetition, as the commitment of Member countries to the global free flow of information and security is already underlined elsewhere in the Recommendation.

### *Notes*

1. Remarks from Hon. Michael Kirby on the 30th anniversary of the OECD Privacy Guidelines, [www.oecd.org/internet/interneteconomy/49710223.pdf](http://www.oecd.org/internet/interneteconomy/49710223.pdf).
2. The system of BCRs is being further developed, see [http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm)
3. See [www.huntonfiles.com/files/webupload/CIPL\\_Galway\\_Conference\\_Summary.pdf](http://www.huntonfiles.com/files/webupload/CIPL_Galway_Conference_Summary.pdf).
4. APEC, APEC Cross-border Privacy Rules System – Policies, rules and guidelines, [www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx)
5. E.g., OECD (2002), OECD (2012b).
6. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, Official Journal of the European Communities, 25 August 2000, L-215, 7-47. See also [www.export.gov/safeharbor](http://www.export.gov/safeharbor).
7. See OECD (2011f).

## *References*

- G8 (2011), Deauville Declaration: Internet,  
[www.g8.utoronto.ca/summit/2011deauville/2011-internet-en.html](http://www.g8.utoronto.ca/summit/2011deauville/2011-internet-en.html)
- OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards A Culture Of Security,  
[www.oecd.org/internet/interneteconomy/15582260.pdf](http://www.oecd.org/internet/interneteconomy/15582260.pdf)
- OECD (2007), Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy,  
[www.oecd.org/internet/interneteconomy/38770483.pdf](http://www.oecd.org/internet/interneteconomy/38770483.pdf).
- OECD (2011a), Council Recommendation on Principles for Internet Policy Making [www.oecd.org/internet/interneteconomy/49258588.pdf](http://www.oecd.org/internet/interneteconomy/49258588.pdf).
- OECD (2011b), Communiqué on Principles for Internet Policy Making [www.oecd.org/internet/interneteconomy/49258588.pdf](http://www.oecd.org/internet/interneteconomy/49258588.pdf).
- OECD (2011c), “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”, *OECD Digital Economy Papers*, No.176,  
<http://dx.doi.org/10.1787/5kgf09z90c31-en>.
- OECD (2011d), “Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy”, *OECD Digital Economy Papers*, No. 178,  
<http://dx.doi.org/10.1787/5kgdpm9wg9xs-en>.
- OECD (2011e), “Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,” [www.oecd.org/sti/interneteconomy/48975226.pdf](http://www.oecd.org/sti/interneteconomy/48975226.pdf)
- OECD (2011f), “Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy”, *OECD Digital Economy Papers*, No. 178,  
<http://dx.doi.org/10.1787/5kgdpm9wg9xs-en>
- OECD (2011g), Council Recommendation on Principles for Internet Policy Making, [www.oecd.org/internet/interneteconomy/49258588.pdf](http://www.oecd.org/internet/interneteconomy/49258588.pdf)
- OECD (2012a), Recommendation of the Council on Regulatory Policy and Governance, [www.oecd.org/gov/regulatorypolicy/49990817.pdf](http://www.oecd.org/gov/regulatorypolicy/49990817.pdf)
- OECD (2012b), Recommendation of the Council on the Protection of Children Online,  
<http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False>.

### *Chapter 3.*

## **Original explanatory memorandum to the OECD Privacy Guidelines (1980)**

### **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 harmonisation 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***

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.

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.

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*

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 this 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.

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.

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*

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.

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.

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***

There are several international agreements on various aspects of telecommunications which, while facilitating relations and co-operation 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).

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 of Human Rights of 4th November, 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December, 1966).

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.

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.

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. The Convention was adopted by the Committee of Ministers on 17th September 1980. It 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.



The *European Community* has carried out studies concerning the problems of harmonisation 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*

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.

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.

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 harmonisation 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 1 July 1979.

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 arose 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 arose, 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.

During its work the Expert Group maintained close contacts with corresponding organs of the Council of Europe. Every effort was 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 will 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.

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*

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.

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.

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*

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.

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***

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***

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***

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.

Some Member countries have emphasised 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***

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.

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

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 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***

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.

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.

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.

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.

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 emphasised 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***

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***

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.

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.

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***

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.

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***

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***

To provide formally for exceptions in Guidelines which are part of a 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”).

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***

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***

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***

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.

The Expert Group 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.

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 person, etc.

#### ***Paragraph 8: Data Quality Principle***

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***

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 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***

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***

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 emphasised 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***

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***

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:

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.

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.

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***

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***

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.

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.

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).

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.

**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.

**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 intentional data traffic. These are matters which were not addressed by the Expert Group, being outside its Mandate.

### ***Paragraph 19: National Implementation***

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. specially set up supervisory bodies, existing control facilities such as courts, public authorities, etc.).

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) 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***

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.

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***

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***

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.

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.

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***

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.

## *Chapter 4.*

### **The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011)**

Thirty years ago OECD governments adopted a set of Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. Faced with twin concerns about threats to privacy from more intensive use of personal data and the risk to the global economy of restrictions on the flow of information, the OECD produced the first internationally agreed statement of the core privacy protection principles.

The Guidelines have been a remarkable success. They represent an international consensus on personal data protection in the public and private sectors. They have influenced the development of national legislation and model codes within OECD member countries, and beyond.

This chapter begins by recalling the development and influence of the Guidelines. It then describes a number of current trends in the processing of personal data and the privacy risks in this evolving environment. It identifies some of the challenges that today's environment brings for protecting privacy under existing approaches, and highlights a number of current initiatives and innovative approaches to privacy. Particular attention is focused on the impact of the Internet and other technologies, consistent with the issues and priorities highlighted in the 2008 Seoul Ministerial on the Future of the Internet Economy.

The chapter aims to take a broad view of the current landscape for privacy, with a primary focus on economic activities. It does not describe in detail the myriad of initiatives to implement the Privacy Guidelines in OECD countries and beyond.

The chapter was prepared with the special assistance of Barbara Bucknell from the Office of the Privacy Commissioner of Canada. It has been informed by a series of events organised by the OECD to mark the 30<sup>th</sup> anniversary of the Privacy Guidelines: [www.oecd.org/sti/privacyanniversary](http://www.oecd.org/sti/privacyanniversary). The Working Party on Information Security and Privacy approved the report for submission to the Committee for Information, Computer and Communications Policy, which declassified it in March 2011.

**Main points*****1. The OECD Privacy Guidelines have been a remarkable success.***

The Guidelines represent the first internationally agreed-upon set of privacy principles.

They have influenced the development of national data protection legislation and model codes within the OECD member countries. The Guidelines have also influenced the development of the APEC Privacy Framework, expanding their reach beyond the OECD membership.

→ Framed in concise, technologically neutral language, the principles have proven to be adaptable to countries with varied governmental and legal structures and to changes in the social and technological environment.

***2. More extensive and innovative uses of personal data are bringing increasing economic and social benefits.***

Organisations have greatly benefited from the many improvements in personal data processing, as have individuals. Personal data is increasingly a core asset for modern business operations and essential to effective government administration. It has become a “currency” for the Internet economy, exchanged for access to online content and services without monetary payment.

→ The role of personal data protection principles in helping to maintain trust is integral to the continued benefits of personal data flows.

***3. The evolving uses of technology and personal data raise challenges for determining the appropriate scope for the application of privacy protections.***

Advances in analytics and the apparent limitations on anonymisation mean that more data than ever can be related to an individual and thus potentially fall within the scope of privacy protections.

Individuals currently play a greater role in generating and disseminating personal data – a role more akin to that of a data controller than a data subject – raising new issues regarding the impact they are having on the privacy of others and themselves. Further consideration may need to be given to their role in privacy protection frameworks.

Given the increasing complexity of interactions between certain types of technology and certain business models, it is becoming more difficult to allocate responsibilities. The traditional concept of data controller (and data

processor) may not be able to encompass all the actors that may have a role to play in data protection.

→ When the scope of application is broad and the allocation of responsibilities unclear, the core privacy principles become more challenging to implement and enforce.

***4. It is increasingly difficult for individuals to understand and make choices related to the uses of their personal data.***

The uses of personal data are becoming increasingly complex, and non-transparent to individuals.

Individuals may face a lack of information, or overly detailed information about how their personal data may be used. Individuals may find it difficult to assess information risks when confronted with complex information and competing interests. Further complications may arise when privacy policies change too frequently.

Access to modify or delete personal data can also be challenging both for individuals to obtain and organisations to provide, given existing business models, and the volume and dissemination of data in the online environment.

→ Challenges related to offering individuals choices (e.g. consent) about how their data is used and how individual access is provided within a broader regime of privacy protection needs further exploration.

***5. The abundance and persistence of personal data, readily available globally, has provided benefits while at the same time increasing the privacy risks faced by individuals and organisations.***

Securing personal data has become a greater challenge. Individuals are exposed to increased potential harms including the risk of identity theft. Data breach notification has become an increasingly important element of privacy oversight.

The growing value of personal data increases the risks that data will be used in ways that neither the organisation nor the individual anticipated when the data was collected.

The combination of various methods of collecting and processing data allows for more detailed monitoring of the activities of individuals.

→ Increased attention is needed to mitigate the privacy risks to individuals posed by monitoring, unanticipated secondary usage, and data security breaches.



***6. Advances in technology and changes in organisational practices have transformed occasional transborder transfers of personal data into a continuous, multipoint global flow.***

There are variations in national and regional approaches to personal data protection, which are more noticeable when applied to global data flows.

Countries have chosen different approaches to protecting data and have expressed differing degrees of concern about barriers to cross-border data flows.

Organisations that operate globally and privacy enforcement authorities may not be certain about questions of applicable law, jurisdiction and oversight.

Organisations may find compliance with complex and sometimes conflicting privacy laws to be difficult and may not be able or willing to tailor their operations to meet the specific requirements of smaller jurisdictions.

The Guidelines have been successful in influencing the development of legislation and model codes, but less successful in encouraging approaches that seek a balance between protecting personal data and preventing barriers to transborder data flows.

→ The importance of effective, global, practical approaches to governing the collection, use and transfer of personal data has never been greater.

***7. There is interest by the global privacy community and commitment within international organisations, governments, and privacy enforcement authorities to addressing current challenges.***

Important and innovative developments since the privacy guidelines – for example, the emergence of a privacy profession, privacy by design, privacy impact assessments, and data breach notification – offer encouraging signs of a broad multi-stakeholder commitment on the part of privacy advocates, the technical community, businesses and governments to protecting privacy.

Greater efforts by privacy enforcement authorities around the world to co-operate represent an important development and a key component of a more globally effective approach to protecting privacy.

Many countries and regions are carefully examining the effectiveness of their data protection regimes, and there are movements to seek consensus on developing privacy protections, such as global privacy standards.

→ These initiatives could play a role in finding practical, effective ways to improve privacy protection and thereby foster the economic and social benefits enabled by more extensive and innovative uses of personal data.

### **The development and influence of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**

The 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (“OECD Guidelines”) represent a consensus of the OECD member countries on personal data handling and protection. The Guidelines were developed because of concerns about the consequences of inconsistent or competing national data protection laws that had arisen in response to new and automated means of processing information. The Guidelines emphasised that OECD countries have a common interest in protecting privacy and individual liberties. At the same time, another goal was to ensure that the spread of privacy laws should not unduly restrict transborder data flows and the economic and social benefits they bring. Faced with the twin concerns about threats to privacy from more intensive use of personal data and the risk to the global economy of restrictions on the flow of information, the OECD produced one of the flagship statements of the core privacy protection principles.

The linking of privacy to the emergence of new technologies dates back at least to the 19<sup>th</sup> century, when Samuel Warren and Louis Brandeis wrote about the impact of the portable camera on the “right to be let alone”.<sup>1</sup> The OECD Guidelines resulted from a number of related developments that began to emerge in the late 1960s around the introduction of first-generation, mainframe computers. Today, in the face of vastly increased computing speed and capacity, innovative products and services and the increased economic value of personal data, many jurisdictions are re-examining their approach to data protection to determine if their current practices are still up to the task of effectively protecting privacy in the face of 21<sup>st</sup> century information and communications technologies while at the same time still supporting the growth of commerce. Similarly, the purpose of this paper is to contribute to a process of assessing the continued effectiveness of the OECD Guidelines, 30 years after their adoption.

#### ***The emergence of computerised processing, concerns about privacy and national legislation***

Privacy became an issue in the late 1960s because of the convergence of two trends: the post-industrial information revolution and the growing government use of personal data. The advantages of using computers to more efficiently process data were increasingly apparent yet at the same

time so too were growing concerns about the possible loss of dignity or the erosion of rights that could result from the misuse of personal data.<sup>2</sup> There was recognition too of the growing awareness in certain circles of the need to empower citizens in claiming their rights.

Governments in many OECD member states responded to these concerns by creating task forces, commissions and committees to study the issue. In 1969, consultations for a law began in the Land of Hesse, Germany.<sup>3</sup> In the United Kingdom, a Committee on Privacy chaired by the Rt. Hon. Kenneth Younger published a 350-page report in 1972. A Canadian Task Force was created “to consider rights and related values, both present and emergent, appurtenant to the individual and the issues raised by possible invasion of privacy through the collection, storage, processing and use of data contained in automated information and filing systems.” The resulting report, *Privacy and Computers*, was published in 1972. The Nordic Council, a forum for discussion among the governments of Denmark, Finland, Iceland, Norway and Sweden, began looking at data protection in 1971. A Swedish Parliamentary Commission, established in 1969, issued a report in 1972 entitled *Computers and Privacy*. In the Netherlands, the State Commission Protection of Private Life in relation to Personal Data Registrations, or “State Commission Koopmans,” was established in 1972, which reported in 1976. The French Ministry of Justice appointed the Tricot Commission on Data Processing and Freedom in 1974, following revelations about a proposal to use personal identifiers to link the personal data in a number of databases and public registers. In Australia, the Australian Law Reform Commission (ALRC) began its work on privacy in 1976 (the report was published in 1983). The ALRC had also issued a report on unfair publication in 1979 that included privacy as a strong consideration.

In the United States, the Secretary of the Department of Health, Education and Welfare (HEW) created a Committee on Automated Personal Data Systems. The Committee’s 1973 report, *Records, Computers and the Rights of Citizens*,<sup>4</sup> is noteworthy because it contained the first explicit reference to “fair information practices”:

*Safeguards for personal privacy based on our concept of mutuality in record-keeping would require adherence by record-keeping organizations to certain fundamental principles of fair information practice.*

- *There must be no personal-data record-keeping systems whose very existence is secret.*
- *There must be a way for an individual to find out what information about him is in a record and how it is used.*
- *There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.*

- *There must be a way for an individual to correct or amend a record of identifiable information about himself.*
- *Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.*

Academics also began to take an interest in the privacy implications of new technologies, beginning in the late 1960s. Alan Westin's *Privacy and Freedom* is one obvious example.<sup>5</sup> Westin went on to co-author *Databanks in a Free Society* with Michael Baker.<sup>6</sup> Arthur Miller's *The Assault on Privacy* was subtitled, *Computers, Data Banks and Dossiers*. Paul Sieghart, a British human rights lawyer and author, published *Privacy and Computers*<sup>7</sup> in 1976 and David Flaherty published a study on government data banks, *Privacy and Government Data Banks: An International Perspective*. Frits Hondius of the Council of Europe wrote *Emerging Data Protection in Europe*, the purpose of which was to "describe the dawn of a new corpus of law in Europe called 'data protection'." In Australia, the Boyer Lectures by Professor Zelman Cowan, which were broadcast by the Australian Broadcasting Commission in 1969, were captured in the book, *The Private Man*.

The concerns identified in these studies and books contributed to legislative responses in several countries. To cite a few examples, the Hesse Parliament adopted the *Data Protection Act* in September 1970. The Swedish government responded to the *Computers and Privacy* report by passing the *Data Act*, the first national data protection legislation, and creating the Data Inspection Board in 1973. In the Netherlands, legislation was proposed in 1981, leading to the *Act on Personal Data Registrations* and the creation of the data protection authority in 1988. The U.S. *Freedom of Information Act* was enacted in 1966, the *Fair Credit Reporting Act* was enacted in 1970, and the *Privacy Act* was passed in 1974. The French (Tricot) Commission led to the Law on Informatics and Freedom in 1978, and the creation of *La Commission nationale de l'informatique et des libertés* (CNIL), the French data protection agency. New Zealand set up its first Privacy Commissioner in 1976 to oversee a national law enforcement database and gave the new Human Rights Commission a broad policy remit the following year. The *Canadian Human Rights Act* of 1977 contained a set of fair information practices for the federal public sector. The Federal Republic of Germany, Norway, Denmark, Austria and Luxembourg also passed legislation before the end of the decade. As a result, more than a third of the then 24 OECD member countries had adopted national legislation by 1980.

The focus on the potential dangers to data privacy posed by the use of information and communication technologies (ICTs) to store and also process personal data had an impact on the legislation that was passed in the 1970s. Firstly, despite the numerous references to “privacy” in the studies and books that were published during the decade, and in some cases in the legislation itself, the focus was on the protection of personal data or data as a means of protecting privacy.

Secondly, there was an emphasis on automated processing of personal data. Sweden’s 1973 *Data Act* only applied to computerised files; France’s 1978 law refers to informatics in its title and the Council of Europe’s 1973 and 1974 resolutions only applied to automatic data processing. The Younger Committee report was limited to looking at computerised processing as suggested by the references to “systems” in the principle.

Most of the government reports and legislation mentioned above contained similar principles for protecting personal data. Although it did not use the term “fair information practices”, the Younger Committee introduced a minimization principle (“the amount of information collected and held should be the minimum necessary for the achievement of a specified purpose”). The Younger Committee’s report also contained a principle to the effect that “care should be taken in coding value judgements.” In 1973, the Council of Europe adopted Resolution (73) 22 on the protection of the privacy of individuals in relation to electronic data banks in the private sector.<sup>9</sup> The resolution contains ten principles. The Council followed this in 1974 with a similar non-binding resolution for the public sector.

Despite these differences, a consensus in many advanced economies around a core set of principles had emerged by the mid-1970s, “on general principles which policy-makers would apply to a wide variety of personal-data systems.”<sup>10</sup> In hindsight, it is remarkable how quickly this developed.

### ***The approach of the OECD***

The growing importance of ICTs and transborder data flows and their implications for privacy first attracted the interest of the OECD in 1969. Initially, work was undertaken by the Computer Utilisation Group, which produced a number of Informatics Studies with titles such as “Computerised Data Banks in Public Administration”, “Digital Information and the Privacy Problem”, and “Policy Issues in Data Protection and Privacy.”

In 1974, the OECD held a two-day seminar that included sessions on “The Personal Identifier and Privacy”, “Right of Citizen Access to their File” and “Rules for Transborder Data Flows.” The seminar was attended by almost 100 people, including many current and future experts and commissioners.

A Synthesis Report was prepared by the OECD Secretariat in 1976. The Report succinctly stated the policy problem that the seminar was attempting to address and offered some possible solutions:

*Innovations in modern information technology, especially computers and telecommunications, bring new dimensions to traditional methods of record-keeping. They have also sharpened public awareness of the human value, "privacy", which may face major changes as the use of automated information and transmission systems expands. What is at stake is the societal control of modern information technology, and while the past decade has seen a "literature of alarm", the 1970s will be dedicated to the development of "social software" in the form of laws, regulations, codes of ethics, etc., necessary to control information technology and ensure that its development will be, on balance, of a positive dimension to humanity.<sup>11</sup>*

This seminar was followed in 1977 by a larger meeting on "Transborder Data Flows and the Protection of Privacy", attended by approximately 300 people from member countries, the private sector and inter-governmental organisations. At the 1977 symposium, the economic value and national interest of transborder data flows was highlighted in a comment made by Louis Joinet of France, at the time, the President of the *Commission nationale de l'informatique et des Libertés*, who was later instrumental in crafting the OECD Guidelines:

*Information is power, and economic information is economic power. Information has an economic value and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This in turn may lead to a loss of national sovereignty through supranational data flows.<sup>12</sup>*

Following the symposium, an Expert Group chaired by Honourable Justice Michael Kirby of Australia, was created to begin work on guidelines. The creation of the Expert Group and the decision to work on guidelines were in response to the concerns that had surfaced over the previous decade about the growing use of personal data and the increasing reliance on computerised processing that prompted several countries to pass legislation. Given its mandate to foster economic growth and contribute to the expansion of world trade, the OECD was also concerned about the possibility that national laws would create barriers to the free flow of information that would impede growth.

The hope was that by reaching agreement on a broad set of fundamental principles to protect personal data that could be adopted by the member countries and other nations, there would be less pressure to regulate or

attempt to control international data flows. The emphasis on trying to ensure that the measures being introduced to protect personal data would not result in restrictions on transborder data flows runs through the Guidelines.

Although there was a broad consensus about the principles and the need to take action, reaching agreement was not easy. According to Justice Kirby, “it is something of a miracle that the OECD Guidelines emerged at all.”<sup>13</sup> One of the key challenges facing the Expert Group is described in the Explanatory Memorandum:

*...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.*

The Explanatory Memorandum also suggests that there was debate around how the Guidelines should address other “key issues” such as sensitive data, automated data processing, the application to legal persons (corporations, associations), oversight and sanctions, retention periods and other implementation matters, applicable law and exceptions.

The Guidelines were a carefully crafted compromise that reflects the differing views of the members of the Expert Group on these and other potentially contentious issues. This spirit of compromise is reflected in many parts of the package of documents that collectively form the Guidelines, beginning in the Council Recommendation that refers to “reconciling fundamental but competing values such as privacy and the free flow of information.”

Although the Guidelines’ eight basic principles do not refer to sensitive data or to automated processing, the Scope section suggests that “different protective measures” can be applied based on the context or the sensitivity of the personal data, and recognises that some member countries may choose to limit the application of the Guidelines to the automatic processing of personal data (see Box 1).

The Guidelines were adopted by the OECD Council on 23 September 1980. This was the same month that the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was adopted, although the Convention was not opened for ratification until 1981. Justice Kirby has suggested that the OECD Expert Group was able to draw on the work of the Council of Europe, the Nordic Council, as well as the contributions of those member countries that had existing privacy legislation. Although Convention 108 differs from the OECD Guidelines in a number of important respects (*e.g.* its binding character, treatment of sensitive data, and application to automated processing) there is substantial consistency between the core principles of the OECD Guidelines and Convention 108.

**Box 1. Basic Principles of National Application (OECD Privacy Guidelines, Part 2)****Collection Limitation Principle**

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**

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**

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**

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**

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**

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**

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
  1. within a reasonable time;
  2. at a charge, if any, that is not excessive;
  3. in a reasonable manner; and
  4. in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

**Accountability Principle**

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



### *The influence of the Guidelines*

The Guidelines were the first internationally agreed upon statement of core information privacy principles that reflected the diverse views and perspectives of countries around the world.

The eight basic principles are concise, technologically neutral, non-binding, and written using commonly understood language. This has made them remarkably adaptable to the varying government and legal structures of the implementing countries and the changing social and technological environment, and has contributed to their enduring influence and importance. The Guidelines reflect an arrangement whereby all OECD members should implement privacy protections consistent with those outlined in the Guidelines (which should be regarded as a minimum) and not restrict data movement to other countries that are abiding by the Guidelines. There are, however, exceptions to the presumption of free flow if the other member country does not substantially observe the Guidelines or if the re-export of data would circumvent domestic legislation. Restrictions may also be imposed if there is no equivalent protection for sensitive information (see Box 2).

#### **Box 2. Basic principles of international application: free flow and legitimate restrictions (OECD Privacy Guidelines, Part 3)**

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

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.

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.

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.

The Guidelines call for member country implementation through a variety of methods, and to ensure that there is no unfair discrimination. The response has included legislation, self-regulation, and enforcement measures that provide a means for individuals to exercise rights, and sanctions and remedies for compliance failures.

#### *Legislative approaches*

The Guidelines have been particularly influential in countries that had not passed legislation by 1980. The Australian Privacy Act of 1988 contains 11 Information Privacy Principles, based directly on the Guidelines. When the Act was amended in 2001 to cover the private sector, ten National Privacy Principles were added, which also include principles covering transborder data flows, anonymity, and identifiers. Following a recent review by the Australian Law Reform Commission (ALRC), the Australian government has agreed with the ALRC's recommendation to create a single set of principles.<sup>14</sup>

The New Zealand *Privacy Act*, passed in 1993, contains 12 principles. The first four principles all relate to collection, elaborating on the OECD's Collection Limitation and Purpose Specification Principles. The New Zealand Act adds a principle on unique identifiers that is not found in the Guidelines. The explicit reference to the OECD Guidelines in a 2010 amendment to the New Zealand Act is a testament to the Guidelines' enduring influence.<sup>15</sup>

Canada's private sector legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which came into force in January 2001, requires organisations to comply with ten principles set out in a Model Code, which was incorporated directly into the Act. This Model Code, the *Model Code for the Protection of Personal Information (CAN/CSA-Q830-96)*, was developed by a committee made up of private sector, government, trade union and civil society representatives working under the auspices of the Canadian Standards Association. The committee used the OECD Guidelines as a starting point. In addition to moving the Accountability Principle to the beginning, the model code created a separate consent principle and added a challenging compliance principle, giving individuals the right to challenge an organisation's compliance with the principles.

In 2003, Japan's *Act on the Protection of Personal Information* was passed and came fully into force on 1 April 2005. This law applies to the collection, use and disclosure of personal data in private businesses that process the personal data of more than 5 000 individuals, and incorporates the OECD privacy principles. With overall responsibility for the Act in the Consumer Affairs Agency, Japan's various ministries develop guidelines

(40 guidelines covering 27 sectors) to assist organisations in implementing the legislation. At the same time, other laws were enacted that cover aspects of the personal data protection practices of government organisations.

Korea's *Act on the Promotion of Information and Communications Network Utilization and Data Protection Act* came into effect in 2001. Generally following the privacy principles laid out in the OECD Guidelines, the law initially applied only to providers of information and communications networks. The Act was broadened in 2009 to include 14 additional types of businesses. The Act contains provisions that require the government to develop policies that promote the use of security measures, protect personal data, and protect youth in the information and communication networks. Transfers of personal data as a result of a merger or change of ownership are also covered under this law.<sup>16</sup>

In 2010, Mexico became the latest OECD country to implement the Guidelines by means of legislation.<sup>17</sup> Also in 2010, Turkey amended its Constitution to give individuals additional rights related to the protection of their personal data, addressing issues of consent, use limitation, access and correction.

In terms of transborder data flows, some of these countries enacted privacy legislation that presumes the free flow of data, making any restrictions an exception (for example, New Zealand, Australia and Canada), while others enacted some form of restriction, with exceptions to enable the free flow of data across borders (for example, Korea and Japan, which prohibit transfers unless consent is present). Those European nations that are OECD member countries as well as member states of the European Union have enacted legislation that is in keeping with the European Union Directive 95/46/EC (the "EU Directive"), which is discussed below.

Sector-specific legislation in areas such as health and financial information has been adopted in many countries. The *Telecommunications Act 1997* in Australia gives the Privacy Commissioner responsibility for monitoring compliance over the part of the law that deals with the privacy of personal information held by carriers, carriage service providers and others. The United States has numerous sector-specific laws that protect privacy, for example in the areas of financial services, health care, and credit reporting. In Canada, several provinces have passed personal health information legislation. These laws form part of the overarching national privacy regime, which establishes a set of substantially similar privacy rules across all spheres of activity.

Some countries have adapted general consumer protection legislation to protect personal data. In the United States, for example, the Federal Trade Commission and the Attorneys General of individual states enforce laws that prohibit unfair and deceptive trade practices in cases involving privacy harms and data security breaches.

Freedom of information legislation in many OECD countries has a data protection component by providing, for example, another means for individuals to access information about themselves held by the government. Certain countries also included particular components of the OECD principles in other types of legislation.<sup>18</sup>

#### Self-regulation

In addition to encouraging the adoption of appropriate legislation, the Guidelines recommend that member countries encourage and support self-regulation. Following the adoption of the Guidelines, the United States Department of Commerce sent letters to 750 corporations urging them to adopt the Guidelines. In Japan, the government has undertaken the role of certifying a number of “Authorized Personal Information Organizations” that advise businesses and resolve privacy disputes.<sup>19</sup> The Guidelines have served as a basis for numerous private sector privacy policies, self-regulatory policies and model codes, and some individual companies and trade associations have endorsed the Guidelines.

#### Enforcement

Nearly all OECD countries have established authorities for enforcing data protection laws. The 2006 OECD *Report on the Cross-Border Enforcement of Privacy Laws* describes the privacy enforcement authorities for OECD countries, their commonalities and differences, as well as their challenges in addressing cross-border issues<sup>20</sup>. Generally speaking, enforcement authorities are a single commissioner, with certain duties to investigate complaints, with some supervising the data processing activities of data controllers. In some countries, the commissions are composed of a body of commissioners. In Japan and Korea, privacy oversight rests with groups of officials in government departments. In France, the authority is supervised by 17 commissioners, 12 of whom are elected or designated by the assemblies or courts they belong to. Many countries also have regional enforcement authorities, such as Australia, Canada, Germany, and the United States. In recent years, there has also been an increased emphasis on enforcement powers, for example, in the United Kingdom. Many of the laws that were passed initially provided oversight bodies with limited powers. Many data protection authorities may go to Court for enforcement, and individuals also may seek redress through the courts for any misuse of personal data<sup>21</sup>.

### Other international instruments

Although the influence of the Guidelines on the EU Directive is less clear, both instruments share, along with Convention 108, many of the same basic principles. The EU Directive developed rules to harmonise data protection within the European Union and to ensure that the standard of privacy protection in Europe would not be weakened by the transfer of data from Europe to other countries.<sup>22</sup> The Directive required protections, additional to those included in the Guidelines, concerning the transfer of personal data outside of the European Union. Binding on EEA member states, the Directive has also been highly influential in the development of privacy legislation outside of Europe.

The OECD's Guidelines were instrumental in the development of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. APEC is a multi-national organisation with a mandate to encourage economic growth, co-operation, trade and investment in the Asia-Pacific region. Seven of the 21 APEC economies are also OECD members. Work on the Framework began in 2003, and it was endorsed by the APEC Ministers in November 2004. The Framework contains nine Information Privacy Principles, including one on preventing harm, and specifically references the OECD Guidelines. In addition to the similarity between the APEC and OECD principles, the APEC Framework is also a non-binding instrument and is intended to encourage the development of appropriate information privacy protections and ensure the free flow of information in the Asia Pacific region.<sup>23</sup>

The United Nations also has Guidelines Concerning Computerized Personal Data Files, adopted on 14 December 1990. These guidelines contain ten principles for inclusion in national legislation. The UN Guidelines are largely rooted in human rights concerns,<sup>24</sup> although there is a principle concerning transborder data flows.

### Influence on other OECD work

The Guidelines have served as a basis for much of the privacy work at the OECD that followed, such as the development of the OECD Privacy Statement Generator and the Radio Frequency Identification Policy Guidance document. Privacy Online: OECD Guidance on Policy and Practice is a collection of the instruments that serve as the foundation for privacy protection at the global level, namely, the 1980 OECD Privacy Guidelines, the 1985 Declaration on Transborder Data Flows and the 1998 Ministerial Declaration on the Protection of Privacy on Global Networks. In 2006, the OECD released a Report on the Cross-border Enforcement of Privacy Laws, and a year later, the OECD Council adopted a new

Recommendation that sets out a framework for co-operation in the enforcement of privacy laws. That Recommendation implements in considerable detail the provision in the Privacy Guidelines addressing mutual assistance.<sup>25</sup>

The OECD Guidelines have also influenced consumer protection work within the OECD, in recognition of the connection between privacy and consumer protection. For example, the OECD's 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce* ("E-commerce Guidelines") specifically incorporate the Privacy Guidelines and state that "Business-to-consumer electronic commerce should be conducted in accordance with the recognised privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980)".<sup>26</sup> In addition, privacy issues are discussed throughout the report "Empowering E-consumers, Strengthening Consumer Protection in the Internet Economy,"<sup>27</sup> that served as the basis for the December 2009 conference celebrating the 10<sup>th</sup> anniversary of the E-commerce Guidelines.

### Current trends in the processing of personal data

In considering current trends in the development of technology and growth of transborder data flows, it may be useful to begin by reviewing what the Explanatory Memorandum stated about the issues related to automatic data processing in 1980:

*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.*<sup>28</sup>

In the 30 years since the Guidelines were adopted, those possibilities have become reality. There have been dramatic changes in the volume and uses of personal data, triggered in part by improvements in the ability to collect, store, process, aggregate, link, analyse, and transfer vast quantities of data. Advances in computing power have combined with easy access to fixed and mobile devices globally connected through the Internet to transform the role of personal data in the economy and society. The shift from analogue to digital technology across communications and entertainment media has also led to much greater capacity to store and share personal data, notably pictures, sound, film, and video images.

Personal data is increasingly a core asset for modern business operations and is essential to effective government administration, a factor that suggests that the trends and innovation described below will continue.

### *Technological developments*

#### *Communications networks*

There has been a tremendous development in communications networks since the era when the Guidelines were adopted. First and foremost has been the widespread adoption of the Internet. Satellite, cable and fibre-optic transmission lines have increased access as well as driven data transfer capacity, and transmission technologies have increased our ability to take advantage of this enhanced delivery capacity. New devices, greater interoperability and a tremendous growth in wireless technologies have also contributed to this increased rate of data transfer.

#### *Fixed and mobile computing devices*

Personal computers were not widely available in 1980. In the ensuing 30 years, there has been a dramatic rise in the number of personal computers in use by individuals at home and in the workplace. In 2008, the percentage of all households in OECD member countries that had access to a computer at home (including personal computers, portable, and handheld) ranged from approximately 12% to 92%, with 75% or more of households in 15 countries surveyed having computer access.<sup>29</sup>

More recently, mobile computing devices – including “smart” phones – have emerged. Powerful but portable, these devices are a transformative technology, combining geolocational data and Internet connectivity to support a broad new range of services and applications, many of which rely on (or involve) the collection and use of personal information to generate revenue. The mobile market has skyrocketed, with the total number of mobile subscriptions in OECD countries at 1.14 billion in 2007.<sup>30</sup> Game consoles and portable gaming devices are other, more recent ways of accessing the Internet that are becoming popular.<sup>31</sup>

What these developments have meant is that there is increasingly easy access to the Internet, leading to a greater collection and use of personal data at a distance and across borders. In 2008, the percentage of all households with access to the Internet in France, the United Kingdom, and Sweden, to name three member countries, was 62.3%, 71.1%, and 84.4%, respectively.<sup>32</sup> By September 2009, the number of Internet users worldwide reached 1.7 billion. Within the OECD, the United States had 230 million internet users, Japan (100 million), Germany (54 million) and the United Kingdom (47 million).<sup>33</sup>

In addition to increased Internet access, most mobile devices also offer other tools that may involve capturing images, sound and location data. The potential for capturing and distributing images and tracking the location and movements of individuals, often without them being aware, has grown significantly over the past thirty years.

#### *Storage, analytics, sensor systems and location data*

In the past, the cost of storing data was a disincentive for keeping information that was no longer, or unlikely to be, needed. Times have changed. Storage costs for digital information are decreasing to the point where data can generally be kept for long periods if not indefinitely. The volume of personal data maintained by organisations and individuals is expanding significantly. Storage practices are evolving: increasingly, organisations and individuals are using third-party data storage services that may be located outside their country. The capacity to tap into this resource has grown, and new business models are providing a good return on investment. Moore's Law, which holds that processing power doubles about every 18 months, especially relative to cost or size, has largely held true over the years. Data processing tools have become increasingly powerful, sophisticated, ubiquitous, and inexpensive, making information easily searchable, linkable and traceable for many stakeholders, not just government and large corporations.

The development and use of algorithms and analytics has made large data sets more accessible and capable of being linked, which can result in increased and new uses of the data, thereby making data more valuable. The remarkable pace of development and evolution of technologies and business models make it less easy to accurately describe potential future uses of information at the time of collection. This has resulted in a desire to keep personal data for an as-yet undefined, later purpose and reflects the intrinsic value of personal data to both business and governments. Search engines, which allow for easy, global searches of any personal data made public, make data retrieval much easier for Internet users. Growing use of linked data sources and contextual semantic technologies allow for greater and more sophisticated automation in the discovery and aggregation of personal data. Automated decision-making through data mining and rule engines is increasingly possible in a variety of contexts. Moreover, searches are no longer restricted to text and numbers: facial recognition applications now allow users to identify individuals in images online with growing accuracy. The phenomenon of "big data", namely, the vast quantities of data that can be stored, linked, and analysed, brings with it the possibility of finding information, trends, insights that were not previously obvious or capable of being ascertained. This may hold great economic and social value, but there can be privacy implications.



Adding more data to the mix are sensor networks. Wireless sensor and actuator networks are networks of nodes that sense and potentially also interact with their environment. They communicate the information through wireless links ‘enabling interaction between people or computers and the surrounding environment.’<sup>34</sup> These networks are being developed in areas such as health care, environment, transportation systems or in the development of energy control systems,<sup>35</sup> such as smart meters. They offer convenience and cost-savings to citizens, industry and governments. At the same time, they also have privacy implications depending on the use of the data collected and the security of the wireless transmission of the data, including the risk of unauthorized third-party interception.

Radio frequency identification (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.”<sup>36</sup> Use of RFID ranges from transportation to government identification and passports to retail purposes, and has the potential to improve business processes and performance by allowing for better tracking of goods as they move through the supply chain. Individuals may not always be aware of RFID devices that are embedded in products they buy, for example. Tags may store personal data, and depending on the strength of the reader and the types of protections applied to the data, may be readable, which, depending on the application and configuration, may expose personal data to others.

Mobile devices, whether through the GPS installed in the device or through the use of sophisticated software on the devices (or both), can supply valuable information about an individual’s whereabouts and movements, allowing for individualised and tailored services, and targeted marketing. If data from various sources such as from mobile devices, RFID-enabled transportation cards, smart passes for highways, video surveillance cameras and other sources of location data is combined, a comprehensive recording of an individual’s location over time could be created. The benefits to individuals, for example, of being able to access a global positioning system on a device are, for some, appealing. At the same time, individuals’ whereabouts and habits could become increasingly available. This may have significant benefits from a safety perspective; it also has significant privacy implications if conclusions are drawn about their preferences, activities, or associations, which may in turn lead to decisions being made about them, without their knowledge or agreement.

*The human body as information*

Advances in genetic technology have important implications for the health of individuals, helping researchers better understand, prevent and treat various diseases. Genetic testing to assess health risks or to determine biological relationships raises issues that affect not only an individual's privacy but also raise the issue of 'group privacy', as our genetic makeup is shared by other members of our family and community. At the same time the indelible nature of genetic information and its potential implications for discriminatory treatment make it particularly sensitive.

Commonly viewed as a means of identification and authentication, biometrical information is beginning to be collected and used in a greater variety of contexts – from voice recognition systems for allowing employees to access business applications<sup>37</sup> to digital fingerprinting to pay for lunch at an elementary school.<sup>38</sup> As technology advances, the use of additional human characteristics as information will continue to pose challenges to notions of privacy and dignity. The reliability of biometric information and systems has improved, and biometrics are generally considered strong and valuable to authentication systems. The question of whether biometrics invades privacy or protects it, or both, as well as the appropriateness of relying on biometrics to resolve problems or make decisions about individuals, will be issues that will need to be considered as biometric technologies evolve.

*Global data flows*

In the 1970s, transborder transfers of computerised data, including personal data, became more common. Airline and ferry boat reservation systems, co-ordination between tax authorities, money transfers, payroll processing, circulation of periodicals, mail orders, credit cards, insurance transactions, and hotel bookings are a few examples of the types of transborder data transfers from that era. The early OECD discussions of transborder data transmissions suggested that their scope and volume were rapidly growing, but there was little systematic research regarding such transfers.<sup>39</sup>

Although better data on global data flows is still needed, it has nevertheless become clear that the situation is markedly different today than in the late 1970s. Data transfers have become data flows, and data can now be accessed from any location. Recent technological developments have radically altered current data flows. In examining international data transfers that occur today, three main changes can be noted: change in scale, change in processing and a change in management.<sup>40</sup> The effect of these changes on the practices of organisations and individuals is discussed further in sections 2.3 and 2.4.

The role of the individual in these flows has also evolved. Whereas in the past, data transfers tended to be business-to-business or government-to-government, changes in technology and practices have increased the scale of those transactions, and have fostered new business-to-consumer, government-to-consumer, and even consumer-to-consumer relationships. Individuals going about their day-to-day activities online (for example, using search engines, chatting with friends, doing their banking or making purchases) may routinely, and often unknowingly, generate transborder data flows. Organisations offer storage and processing services at a distance to individuals, migrating e-mail, pictures, videos, and documents away from the personal computer and to third-party servers. This allows individuals to have convenient access anywhere in the world where there is Internet access. Some individuals may not have a clear idea of where data is stored beyond their computer. Some of the challenges of disparate data locations are further explored in below.

### *Changes in organisational practices*

New technological capabilities and other innovations have brought about changes in how organisations operate, helping them to increase their efficiency, improve user convenience, and introduce new products. The ability to engage other parties, in other parts of the world, in the delivery of a product or service can make an organisation more flexible and efficient. Practices vary from storing data in different jurisdictions via the “cloud” to outsourcing certain activities to organisations around the world.<sup>41</sup> New technologies have also fostered the creation of different kinds of activities and new kinds of data. For some organisations, the very use of personal data – whether for sale to third parties, advertising, or for tailoring their own services – is a core element of their business model.

### *Changing business models*

With new technologies have come new business models. Today, data transmissions “occur as part of a networked series of processes made to deliver a business result,” in contrast with data transfers that in the past were limited, finalised in advance, involving centralised databases, and occurring at a predictable moment.<sup>42</sup> Electronic international data transfers in areas such as human resources, financial services, education, e-commerce, public safety, and health research are now an integral part of the global economy.

The provision of computing resources at a distance, for example, over the Internet, allows organisations and individuals to access services remotely although their data may be stored anywhere in the world. Data transfers are nearly instantaneous, virtually cost-free, and can occur with the click of a

button, moving data quickly and easily around the globe. As a result, organisations can increasingly determine that certain processes or parts of processes can be handled externally. Indeed, ICTs enable organisations to take advantage of assistance and expertise in multiple locations around the world, thereby meeting customer expectations of improved (and near-instant) service and meeting management demands for increased productivity. An example of this is the “follow the sun” model, which is often used for help desk operations; it ensures that service can be provided to customers at any time of the day, wherever they are located.

The overall result is that organisations have greater flexibility, reduced costs, greater storage capabilities, more mobility, and physical security.<sup>43</sup> Such an approach is not just available to large, multinational organisations. Increasingly, small and medium-sized organisations as well as individuals, are able to take advantage of these global services. The other result, from a personal data protection perspective, is that global data flows are often handled through complex arrangements involving a network of data controllers (namely, those who keep, control, or use personal data) and subcontractors and service providers operating globally.

New business models built on personal data are on the rise. Technology has enabled individuals to share personal data more easily (and readily) and organisations that provide platforms for user-generated content, typically at no charge, seek ways to generate revenue, often using personal data to do so. Even the individual posting such content can derive revenue from his or her postings. The rise of targeted or behavioural advertising – the tracking of an individual’s activities online, over time, in order to deliver advertising that is targeted to the individual’s interests – reflects the need for organisations to find ways to support their businesses and/or their ability to offer services to individuals without direct charge. In 2008, online advertising was worth more than USD 55 billion worldwide, or 10% of global advertising revenue.<sup>44</sup> Falling computer costs, as well as falling processing costs, increased processing speed and capacity, combined with increasingly sophisticated aggregation and analytical tools also allow organisations to extract greater value from data. Profiling, behavioural targeting, and audience segmentation can occur on a much larger and more advanced scale. There may be other uses for the data, besides advertising, that have not yet been fully realised. For example, there has been recent growth in aggregating and analysing personal data to report on natural disasters and to predict health risks. The extent to which these uses rely on information about identifiable individuals and the extent to which their privacy is at risk continue to be a matter of debate (see section 4.1).

*Changes in the public sector*

Public sector bodies are taking advantage of the technological changes to accomplish their mandates or improve their ability to deliver public services through more effective processing of personal data. Citizens increasingly look to the Internet to obtain information about government services and operations.<sup>45</sup> The public sector is also beginning to change how it uses the Internet to inform and engage the public and in so doing, has the potential to collect personal data via this medium. Some governments are using social media to engage the public. For example, a number of privacy enforcement authorities and government agencies maintain a presence on popular sites like Facebook, use Twitter, seek input into public policy, and they blog.<sup>46</sup>

More generally, there is increasing concern in some quarters that personal data collected in one context may be used in other contexts. Information collected by the private sector for a business purpose may be requested or obtained through compulsory processes provided certain burdens are met by the public sector (if permitted by law), or the private sector may be required by the public sector to collect and retain personal data for public policy purposes, such as revenue collection, law enforcement, public safety, public interest, and national security. Such data sharing occurs across a range of economic and social activities that includes hospitality, communications, health, retail, entertainment and financial services. This continues to be an area of considerable debate as the public sector seeks information collected by the private sector in the conduct of business.

*Changes in individuals' practices*

With increased connectivity of individuals to the Internet, more people are conducting business transactions online, including shopping, banking, and travel arrangements. In OECD countries, the number of adult consumers purchasing goods and services over the Internet is rising, from an average of 26.9% in 2004 to 35% in 2008.<sup>47</sup> In terms of goods, a Nielsen survey noted that, in 2007, the most popular purchases over the Internet worldwide were books, clothing, videos, DVDs, games, airline tickets and electronic equipment.<sup>48</sup> In the United States, by the third quarter of 2009, 3.6% of all retail commerce was done online.<sup>49</sup> In making these transactions, increased amounts of personal data are being shared online with organisations.

However, it is another, more recent change that is having a very significant effect on privacy and one which was not foreseen when the OECD Guidelines were developed and adopted. The development of simple yet powerful applications for individuals to create and share information – often personal data about themselves or their friends and family – is a key aspect of the “Web 2.0” phenomenon.

Internet users worldwide are using new tools and services and changing their behaviour online. Personal data is often volunteered by individuals, rather than directly requested and collected by organisations. Large numbers of individuals are now blogging, posting pictures and videos online, conducting business transactions among themselves, and interacting with large groups of friends or the public through social networking sites. According to the photograph and video sharing web site, Flickr, four billion photographs had been posted to the site as of October 2009.<sup>50</sup> Facebook states that it has approximately 500 million users, with 50% of its active users logging on in any given day.<sup>51</sup> With the move from fixed-lines to mobile phones to smart phones, individuals are increasingly connected all the time and taking advantage of expanding opportunities to convey their location and related data to other individuals and third parties. And individuals are not only posting personal data about themselves; they are also disseminating information about others (sometimes without the other person's consent). This behaviour may challenge assumptions on which some privacy concepts, such as that of data controller, are predicated (for example, that only organisations or governments engage in personal data sharing).

Young people are active participants in the trend of posting data about themselves and others. Some suggest that there has been a shift in attitudes towards self-disclosure, particularly among “digital natives” (those born after the Internet became a phenomenon), who may be more likely to live their personal lives online, while others contend that young people do care about privacy. Behaviours are likely to be influenced in part by the types of platforms and settings made available for social networking and other new media. While ideas about privacy may be changing, there are many examples of “consumer backlash” when companies are perceived to have pushed too far. Media stories concerning online privacy abound. Privacy clearly remains a concern for many individuals, businesses and governments; whether there is any substantial change in attitudes towards privacy is an area that needs further exploration.

Although individuals are more active participants in personal data flows, many users may not fully appreciate the way their information is processed and the associated privacy implications. Research in the field of behavioural economics, which builds on research into decision-making, may provide worthwhile insight into how individuals make choices in relation to disclosing data and protecting privacy. Difficulties in selecting from a large array of options, a growing inability to calculate and compare the risks and benefits, and the tendency to focus on more immediate effects contribute to an environment in which individuals generally concerned about their privacy may not always act in ways to protect it.<sup>52</sup> The challenges that these tendencies present to traditional approaches to privacy protection are explored further in section 4.2.

Some individuals have, however, adopted various strategies to manage their online identities or to protect their privacy. Some use multiple identities on the Internet, some of which are self-created, while others are provided to them. Individuals may also use a complex mix of interrelated “partial” identities with varying levels of accurate personal data. It is possible that decisions about individuals’ identity could be made based on misinformation. Depending on the use of this data, the consequences for the individual may range from the serious (job loss, for example) to less consequential (less-than-accurate targeted advertising). The implications for organisations are that a potentially valuable employee was not hired or advertising money was not well spent.

The social nature of the Internet and related networking technologies is raising interesting issues. This is new territory for society. The ‘mediated public’ space of social networking services has certain characteristics that make it different from how we have communicated with others in the past: namely, the persistence, searchability, replicability of data and the invisibility of the audience on the web.<sup>53</sup> The opportunities from tapping into such data-rich resources are enormous; the consequences of this mix of public and private space may continue to prove challenging for individuals, organisations and data protection authorities.

### **Privacy risks in the evolving environment**

The dramatic opportunities enabled by changes in technologies and global flows have also raised new challenges and concerns for individuals, organisations, and society with respect to the protection of privacy. There is a general perception that certain risks associated with privacy have increased as a result of the shift in scale and volume of personal data flows and the ability to store data indefinitely. These changes, along with the evolving role of individuals and the increasing economic value of personal data, give rise to concerns related to the security of personal data, unanticipated uses, monitoring and trust. The result is a privacy environment that is challenging for organisations and individuals to navigate.

#### ***Security***

Given its economic value, organisations often retain large amounts of personal data for various purposes. In recent years, high-profile “data breaches” have shone a light on the challenges of safeguarding personal data. Personal data is valuable not only to governments, legitimate organisations, and individuals; it is valuable to criminal elements as well. The consequences for individuals from the misuse of their personal data, whether

accidentally lost, leaked or purposefully stolen, are significant. As a result of this environment, the security of personal data has become an issue of concern to governments, businesses and citizens.

#### *Internal factors*

Generally speaking, a “data breach” is a loss, unauthorised access to or disclosure of personal data as a result of a failure of the organisation to effectively safeguard the data. Organisations have long been collecting personal data in one form or another for various purposes. To some degree, personal data has always been at risk, regardless of the form in which it is retained. Privacy breaches involving paper records, for example, continue to occur. However, the sheer volume of personal data being transferred over public networks and retained by organisations has changed the risk profile, potentially exposing larger quantities of data in a single breach.

Data breaches are frequently the result of internal factors, such as errors or deliberate malicious activity on the part of employees,<sup>54</sup> as well as errors or malicious activity on the part of third parties that are involved in processing personal data on behalf of organisations. Twenty-five million child benefit records held on an electronic device that disappeared as a result of a series of employee errors is but one example of a type of breach that is increasingly familiar.<sup>55</sup> A lack of employee training and awareness, inadequate processes and security rules around personal data and equipment, over-collection of data and undefined retention periods, and/or a lack of adequate oversight are some of the factors that often lead to breaches.

The potential harm, including the risk of identity theft, to individuals from the misuse of their personal data is significant. The potential harm to organisations from breaches is also considerable. There is a substantial financial cost in recovering from the breach and fixing problems within the organisation to prevent a recurrence. Organisations may be subject to legal actions, including private actions or fines levied by various authorities, where allowed. There are also costs to the organisation’s reputation. A loss of trust or confidence can have serious financial consequences on organisations.<sup>56</sup>

#### *External factors*

Personal data is also at risk of intrusion from outside sources, and organisations are not the only vulnerable party; individuals’ home computers and other devices are also at risk. Data is increasingly under threat from criminals, able to make fraudulent use of identity information gained through phishing or malicious spam, and more generally, techniques called malware (short for malicious software).



Malware has become a critical threat to the security of all who use the Internet – whether large organisations or individuals. Estimates indicate that there are tens of millions of compromised machines.<sup>57</sup> Often control of these computers is gained by infecting them with viruses. By one estimate, the total number of active bots (as in, highly aggressive bots that are attacking a number of computers) is approximately five million worldwide.<sup>58</sup> While criminal activity is at the root of such attacks, other parties, such as internet service providers, e-commerce companies, and users, have an influence on the effects of malware through the actions they take (or do not take). Strategies to mitigate the threat are evolving. The illicit use of personal data is more than a security issue. It raises questions of trust, applicable law, and the need for co-operation amongst law enforcement and privacy enforcement authorities, as well as private sector organisations, and highlights the reality that data protection laws were not intended to deal with such criminal uses of personal data.

### *Unanticipated uses of personal data*

The ability to store data indefinitely and strides in analytics present enormous potential for using personal data for other purposes, possibly bringing significant economic or social benefits to both individuals and organisations. However, using personal data in ways that neither the organisation nor the individual anticipated when the data was collected can also contribute to the perception that privacy is at risk.

Analysing the digital trails left by individuals, by mining information about preferences, interests, behaviours, or buying patterns expressed on social networking sites, to cite but one example, represents a source of revenue for some organisations that provide services at no direct fee to Internet users. Health research is another area in which data collected for a particular purpose may later be used for other purposes not anticipated at the time of collection (possibly as a result of technological advances or breakthroughs in other areas). A recent example of an unanticipated use of personal data with a positive outcome involved the U.S. Centers for Disease Control and Prevention tracing a salmonella strain to its source because patients had used a “frequent shopper” card when buying groceries. In this instance, patients’ permission was obtained, the information accessed, and the source of the outbreak was more easily located.

Some individuals may welcome some unanticipated uses of personal data, while others may not. Some unanticipated uses of personal data may be reconcilable with the original purposes for collection and use, whereas others may not be. Given technological developments and new business models, it is generally not possible to know or anticipate all the potential future uses of data at the time of collection. Given that data could live

“forever”, some possible uses are unknown when consent is obtained and some of these future uses may not compromise privacy. Limiting uses of personal data may be perceived by some organisations as a barrier to the flow of personal data and the economic benefits that come from using that data. As businesses try to maximise the value of the information they hold, there is a risk of conflict with the expectations of individuals about how their data can or should be stored or used, with the possible result that individuals may not want to interact with that organisation.

Generally, individuals want to know about and be able to choose whether to consent to new, unrelated uses, and data protection regimes typically require this (subject to some exceptions to consent). Obtaining consent, either in terms of the permission organisations obtained initially or in going back to individuals to obtain consent for new purposes, presents risks. Many purposes for collecting personal data may be difficult to explain and equally difficult to understand. If the initial consent language is overly broad to take into account any potential uses of personal data, individuals may not know or understand what could happen to their personal data, and any consent they provide is arguably less than informed. Consequently, their trust in the organisation may be placed at risk. Returning to individuals to obtain consent may, in some instances, also risk the trust of the individual depending on how often consent is requested and what the new uses are. Privacy policies that are revised frequently to reflect rapidly changing uses risk confusing individuals and potentially making them wary of the organisation's practices.

New uses of personal data can also create more personal data. Collecting increasing amounts of personal data can create security challenges for organisations, as more personal data is potentially at risk of privacy breaches. Unanticipated uses of personal data may also present a risk that the organisation is not being fully transparent about their practices, or is not limiting or obtaining new consent to their uses of personal data. On the other hand, being overly restrictive may limit innovation that could bring social or economic benefits or may limit the growth in revenues of certain organisations. While there is a risk that personal data could be misused, there is also a risk that valuable benefits from new uses of personal data might be lost.

### ***Monitoring***

Monitoring of individuals is on the rise. Developing a better understanding of individuals for social benefit purposes or for commercial purposes is one motivation for monitoring individuals. While monitoring may be conducted for legitimate purposes, there is always a risk that such activities may be perceived as excessive. There is also the risk that, in some instances,

monitoring may not be used legally. The examples discussed in this section are intended to provide an overview of the types of monitoring in existence. They are not intended to suggest that they are necessarily inappropriate.

Types of monitoring systems include closed circuit television cameras (CCTV), which have been widely in use for some time. Some examples of where CCTV systems have been put in place include banks, shopping malls, airports, train stations, subways, apartment building corridors, and parking lots. Global Positioning Systems on mobile phones and in vehicles can be used to monitor an individual's whereabouts.

These examples are of systems whose primary purpose is to monitor. However, monitoring can often be a by-product of some other service or technology, where data is collected and stored for other reasons, and then later analysed and used for a monitoring purpose (and may be considered an unanticipated use, as described in section 3.2). Deep packet inspection, ostensibly used for managing internet traffic, has the potential to be used for tracking individuals for advertising purposes, for example, because it has the ability to "look into" the content of messages sent over the Internet. Cookies placed on computers to help web sites "remember" the visitor in order to provide better, streamlined service for the individual may also be useful for tracking and targeting audiences to serve advertisements.<sup>59</sup> Sensors in homes, used for monitoring power usage, is another example of a system that may be highly useful for helping to manage power grids and very beneficial to the environment, but also can have privacy implications through the same monitoring capabilities.<sup>60</sup> The use of loyalty cards by individuals to obtain discounts or special offers also records an individual's spending habits. The combination of various types of technology (i.e. information from surveillance cameras, GPS, databases) can provide for more consistent and comprehensive monitoring of individuals.<sup>61</sup>

Some employers monitor employees' use of websites and proprietary equipment to protect against litigation, illegal intrusions, to utilise limited bandwidth more effectively, to ensure employee productivity,<sup>62</sup> and to protect customer information. In the private sector, according to one survey, 66% of U.S. employers monitor employees' Internet usage on company computers, and 65% use software to block connections to inappropriate web sites – up 27% from 2001. Monitoring takes various forms, from tracking keystrokes to monitoring blogs to see what is written about the company. There is no reason to believe that U.S. employers are exceptional in this regard.

Increased monitoring results in increased information collection and storage that may be vulnerable to breaches or misuse. It may also contribute to a sense that the individual's private space is shrinking, and there is concern

that monitoring can lead to illegal discrimination against individuals. While monitoring may contribute to a sense of security, improved efficiency may provide economic or social benefits for some, for others it may cause a decline in trust and freedom.

### *Trust*

In simple terms, trust means having faith or confidence in something or someone. It is at the core of the relationship between business and customer, government and citizen. With the rapid evolution of technology, trust remains critical. If individuals and organisations are to take advantage of the benefits arising from technological developments, they must have confidence in their reliability and safety. All of the issues noted above address the question of trust in these relationships: if individuals believe that data about them is held securely and collected for the stated purposes, if they are comfortable relying on organisations to inform them of, and seek consent for, new uses of their personal data, if they feel that any surveillance of them is for appropriate reasons and they are aware of it, then trust is strengthened.

However, if those conditions are not met, then trust can be undermined. For example, there is a risk that ID theft and high-profile data breaches may result in a loss of trust, particularly when they involve activities like e-banking and e-health that rely on sensitive information. Organisations are focussing on risks to their reputations from actual privacy incidents but certain practices involving data aggregation, processing and mining, for example, can also undermine trust if they occur without users being aware. Trust can be eroded if organisations frequently change their privacy policies to allow for increasingly broader uses of personal data. If users sense that they do not understand or lack control of an organisation's use of their personal data, they may reconsider their relationship with that organisation. Education and awareness of actual risks and potential solutions are important for individuals to make informed decisions.

Maintaining trust (or restoring it after a breach) is vital to organisations. Careful attention to transparency, accountability, security, purpose limitations, and accessibility will help. Enforcement of data privacy laws is another means of reinforcing trust (including remedies). Questions remain, however, as to the best combination of policies and tools to protect privacy and preserve (or restore) trust in this evolving landscape.

### Considerations and challenges to existing privacy approaches

Are changes in technology, business models, and the role of the individual challenging the effective application of traditional core privacy concepts? There is a concern among some observers that privacy principles are being tested on many fronts and that the approaches taken to date may not be sufficient to respond to future challenges. That many key players are currently pausing to assess the situation may be symptomatic of a need to understand if and where the core privacy principles are being stretched.

Examples of such developments include the European Commission's launch in July 2009, of the Consultation on the legal framework for the fundamental right to protection of personal data, which is specifically examining the challenges to data protection, in light of globalisation and new technologies. In late 2009, the Federal Trade Commission launched its privacy roundtables to explore the privacy challenges posed by 21st century technology and business practices that collect and use consumer data, and how best to protect consumer privacy while balancing the beneficial uses of such information. Perhaps ahead of others, in 2006, the Australian Law Reform Commission launched an inquiry into whether Australia's data protection legislation provided adequate protection given changes in technology and possible changes in attitudes towards privacy. New Zealand's Law Commission is also conducting a privacy law review, in part to review social, technological and international developments that may have an impact on privacy in New Zealand.<sup>63</sup> In 2010, Canada's Office of the Privacy Commissioner undertook consultations on new technologies and their implications on privacy protection, in advance of an upcoming mandated review of its private-sector privacy law.

In addition to reflecting on the robustness of the core privacy principles, there is an increasing concern that the long-standing territorial/regional approaches to data protection may no longer be sufficient as the world increasingly moves online and data is available everywhere, at any time.

#### *Scope of privacy protections*

Distinguishing between what is "personal data" and what is not is becoming gradually more difficult. Technological progress increasingly permits data to be linked back to identifiable individuals in ways not anticipated when the data was collected. And technological progress is also making it easier, faster, and more affordable to do so. Data can be combined with other data and in the process may make individuals identifiable – sometimes to a high degree of statistical probability. For example, although currently there is some debate about whether IP addresses are personal data,

there is an argument to be made in favour of considering it personal data in certain contexts when it is possible to identify an individual by linking an IP address to other information, such as web searches. Information garnered by web searches can also reveal very sensitive information about an individual's practices, preferences and beliefs. The volume of next generation IP addresses, IPv6, will allow greater use of static IP addresses, thereby potentially increasing the ease with which individuals can be identified.

How apparently disparate pieces of data can be linked to identifiable individuals has been illustrated in a number of relatively recent high-profile instances where “anonymised” databases were released publicly and researchers were able to link the data back to individuals by combining the anonymised data with information contained in other databases.<sup>64</sup> Such developments are posing challenges to privacy approaches, as increasing amounts and categories of data are brought within the scope of various privacy regimes, and the workability of the key protections provided by the privacy principles is tested. Questions around obtaining consent, transparency, data quality, access and safeguards are some of the key data protection principles that are being increasingly challenged in this regard. Furthermore, if any data has the potential to be personal data when combined with other data – and therefore subject to privacy regimes – the impact on the availability of data for a number of activities that have traditionally relied on anonymised data may need to be considered.

The perceived impermeability of anonymised data has historically provided an easy solution to privacy concerns raised with respect to various spheres of activity, such as health research. However, efforts to protect personal data through anonymisation may instead be placing that same data at risk. If apparently “anonymised” data can be relatively easily “re-anonymised” in some cases, data protection requirements could then come into play. In areas such as health research, this could pose challenges (particularly around obtaining consent). Valuable social and economic benefits from such data flows may be placed at risk.<sup>65</sup> The practical limits of pseudonymisation and anonymisation are clearly being tested, and such limits may have implications for identity management strategies that facilitate anonymity and pseudonymity. There is the possibility that identities with different degrees of pseudonymity or that contain varying sets of attributes may allow others to discover the individual's identity. This may place free expression, safety, and free association at risk.<sup>66</sup>

The concept of “data controller” is also under scrutiny.<sup>67</sup> Given the large number of actors in the global value network (including individuals), roles and responsibilities are becoming blurred, and consideration needs to be given to how well adapted the notion of the data controller is to today's environment.

Given the relatively static data transfers and comparatively simple business models and relationships in place when data protection principles were first being drawn up, the concept of data controller did not contemplate scenarios where many players could be considered data controllers. Increasingly complex business models and relationships, as well as new technologies, can make it challenging to determine who the data controller is and therefore who is responsible for protecting the personal data. Subcontracting, outsourcing, evolving partnerships between organisations in value chains, behavioural advertising, and other emerging business models can add layers of complexity in determining responsibilities and identifying roles. Often an entity can be a controller related to one use of information and a co-controller, processor or sub-processor for another.

Another example of new business models and new technologies that challenge the clear determination of data controllership concerns online platforms that can be accessed by third parties to develop applications, using personal data. While this may foster innovation and economic growth, the issue of which party is accountable for protecting the personal data of the users is one of serious concern to many observers, users, and privacy regulators.<sup>68</sup> In this context, individuals in a possibly non-commercial capacity may be acting as controllers and processors by developing applications, creating content or disseminating information. Another example of the changing nature of the data controller concerns RFID technologies. Does a retailer that sells goods with RFID chips embedded in them, but not enabled, bear any responsibility as a data controller?

The concept of data controller also did not necessarily contemplate the possibility of individuals acting in a manner similar to data controllers with respect to the personal data of others, a development that has been triggered by the emergence of Web 2.0. User-generated and crowd-sourced content raise issues around responsibility and liability. For example, videos that individuals post online about themselves can be reposted by others and even manipulated without the individual knowing about it. Making posts on social networking sites that refer to third parties or posting photographs of others are a few of the examples where individuals disclose the personal data of other parties, often without their knowledge or consent. The consequences to the individual in terms of reputation and future education and employment prospects can be significant. Many privacy laws do not apply to the use of personal data by individuals in a personal or domestic capacity, and the individual may be left largely unaccountable for his or her actions. Given the key role that individuals play in transmitting personal data, education and awareness activities may be required to help them better understand the risks involved in posting information about themselves and others online, and further consideration may need to be given to their role in privacy protection frameworks.

Given the increasing complexity of interactions between certain types of technology and certain business models, the concept of data controller and processor as currently used may not accurately reflect the continuum of roles and responsibilities that new business models contemplate. Further consideration of how these concepts are used may be needed in order to ensure that responsibilities are properly addressed and allocated.

### *Role of transparency, purpose and consent*

The individual is an active player in personal data flows, and technology and business models are presenting new kinds of uses of personal data. Privacy principles have given weight to the importance of individual control in privacy protection but questions can be asked about whether such emphasis is providing the best protection.

OECD's *Consumer Policy Toolkit* devotes some attention to the role that behavioural economics may play in individuals' choices and the implications that this may have for organisations and policy makers in terms of information provided to consumers to help them make choices. This work may also prove instructive in the area of privacy protection. As noted in the Toolkit,

Behavioural research has shown that how information is presented, or framed, can have dramatic effects on how consumers respond to that information, so policymakers must use care when designing disclosures if they want to achieve certain results.<sup>69</sup>

Individuals tend to rely on "rules of thumb" when making decisions, a tendency that may lead them to ignore certain options or simply not make a choice. They also present inconsistencies when weighing probabilities, and may appear to place more value on the present than on the future. In turn, such behaviours affect how information is absorbed. More information for individuals about an organisation's privacy practices and personal data usage may not always be better. How choices are presented to individuals also appears to play a role in how choices are made. This has implications for default settings on web sites, for example. If they are overwhelmed by choices or complex information, individuals will tend to choose what is presented to them. Providing information that is understandable is a key component of transparency.

Given this, common approaches to notification and consent may not be providing the privacy protection originally intended. As data usage has become more complex, so too have the privacy policies that describe them. Many organisations tend to rely on these as a basis for consent, but given the implications about how individuals make decisions, questions can be asked about whether this focus on privacy notices and consent can continue to bear



the weight they are often assigned in the process of affording protection. Do they allocate too much risk to the consenting individual, who rarely reads the information or understands it if they do? Alternatively, we may also need to consider whether an overly rigid interpretation of the concept of consent, in other words, one which assumes that explicit and specific consent is required for each and every transfer of information necessary to fulfil the original purpose of the transaction, runs the risk of being used to weaken the control which many privacy laws specifically aim to give individuals.

There is also the issue of the extent to which individuals have meaningful choices about what information they disclose. Typically, individuals cannot use a service unless they agree to the terms of use, which, in addition to being complex or legalistic, frequently present a “take it or leave it” approach. Under such an approach the user must agree to provide personal data for all of the purposes the organisation represents – even if some are not directly related to the service – in order to access the service. This substantially limits the ability of the individual to protect their personal data by giving meaningful consent. Generally, the emphasis on consent based on overly complex privacy policies that provide few real options and few limitations on collection and use diminish the effectiveness of privacy protections that are intended to support the individual’s role in controlling his or her own personal data.

#### *Access and correction*

Equally challenging to the notion of individual control is access and correction in the digital age. The dynamic “information life cycle” that characterises the collection, storage, use, and disclosure of personal data online is posing a challenge to the exercise of rights related to access, correction and erasure in a practical way. For example, how does one exercise his or her right to access personal data from a mapping site where images of streets were taken and the individual may have appeared in them? Or, if an individual wanted to know how and why a particular advertisement was served to them while they were surfing the Internet, how would they go about finding out? Who would they ask? Organisations may also find it challenging to explain the provenance of the data (although work in this area is being undertaken to address this issue – see section 5). When individuals create their own profiles on social networking sites, the ability to obtain access and make corrections may be obvious. But it is often not obvious how an individual can find out what other information (information that they did not post) may appear about them on the site and other locations. Rapid dissemination, indexing, caching and mirroring of data also pose problems for individuals seeking to correct personal data (or have it removed). The Guidelines do not contain a principle that directly relates to retention or disposal, and it is now more costly to delete data than to retain it.

Given the increasing reliance on various transactional data for automated risk management and profiling, the need for accuracy and the ability to correct information is likely even greater now than in the past. Organisations may also find it challenging to authenticate individuals who request access, correction or erasure, when the individual has had no prior relationship with the organisation.

### *National and regional approaches*

Global flows of personal data are testing the territorial approach to data protection. When organisations operate internationally, individuals can connect to the Internet from anywhere in the world, and data stored in the “cloud” can be backed up in multiple locations (locations only made known to the cloud storage operator), questions of jurisdiction and oversight become complex, and there may be little certainty about the answers among organisations and privacy regulators. Safeguarding the personal data of individuals is needed regardless of where it is located but ensuring that that happens is not a simple matter. Would more consistent rules bring economic benefits in terms of jobs and growth and still provide appropriate protection to personal data wherever it is? Does the problem rest with the diversity of rules, the diversity of methods for ensuring compliance or a lack of understanding of national laws? The need to address these global governance issues has become increasingly acute as the gap widens between a territorial approach to regulation and the movement of data processing around the world.

The current patchwork of national or regional oversight does not, arguably, provide the protection of personal data that individuals may expect in a global economy. Some non-OECD member countries do not have privacy protection regimes or model codes. Among those that do, many of those regimes contain cross-border prohibitions.<sup>70</sup> Even among OECD member countries, there are variations. As detailed in section 1.3, countries and regions have chosen different approaches to protecting data and have expressed differing degrees of concern about barriers to cross-border data flows. These differences have presented various compliance challenges.

While it would appear that a globally agreed-upon set of standards, with global enforcement, could present the kind of privacy protection individuals expect while enabling the free flow of data, this approach is not without its challenges. Indeed, an international approach is not a new idea as it was part of the reason for developing the OECD Guidelines over 30 years ago.

The recent report on the “Future of Privacy” by the European Union’s Article 29 Data Protection Working Party/Working Party on Police and Justice recognises the challenges posed by globalisation of data flows and

different privacy regimes. It makes a number of suggestions as to how data protection can be ensured wherever it is processed, highlighting the need for international global standards and international agreements.<sup>71</sup> Other regions, for example, APEC, are also recognising the challenges that the global nature of data flows have on protecting personal data and are interested in finding common approaches to privacy protection. While recognition for the need for a common, global approach is growing, multiple regional approaches may pose further challenges in terms of their workability. Diverse cultural and legal traditions add to the complexity of finding a solution.

In addition to seeking a global standard, consideration needs to be given to ways to improve current co-ordination among the increasing number of regional and international fora for addressing privacy issues and enhancing multi-stakeholder participation. Recent efforts to improve cross-border enforcement co-operation are a step in the right direction. These are discussed in section 5.2, as well as in the OECD Report on Cross-border Privacy Enforcement Co-operation. There may be parallels with other efforts at global legal co-operation that could provide lessons for cohesive privacy protection.

Minimising differences is significant as organisations operating globally may not always be able, or willing, to tailor their service offerings to meet the specific needs of smaller jurisdictions. Individuals expect privacy protection wherever they are. The issue of reducing global compliance challenges facing businesses while ensuring more effective data privacy protection remains at the forefront even today, some 30 years after the first internationally agreed set of privacy principles were adopted.

### **Evolution and innovation in privacy governance**

Although the fundamental principles of the Guidelines have remained unchanged over 30 years, there have been many innovative responses to the changing environment. The discussion below is not intended to be an exhaustive list of the various developments that have arisen over the years. The following review also does not attempt, for example, to outline the changes in governance, oversight or enforcement mechanisms over the past 30 years. Those mechanisms were extensively covered in the 2006 OECD *Report on Cross-Border Enforcement of Privacy Laws*.<sup>72</sup> Rather, the following is a selection of key innovations in data protection since 1980.

*Legislation that focuses on data security*

Particular types of privacy problems have elicited special attention in recent years. Numerous countries (and in the United States and Canada, individual states and some provinces) have passed or are about to enact breach notification laws that would require organisations to inform individuals or authorities when a breach of security has led to a disclosure of their personal data. Many nations have also passed (or are about to pass) anti-spam legislation, often based on OECD guidance on combating spam,<sup>73</sup> which can be viewed as supplementary data protection legislation.

*Information management/privacy by design*

While there has been some evolution in the substantive rules governing privacy practices in recent years, the most dramatic initiatives and changes have emerged on the more practical aspects of implementing data privacy protections. Some initiatives involve the use of technical measures to protect privacy, some involve managing the lifecycle of personal data, while still others focus on global data transfers.

Although the Guidelines address security concerns, the environment was considerably different at the time of their development – before the Internet, unprecedented global data flows, and the arrival of the open and underground markets in personal data. Threats did not require the extensive evaluation that today's environment demands. In 1992, the OECD *Guidelines for the Security of Information Systems and Networks* were developed to provide more detail concerning required security practices. Today, privacy impact assessments (PIAs) are helping organisations analyse the “life cycle” of personal data and take privacy into account before introducing new technologies or programmes. Such efforts can be seen as part of an overall privacy management framework and are an integral part of a mature security risk assessment. This has meant a new focus on information security that recognises that personal data is an asset that requires sustained protection. This transformation of the risk assessment and recognition of the parties potentially harmed from threats to information systems are very significant developments, and, in several countries, are largely a result of data breaches and the consequences that follow under data breach notification laws (i.e. fines, the costs of providing notice to affected individuals, and reputational harm).

Privacy impact assessments (PIAs) evolved in the 1990s as a means of systematically assessing risk in order to anticipate and mitigate privacy problems. Where they are commonplace, they are used typically by the public sector when introducing electronic initiatives<sup>74</sup> although the private sector may also use them. Some pieces of legislation require organisations to

conduct PIAs. For example, the US *E-Government Act of 2002* mandates PIAs<sup>75</sup> for all federal IT systems that hold personally identifiable information, and Alberta's *Health Information Act*, requires that a PIA be carried out under certain circumstances.<sup>76</sup> Similarly, the European Commission recommendation on Radio Frequency Identification (RFID) requires operators to conduct an assessment of the implications of an RFID application implementation for the protection of personal data and privacy, including whether the application could be used to monitor an individual.<sup>77</sup> Implemented as a tool for accountability, they can help organisations develop a “culture of privacy,” build trust and assist with legal compliance, among other benefits.<sup>78</sup> They promote cohesion between privacy and security communities within the organisation. They can also minimise costs in the longer term since fixing privacy problems after the fact can be very costly for organisations.

Some organisations have external verifications or audits conducted on their privacy practices. Some also conduct audits on any third parties that are involved in data processing on behalf of the organisation.

Leveraging technology to enhance privacy has been recognised as a valuable approach in recent years. The concept of Privacy Enhancing Technologies (PETs) gained ground in the 1990s, and the European Commission held a symposium on the issue in 2003 and 2009. “Privacy by design” is a concept in which privacy is a default design objective in any IT system or business practice.<sup>79</sup> Following this paradigm, technologies, processes, and practices to protect privacy are built into the system architecture and not added on later as an afterthought. In this way personal data is managed throughout its life cycle. One of the goals is to be transparent to users and providers and to incorporate the elements of “fair information practices” into the system’s architecture.<sup>80</sup> Some of the challenges in helping individuals remain in control of their personal data, particularly with respect to providing access to and enabling them to correct their personal data, may be addressed through technical standards and tools. These standards and tools can record and describe the actual lifecycle of personal data collected and held by an organisation (such as, provenance) and may assist organisations’ management of personal data and facilitate accountability.

In an effort to facilitate flows of personal data from one system to another (where appropriate), systems for managing digital identities, and associated personal data, are moving towards greater interoperability. Depending on how they are used, they can offer the potential of giving individuals greater control over their identities and personal data, often increasing the utility of data due to improved accuracy and otherwise enabling innovation.<sup>81</sup> They can also be used to help address the challenge organisations may have in authenticating individuals who request access,

correction or erasure of their personal data. Recognising the important contribution identity management can play to improving privacy and security, the OECD developed a primer on digital identity management.

The concept of a “privacy management framework” is another approach that has developed to help organisations better manage their personal data handling practices. Generally speaking, privacy management frameworks include the policies, procedures, and systems (including considerations of how to optimize technology to enable privacy) that organisations employ to ensure that personal data is properly protected, risks are managed, and privacy legislation is complied with. Such frameworks can incorporate PIAs into an organisation’s risk management and can promote accountability through reporting, audits, education, and performance appraisals.<sup>82</sup> A strategic information management approach is similar. It recognises that information (whether personal or not) is an important business asset. Its goal is to ensure that data is protected appropriately, that laws regulating the data are complied with, and that costs and benefits of particular uses of data are assessed.<sup>83</sup>

As outlined in the OECD *Guidelines for the Security of Information Systems and Networks*, with the Internet supporting critical infrastructures and playing a greater role in business and government transactions, the security of information systems is critical.<sup>84</sup> Governments and organisations have adopted a number of approaches, from passing legislation aimed at fighting cybercrime, to establishing policies, to education. International co-operation has also played a key role in facilitating the sharing of best practices.

There has also been some work on finding innovative, non-technical means of improving transparency for individuals. For example, different types of privacy policy presentations, intended to improve readability of policies by online users are being studied.<sup>85</sup> Efforts have been made to simplify privacy policies (for example, short form policies, video policies), and privacy controls have been presented in the form of dashboards and decision trees. Other efforts include tools to help Internet users access and track the various policies governing the web sites they visit.<sup>86</sup> Some of these new tools may provide a promising path forward in terms of increasing transparency and providing for user control.

### ***Role of accountability***

Accountability is a principle in the OECD Guidelines and has been included in numerous data protection laws. Over the past 30 years, various instruments have evolved which focus on accountability, some of which are detailed below. While the principle is not new, there is growing interest in

how the principle can be better used to promote and define organisational responsibility for privacy protection. The development of better data security practices and more basic considerations of privacy within organisations in response to data breach legislation indicate an evolution in accountability.

In the European Union, organisations are prevented from transferring personal data to jurisdictions outside of the union unless the European Commission has determined that there exists “adequate” legal protection of the data or that adequacy is ensured by other means. One approach that has been developed to meet the adequacy requirement is the EU-US Safe Harbor Framework (“Safe Harbor”). Safe Harbor was developed as a means to help EU organisations comply with the European Directive on Data Protection in order to enable personal data flows to continue to the United States. Organisations in the US that self-certify to Safe Harbor demonstrate to EU data exporters that they provide privacy protection that is deemed adequate by the European Commission. Eligible companies self-certify that they adhere to the Safe Harbor requirements.<sup>87</sup>

Another use of accountability to facilitate cross-border transfers of personal data and protect personal data processed outside of the EU by multinational organisations is Binding Corporate Rules (BCRs). BCRs are codes that protect personal data in such transfers and in order to assert adequacy within the context of EU data protection requirements. A key element of BCRs is that the “binding nature of the rules in practice. . . would imply that the members of the corporate group, as well as each employee within it, will feel compelled to comply.”<sup>88</sup> Companies are required to demonstrate such compliance to the appropriate data protection authorities. This includes, among other things, showing that a policy is in place, employees are aware of it and have been trained appropriately, a person who is responsible for compliance has been appointed, audits are undertaken, a system for handling complaints has been set up, and the organisation is being transparent about the transfer of data. In short, BCRs compel organisations to demonstrate how they are in compliance with all aspects of applicable data protection legislation.

APEC members are developing Cross-Border Privacy Rules (CBPRs), which is a mechanism to implement the principles in the APEC Privacy Framework.<sup>89</sup> Accountability is a key component of CBPRs as they include a role for accountability agents, which may include trustmarks, seals, and other private bodies.

An initiative known as the “Galway Project” (continuing now as the “Paris Project”) has brought together a group of government, business and academic representatives to develop the concept of accountability. As part

of this work, it is examining how accountability can address the protection of cross-border information transfers.<sup>90</sup> The Article 29 Working Party recently issued an opinion on the principle of accountability, proposing that such a principle be added to the EU Directive.<sup>91</sup> This principle aims at strengthening the role of data controllers and increasing their responsibility for compliance. The principle would explicitly require data controllers to implement appropriate and effective measures to put into effect the legal principles and obligations and demonstrate this to the supervisory authority upon request.

Trustmarks have also arisen in recent years as a means of assuring consumers that identified web sites offer privacy protection for its users. For example, a Japanese industry run programme started in 1998, the PrivacyMark System, has issued trustmarks to nearly 12 000 entities in Japan.<sup>92</sup> Generally, in order to obtain a trustmark or seal, an organisation must show that it is adhering to good privacy practices. Although trustmarks have been criticised for, among other things, the variability in privacy standards that they set and their lack of enforcement,<sup>93</sup> in those countries without privacy laws, they may offer an important layer of protection.

#### ***Cross-border enforcement co-operation by privacy enforcement authorities***

Authorities with privacy enforcement responsibility are increasingly exploring mechanisms to co-operate with one another on a global basis in order to pursue complaints or conduct investigations relating to the activities of organisations outside of their borders. The OECD *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007) represents a commitment on the part of member countries to promote closer co-operation among privacy enforcement authorities to help them exchange information and carry out investigations with their foreign counterparts.<sup>94</sup>

Likewise, the APEC Co-operation Arrangement for Cross-border Privacy Enforcement (2009) represents an important step in support of a voluntary system of cross-border privacy rules based on the APEC Privacy Framework.<sup>95</sup> The APEC Arrangement was designed to be compatible with the OECD Recommendation in key respects, for instance, using similar definitions and anticipating the swapping of the list of economy contact points with the similar OECD list of national contact points.

The International Conference of Data Protection and Privacy Commissioners has adopted resolutions concerning international co-operation with other independent data protection authorities. The Article 29 Data Protection Working Party has also recognized the importance of co-operation in enforcing data protection laws.



In March 2010, 11 privacy enforcement authorities launched the Global Privacy Enforcement Network (GPEN), in recognition of the need to co-operate. The GPEN is a network designed to focus on the practical aspects of privacy enforcement co-operation. Among other things, GPEN provides points of contact for participating authorities to facilitate bilateral investigative and enforcement co-operation on specific matters. In addition, the GPEN participants intend to discuss enforcement issues, trends and experiences, as well as investigative techniques. The number of privacy enforcement authorities participating in GPEN has risen to 18 since the launch.

In 2009, the European Union and the United States High Level Contact Group (HLCG) issued a set of common principles on privacy and personal data protection for law enforcement purposes.<sup>96</sup> These principles complement the OECD Guidelines and provide a basis for further enhanced co-operation among law enforcement authorities while ensuring the privacy of EU and US individuals.

#### *A nascent privacy profession*

In recent years, organisations have responded in various ways to enhance privacy. Faced with organisational changes as a result of technology and increased operations in multiple jurisdictions, many of which have existing legal privacy requirements or have adopted new ones in recent years, organisations are increasingly devoting more resources to internal governance mechanisms to protect personal data. With this, we have seen the rise of the privacy practitioner.<sup>97</sup>

In some cases there is a statutory basis to support or encourage the role of the privacy professional. For example, Germany's *Bundesdatenschutzgesetz* (Federal Data Protection Act) sets out specific requirements concerning the data protection officials in organisations. Canada's federal private sector legislation, PIPEDA, requires an organisation to designate an individual(s) to be responsible for its personal data handling activities, and the EU Directive also contains a reference to a personal data protection official. New Zealand's *Privacy Act* requires every agency in both the public and private sectors to appoint a privacy officer. Various pieces of US legislation require federal agencies to have Chief Privacy Officers or Senior Agency Officials for Privacy.

Some work has begun on defining the competencies of the privacy professional, with the Canadian Access and Privacy Association developing a professional standards and certification project.<sup>98</sup> The emergence of a privacy profession has facilitated information sharing among privacy practitioners and it has contributed to organisational expertise. A number of organisations have also been created to support privacy practitioners.

The International Association of Privacy Professionals (IAPP) was founded in 2000 to define, promote and improve the privacy profession globally. It provides a credential programme in information privacy, as well as educational and professional development services, and hosts yearly conferences on privacy. Members of the European Privacy Officers Forum (EPOF) include data protection compliance officers and counsel from Europe. Members exchange information regarding data protection compliance, and the forum serves as a means for data protection authorities and business representatives to interact and discuss issues of mutual concern.<sup>99</sup> Members in the European Privacy Officers Network (EPON) include data protection professionals who work for organisations that operate in more than one country. It meets three times a year to discuss privacy issues related to cross-border data flows.<sup>100</sup>

In the past 10 years, there has been an explosion in the number of newsletters and books on privacy and data protection. Given technological changes, the passage of new laws, the effects of international events on national security, and the development of a privacy profession, there is an increased interest on the part of academics, lawyers and the media in the issue of privacy.

### *The growing voice of civil society*

Civil society has long been an important voice in promoting data protection, conducting and publishing research, and holding organisations and data protection authorities accountable in a variety of ways. Representatives of civil society attend OECD Working Party on Information Security and Privacy meetings through the Civil Society Information Society Advisory Committee (CSISAC), and participate in the work of APEC as well. Civil society has been an important part of the International Conference of Data Protection and Privacy Commissioners for many years, speaking at the conference and holding parallel conferences, and recently adopting a declaration of its own, the Madrid Declaration – Global Standards for a Global World.<sup>101</sup>

Privacy International celebrated its 20<sup>th</sup> anniversary in 2010, and many other organisations (some are listed below) have developed to advocate on myriad issues, such as consumer protection, intellectual property rights, PETs, and identity theft deterrence measures. These groups have, over the years, raised important issues through filing complaints to oversight authorities on matters, such as cookies, data transfers, street-level imaging, and social networking site practices. They have joined together in coalitions, such as the European Digital Rights Initiative (EDRI), The Public Voice Coalition, the U.S. Privacy Coalition, and the Trans Atlantic Consumer Dialogue, to raise public awareness of privacy issues.

The Public Voice Coalition was established in 1996 by the Electronic Privacy Information Center (EPIC) to promote public participation in the future of the Internet. It works towards bringing civil society and government together to discuss public policy issues and has been a partner with the OECD in a number of events.<sup>102</sup> The Trans Atlantic Consumer Dialogue (TACD) is a forum of United States and European Union consumer organisations. It develops and provides joint consumer policy recommendations to United States and European Union governments, and promotes consumer interests. One of its key work areas is the information society.<sup>103</sup>

### *Education, awareness*

There is a growing recognition that more needs to be done to make individuals aware of their rights and to promote data protection generally. To this end, Data Privacy Day/Data Protection Day is celebrated every year with events in Canada, the United States, and 27 European countries, on January 28 to raise awareness and generate discussion about the importance of privacy.<sup>104</sup> Privacy Awareness Week, celebrated since 2006 in the Asia-Pacific Region, now during May, also has the same purpose of raising awareness of the importance of privacy.<sup>105</sup> There have also been some recent efforts to find a single date to acknowledge privacy protection worldwide.

The London Initiative flowed from the 2006 International Conference of Data and Privacy Commissioners in London. It represents a “commitment by data protection authorities to focus on pragmatic effectiveness and improved communication.”<sup>106</sup>

Some organisations have developed online information resources for the benefit of organisations and individuals. For example, the OECD has a Privacy Policy Statement Generator, which is a tool designed to assist organisations in conducting an internal review of its existing personal data practices and developing a privacy policy.<sup>107</sup> The Virtual Privacy Office is a joint project of several data protection authorities that provides education information for anyone interested in privacy via a web site. It is managed by the Independent Centre for Privacy Protection Schleswig-Holstein.<sup>108</sup> The International Privacy Law Library enables searches on databases that specialise in privacy law. These databases are available in the WorldLII library.<sup>109</sup>

Many privacy enforcement authorities also have a specific mandate to promote privacy or data protection through public education. This mandate manifests itself in a variety of ways, from using web sites or Web 2.0 media to inform individuals and organisations about privacy, to speeches, news releases, opinion pieces for news media, conferences, and other forms of outreach to the public and organisations.

### *A move towards harmonisation*

Under the auspices of the International Conference of Data Protection and Privacy Commissioners, the Spanish Data Protection Authority is leading a project to develop, disseminate and promote the Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the Processing of Personal Data. A very recent attempt to present a global norm, the proposal articulates a draft set of minimum privacy principles that members of the International Conference believe are “present in different instruments, guidelines or recommendations of international scope and that have received a broad consensus in their respective geographical, economic or legal areas.”<sup>110</sup> The Joint Proposal also incorporates various recent data protection measures, including information management strategies, employee training, and appointment of individuals who are responsible for an organisation’s data protection practices, codes of practice, audits, privacy enhancing technologies, and privacy impact assessments. At the 31<sup>st</sup> International Conference of Data Protection and Privacy Commissioners, members adopted a resolution (the “Madrid Resolution”) in support of the Joint Proposal for a Draft of International Standards on 6 November 2009.

In 2005, the International Conference of Data Protection and Privacy Commissioners issued the Montreux Declaration, aimed at strengthening the universal nature of data protection principles.<sup>111</sup> There was a similar bid at the World Summit on the Information Society to have privacy recognised as a human right.<sup>112</sup>

In April 2010, the Council on General Affairs and Policy of The Hague Conference on Private International Law adopted a document entitled “Cross-Border Data Flows and Protection of Privacy” that outlines the organisation's possible future work in the area of privacy and data protection law. The document contains an overview of international data protection initiatives of the last few years, and addresses various cross-border co-operation issues, including problems created by the difficulty of determining applicable law and jurisdiction in cross-border data flows. The paper concludes by identifying three areas where The Hague Conference could play a role, namely *i*) identifying possible uncertainties on the applicable law to cross-border data flows, *ii*) assessing the feasibility of tools already successfully implemented by the The Hague Conference on transnational co-operation and co-ordination in other contexts as models for cross-border data flow questions; and *iii*) contributing to the ongoing debate whether additional multilateral efforts are feasible and/or desirable and whether it would bring added advantages with respect to existing instruments.

### *International and regional networks of privacy authorities*

Authorities with responsibility for protecting personal data and privacy and other stakeholders meet regularly in a variety of forums to share best practices and expertise, to promote data protection, and to discuss issues of mutual interest. Some of these groupings include members from around the world; others are more regionally focused. All represent attempts to work together, learn from each other, and build international co-operation.

The International Conference of Data Protection and Privacy Commissioners has been meeting regularly for more than three decades. In addition to Commissioners and representatives from their offices, conference participants include representatives of industry and government, civil society, and academics. There is also a members-only “closed-session” meeting to discuss and adopt resolutions, and other conference business. The International Working Group on Data Protection in Telecommunications has adopted numerous recommendations aimed at improving the protection of privacy in telecommunications. The Group is composed of representatives of privacy enforcement authorities, other government and international organisations.<sup>113</sup>

The Conference and the Working Group are well-established networks. However, in recent years, there has been a dramatic growth in the number of new networks appearing. Various regional networks have been bringing together countries with common geographic or linguistic links. Some examples include the Ibero-American Data Protection Network, which was formed “to foster, maintain and strengthen a close and constant exchange of information, experiences and knowledge among Ibero-American Countries, through dialogue and collaboration in issues related to personal data protection.”<sup>114</sup> The Asia Pacific Privacy Authorities (APPA) Forum meets twice a year to facilitate the sharing of knowledge and resources between privacy authorities within the region, foster co-operation, promote best practice, and work to continuously improve performance.<sup>115</sup> The Article 29 Working Party is an independent body that provides expert opinions on data protection to the European Commission, promotes a uniform application of the European Directive among the various states, advises the Commission about any measures that may affect privacy rights, and makes recommendations on data protection issues in the European Community.<sup>116</sup> Since 1991, European data protection authorities have been meeting annually at the Spring Conference of European Data Protection Authorities. Under this conference, the Working Party on Police and Justice operates. This is the body of European authorities that advises on any matters related to police and judicial co-operation. Moreover, staff members of authorities meet twice a year in the conference’s Case Handling Workshops, which exchange information on the day-to-day business of the authorities. The

*Association francophone des autorités de protection des données personnelles* was established in 2007. It promotes co-operation and training among French-speaking countries in the area of personal data protection. Its objective is to provide a structure for countries that have recently adopted privacy legislation. It constitutes a source of expertise for countries where there is no data protection legislation in place yet.<sup>117</sup>

### ***Technical standards work and the open technical community***

International standards bodies are currently working on establishing technical standards to assist organisations in better protecting personal data. The International Organization for Standardization (ISO) is working on technical standards for a Privacy Framework and Privacy Reference Architecture. Regional standards organisations, such as the American National Standards Institute (ANSI), and the European Committee for Standardization (CEN), are other examples of other organisations working on data protection standards. The European Telecommunications Standards Institute (ETSI) produces standards for Information and Communications Technologies. CEN/ISSS reported to the European Commission in 2003, on the utility of standards in enforcing the Directive. Much work continues in setting standards for networks, biometrics, identity and authentication, cryptographic protocols, security management, de-identification of health information, data storage, and other standards that have a bearing on privacy architectures.

Privacy has also gained increasing prominence in Internet governance discussions, particularly at the annual United Nations Internet Governance Forum (IGF) and the regional IGFs. In 2009 and 2010, the IGF program included a main session on Security, Openness and Privacy, as well as numerous workshops devoted to privacy issues. This is an example of the growing recognition of the value of multi-stakeholder collaboration and a holistic approach to privacy issues.<sup>118</sup>

Many organisations working on Internet technologies are beginning to focus more explicitly on personal data privacy. Supporting these efforts, standards-setting organisations are actively developing privacy-protecting patterns within their specifications.

In this effort, work within general standards-setting organisations, such as the Internet Engineering Task Force (IETF) (e.g. OAuth), World Wide Web Consortium (W3C) (e.g. STS), and the Organization for the Advancement of Structured Information Standards (OASIS) (e.g. SAML, XACML), is finding common ground with organisations such as the OpenID Foundation, Information Card Foundation, and the Kantara Initiative that are focused more specifically on identity solutions. The

commonality found across the many stakeholders is the growing understanding that users play an important role alongside government and enterprise in the protection of their privacy and personal data.<sup>119</sup>

Accompanying many efforts is a paradigm shift away from centralised command-and-control approaches relying entirely on cryptographic security as a means of handling and protecting personal data. The emerging focus is on providing granular access to specific personal data that may be distributed across multiple “authoritative sources” (e.g. health services, financial services, or government services).

## Conclusion

The OECD Privacy Guidelines have been a remarkable success, representing the first internationally agreed-upon set of privacy principles. The eight basic principles are concise, technologically neutral, and written using commonly understood language. This has made them adaptable to various government and legal structures, as well as to the changing social and technological environment, and has contributed to their enduring influence and importance. In the ensuing 30 years, they have been highly influential in the development of national data protection legislation and model codes within the OECD member countries. They have also influenced the development of the APEC Privacy Framework, thus expanding the reach of the Guidelines outside of the OECD member countries.

The Guidelines were forward-looking in orientation, anticipating many of the technological advancements that have since arisen. The improvements in processing of personal data have brought significant economic benefits as organisations have been able to expand their reach globally and have found innovative uses of personal data. Individuals have been able to seek information and products that are of benefit to them. Individuals have also experienced social benefits and are able to maintain contacts and relationships or conduct personal research or engage with their governments. The role of personal data protection principles in helping to maintain trust is integral to the continued benefits of personal data flows.

The scale and capabilities of data gathering, aggregation, correlation and analysis are radically different from what they were in 1980. Business models and data flows have also evolved. These changes are placing pressure on the scope of the privacy protections outlined in the Guidelines. The definition of personal data in the Guidelines is broad (“any information related to an identified or identifiable individual”) which, given the current power of analytics and the apparent limitations of anonymisation techniques, means vast amounts of data potentially now fall under the scope of privacy regimes.

In addition to the expanding amount of data that can be considered “personal data”, the concepts of data controller and data processor are under scrutiny. What was not foreseen at the time of the Guidelines was the key part that the individual would play in personal data flows and how personal data would become a “currency” on the Internet, such is the perceived economic value of the data. The individual was a passive player when personal data protection principles were being developed. Today, the individual is an active player in personal data creation and dissemination and may need to better understand his/her role in privacy protection. Certain types of technology and certain business models also present hurdles in determining who the data controller is. When the scope of data protection is broad and the responsible party is unclear, the core privacy principles become more challenging to implement and enforce. The risk is that personal data is not being adequately protected.

Although the individual is an active player in personal data flows, the ability to exert control over his/her own personal data is now more difficult. Individuals often face a lack of information or overly complex information about how, why and by whom their personal data may be used. Relying on “rules of thumb” when making decisions, presenting inconsistencies when weighing probabilities, placing more value on the present than on the future, affect how individuals understand information that is presented to them and may affect how they make privacy decisions. A further complication may arise when privacy policies change too frequently, which may also add to the general confusion of individuals. Obtaining access to their personal data can also be challenging both for individuals and organisations, given business models and the volume of data. The degree of protection ensured by obtaining individuals’ consent to uses and individuals’ control of their personal data by having access to it is less clear and may need further consideration.

Data also lives on. The costs of storing data today are far less than in 1980 while the costs of disposing of it are greater. The Guidelines do not contain a data retention principle although many privacy regimes do. The implications of data persistence are nonetheless significant – whether it is the effect on an individual’s reputation, the unanticipated and unauthorised uses of data, or the threats from breaches or malware to increasing amounts data that is stored indeterminately. Data breach notification has become an increasingly significant element of privacy oversight.

Advances in technology along with changes in organisation’s business models and practices have turned personal data transfers into personal data flows. Data is moving across borders, continuously. In light of this, security of personal data is paramount. Whether it is the result of mishandling of personal data by an organisation or threats to the security of data from outside forces, greater volumes of personal data are at risk and require protection more than ever.



The global nature of data flows has brought uncertainty over questions of applicable law, jurisdiction and oversight. Some organisations may not always be able or willing to tailor their services to meet the specific needs of each jurisdiction. Challenges to compliance with multiple data protection regimes may be significant, and personal data and economic growth may be threatened.

The current volume of data flows has highlighted the differences that remain among various national and regional approaches to data protection. The Guidelines sought to strike a balance between legitimate concerns regarding the need to establish principles to protect personal data and at the same time to prevent data flows from being inhibited.<sup>120</sup> They reflect the debate and the legislative work that went on in various Member countries in the years prior to the adoption. The Guidelines also reflect an arrangement whereby all OECD members at the time should implement privacy protections consistent with those outlined in the Guidelines (which should be regarded as a minimum) and not restrict data movement to other countries that are abiding by the Guidelines (subject to some exceptions). This arrangement, however, has not been reflected in all privacy regimes since implementation. For example, the EU Directive imposes requirements that go beyond those laid out in the Guidelines, and many OECD member countries have legislation that imposes similar requirements. Countries have chosen different approaches to protecting data and have expressed differing degrees of concern about barriers to cross-border data flows. Some countries have not implemented national legislation on data protection. Questions can be asked, therefore, about how influential the Guidelines have been in encouraging approaches that seek a balance between protecting personal data and preventing barriers to transborder data flows.

A renewed focus in recent years on finding common approaches to privacy protection at a global level, such as the development of international standards, is a response to the borderless nature of data flows, concerns around impediments to those flows, and the different cultural and legal traditions that have shaped the implementation of the Guidelines over the past 30 years. It is also a response to the challenges posed by technological and business model changes in recent years. The Guidelines have, in many respects, faced these challenges well. It is clear, however, that global solutions are needed and that a better understanding of different cultures' views of privacy and the social and economic value of transborder data flows is required to achieve this goal.

When the Guidelines were developed, the drafters drew on the work of others sources, such as the Nordic Council, the United States Government, and the Council of Europe. Currently, many key players, such as the European Union and the United States, are taking a careful look at the

effectiveness of their personal data protection regimes. There are movements to seek consensus on developing privacy protections in increasing numbers of countries. In going forward, attention should be given to studying these approaches in order to learn best practices and to build consensus within the privacy, business and government community to ensure a balance between legitimate organisational interests in data flows and the need for protecting privacy in the 21<sup>st</sup> century.

Our current legal and policy frameworks – most of which were developed in the 1970s or 1980s – could take advantage of more recent approaches to protecting privacy in today's environment. Various innovations in privacy governance have appeared over the past two decades to respond to the challenges to privacy that have resulted from technological changes. They vary from technological responses to the use of privacy by design and a focus on data management, from international and regional networks and co-operation efforts to a deepening examination of the role of accountability, and the need for education and awareness. Close attention may need to be given to the role these responses can play in improving privacy protection.

## Notes

1. See Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," in *Harvard Law Review*. Vol. IV, No. 6 (15 December 1890). In 1928, as a Justice on the U.S. Supreme Court, Brandeis once again addressed the impact of technology on privacy when he dissented in a 1928 ruling that allowed warrantless wiretaps. [http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy\\_brand\\_warr2.html](http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html)
2. See Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).
3. See [www.habeasdata.org/Interview-with-Spiros-Simitis](http://www.habeasdata.org/Interview-with-Spiros-Simitis).
4. See <http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>.
5. See Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967).
6. See Alan F. Westin and Michael Baker, *Databanks in a Free Society* (New York: Quadrangle/New York Times Cook Co., 1972).
7. See Paul Sieghart, *Privacy and Computers* (London: Latimer, 1976).
8. See Frits W. Hondius, *Emerging Data Protection in Europe*, (Amsterdam; North-Holland Publishing Company, 1975).
9. See [www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/data\\_protection/documents/international%20legal%20instruments/1Resolution\(73\)22\\_EN.pdf](http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/international%20legal%20instruments/1Resolution(73)22_EN.pdf).
10. See James Rule, Douglas McAdam, Linda Stearns and David Uglow, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies* (New York: Elsevier, 1980), p. 111.
11. See OECD (1976), *Policy Issues in data protection and privacy: concepts and perspectives*, OECD, Paris.
12. Quoted in John M. Eger, "Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers?" in *Law and Policy in International Business*, Vol. 10, No. 4 (1978) pp. 1065-66.
13. See the Honourable Justice Michael Kirby, "Privacy Protection – A New Beginning", presentation to the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September, 1999 [www.austlii.edu.au/au/journals/PLPR/1999/41.html](http://www.austlii.edu.au/au/journals/PLPR/1999/41.html).
14. See Australian Government First Stage Response to ALRC Privacy Report, October 2009, [www.dpmc.gov.au/privacy/alrc\\_docs/stage1\\_au\\_govt\\_response.pdf](http://www.dpmc.gov.au/privacy/alrc_docs/stage1_au_govt_response.pdf).

15. Privacy (Cross-border Information) Amendment Bill inserts a new Schedule 5A into the *Privacy Act 1993*.
16. See Françoise Gilbert, *Global Privacy and Security Law*, Vol. 2 (Aspen, 2009) §57.01-57.02[B], 57.02[E], 57.02[F].
17. The Spanish version of the legislation can be found here: [www.dof.gob.mx/nota\\_detalle.php?codigo=5150631&fecha=05/07/2010](http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010). For an unofficial translation into English, visit: [https://www.privacyassociation.org/images/uploads/Mexico%20Federal%20Data%20Protection%20Act%20\(July%202010\).pdf](https://www.privacyassociation.org/images/uploads/Mexico%20Federal%20Data%20Protection%20Act%20(July%202010).pdf).
18. For example, the United States passed the *Federal Information Security Management Act, 2002*, which requires each federal agency to develop, document and implement a programme to provide information security. With respect to accountability, the *US Appropriations Act 2005* created the positions of Chief Privacy Officers and Senior Officers for Privacy in all federal agencies. Japan's *Act on the Protection of Personal Information* requires businesses to appoint Chief Privacy Officers to implement the organisation's privacy practices.
19. See [http://privacymark.org/protection\\_group/about.html](http://privacymark.org/protection_group/about.html).
20. See OECD (2006), *Report on Cross-Border Enforcement of Privacy Laws*, OECD, Paris [www.oecd.org/dataoecd/17/43/37558845.pdf](http://www.oecd.org/dataoecd/17/43/37558845.pdf).
21. Many laws penalize those who violate the principles. The US *Computer Fraud and Abuse Act*, which establishes criminal penalties for unauthorised access to computers or networks, and Japan's *Act concerning the Protection of Personal Information Held by Administrative Organs*, which outlines criminal provisions for government officials who leak personal information without justification, are two examples.
22. See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>
23. See *APEC Privacy Framework*, 2004, para 4.
24. See "International agreements to protect personal data," Lee A. Bygrave, in *Global Privacy Protection: The First Generation*, James B. Rule and Graham William Greenleaf, (Cheltenham: Edward Elgar Publishing Limited, 2008), pp 29-30.
25. See [www.oecd.org/sti/privacycooperation](http://www.oecd.org/sti/privacycooperation).
26. See OECD (1999), *Guidelines for Consumer Protection in the Context of Electronic Commerce*, OECD, Paris [www.oecd.org/document/51/0,2340,en\\_2649\\_34267\\_1824435\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1_1,00.html)
27. See OECD (2009), *Empowering E-consumers, Strengthening Consumer Protection in the Internet Economy*, OECD, Paris [www.oecd.org/dataoecd/44/13/44047583.pdf](http://www.oecd.org/dataoecd/44/13/44047583.pdf).

28. See OECD (1980), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: Explanatory Memorandum*, OECD, Paris [www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html).
29. See OECD *Key ICT Indicators* [www.oecd.org/sti/ICTIndicators](http://www.oecd.org/sti/ICTIndicators).
30. See OECD (2009), *Communications Outlook*, OECD, Paris [www.oecd.org/document/44/0,3343,en\\_2649\\_34225\\_43435308\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/44/0,3343,en_2649_34225_43435308_1_1_1_1,00.html).
31. See [www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx](http://www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx).
32. See OECD *Key ICT Indicators* [www.oecd.org/sti/ICTIndicators](http://www.oecd.org/sti/ICTIndicators).
33. See Internet World Stats, January 2010, [www.internetworldstats.com](http://www.internetworldstats.com).
34. Verdone et al., (2008), as cited in OECD (2009) *Smart Sensor Networks: Technologies and Applications for Green Growth*, Paris, 2009 [www.oecd.org/dataoecd/39/62/44379113.pdf](http://www.oecd.org/dataoecd/39/62/44379113.pdf).
35. See OECD (2009), *Smart Sensor Networks: Technologies and Applications for Green Growth*, Paris, 2009 [www.oecd.org/dataoecd/39/62/44379113.pdf](http://www.oecd.org/dataoecd/39/62/44379113.pdf).
36. See OECD *Policy Guidance on Radio Frequency Identification*, Paris, 2008 [www.oecd.org/dataoecd/19/42/40892347.pdf](http://www.oecd.org/dataoecd/19/42/40892347.pdf).
37. See [www.priv.gc.ca/cf-dc/2004/cf-dc\\_040903\\_e.cfm](http://www.priv.gc.ca/cf-dc/2004/cf-dc_040903_e.cfm).
38. See [www.thirdfactor.com/2009/11/06/pittsburgh-schools-requiring-biometric-lunch-payment%20](http://www.thirdfactor.com/2009/11/06/pittsburgh-schools-requiring-biometric-lunch-payment%20).
39. Five years after the acceptance of the Guidelines, the importance of these flows were highlighted again in the OECD Declaration on Transborder Data Flows (1985). Member countries agreed to conduct further work on this issue.
40. See Paul Schwartz, “Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment, 2009”, A Report from the Privacy Projects.org <http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf>.
41. Cloud computing, includes activities such as Web 2.0, web services, the Grid, and Software as a Service (SaaS), which are enabling users to tap data and software residing on the Internet, rather than on a personal computer or a local server (from the OECD Briefing Paper on Cloud Computing and Public Policy).
42. Ibid, para. 47.
43. The NIST definition of cloud computing is as follows: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage,

applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” This cloud model promotes availability and is composed of essential characteristics, service models, and deployment models. See the “NIST Definition of Cloud Computing, version 15”, by Peter Mell and Tim Grance, 10-07-09.

44. See ZenithOptiMedia, July 2009, “Global advertising downturn slows despite disappointing Q1. Mild global recovery in 2010; all regions to return to growth in 2011”, [www.zenithoptimedia.com/gff/pdf/Adspend%20forecasts%20July%202009.pdf](http://www.zenithoptimedia.com/gff/pdf/Adspend%20forecasts%20July%202009.pdf).
45. Google reports that 75% of all Internet users in the United States visit government web sites, 48% have looked online for information about a public policy issue with their local, state or federal government, and 41% have downloaded government forms. From Google’s Government Toolkit, citing eMarketer.
46. See e.g. [www.facebook.com/CNIL](http://www.facebook.com/CNIL); [www.facebook.com/pages/Tel-Aviv-Yafo-Israel/ILITA/250200592257](http://www.facebook.com/pages/Tel-Aviv-Yafo-Israel/ILITA/250200592257); [www.state.gov/](http://www.state.gov/).
47. See OECD (2009), *OECD Conference on Empowering E-consumers: Strengthening Consumer Protection in the Internet Economy, Background Report*, OECD, Paris [www.oecd.org/dataoecd/42/59/44050135.pdf](http://www.oecd.org/dataoecd/42/59/44050135.pdf).
48. See [my.nielsen.com/site/20080414.shtml](http://my.nielsen.com/site/20080414.shtml).
49. See US Census Bureau, EStats, 2010 Annual Service Survey
50. See Flickr Blog, 12 October 2009; <http://blog.flickr.net/en/2009/10/12/4000000000/> The statistic quoted in the report was as of 12 October 2009.
51. See Facebook Press Room: [www.facebook.com/press/info.php?statistics](http://www.facebook.com/press/info.php?statistics) The statistic quoted in the report was as of 10 November 2010.
52. See Alessandro Acquisti, “Privacy in Electronic Commerce and the Economics of Immediate Gratification,” *Proceedings of ACM Electronic Commerce Conference (EC 04)* (New York, NY: ACM Press, 2004), 21-29, [www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf](http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf). See also, OECD (2010) *Consumer Policy ToolKit*, OECD, Paris.
53. See Danah Boyd, “Social Network Sites: Public, Private, or What?” Knowledge Tree 13 <http://kt.flexiblelearning.net.au/kt2007/>.
54. See [www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white\\_paper\\_c11-499060.pdf](http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-499060.pdf) for a study of data leakage and employee behaviours in 10 countries. See also, [www.priv.gc.ca/information/ar/200809/2008\\_pipeda\\_e.cfm](http://www.priv.gc.ca/information/ar/200809/2008_pipeda_e.cfm).
55. See “Timeline: Child Benefits Records Loss”, BBC News; 25 June, 2008, <http://news.bbc.co.uk/2/hi/7104368.stm>

56. See [www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf](http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf).
57. Compromised machines are computers that are controlled by one or many outside sources (“botnets” or “bots”). See OECD (2008/1), *Economics of Malware: Security Decisions, Incentives and Externalities*, OECD, Paris [www.oecd.org/dataoecd/53/17/40722462.pdf](http://www.oecd.org/dataoecd/53/17/40722462.pdf)
58. See MessageLabs Intelligence: 2010 Annual Security Report, available at [www.messagelabs.com/mlireport/MessageLabsIntelligence\\_2010\\_Annual\\_Report\\_FINAL.pdf](http://www.messagelabs.com/mlireport/MessageLabsIntelligence_2010_Annual_Report_FINAL.pdf)
59. See Article 29 Working Party opinion 2/2010 on online behavioural advertising, 22 June 2010.
60. See “Comment of epic.org to The National Institute of Standards and Technology, Smart Grid Standards”, 1 December, 2009; [http://epic.org/privacy/smartgrid/EPIC\\_Smart\\_Grid-Cybersecurity\\_12-01-09.2.pdf](http://epic.org/privacy/smartgrid/EPIC_Smart_Grid-Cybersecurity_12-01-09.2.pdf).
61. See the UK Information Commissioner, *A Report on the Surveillance Society*, September 2006, [www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/surveillance\\_society\\_full\\_report\\_2006.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf).
62. See “2007 Electronic Monitoring & Surveillance Survey”, conducted by the American Management Association and The ePolicy Institute [www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx#blank](http://www.amanet.org/training/articles/The-Latest-on-Workplace-Monitoring-and-Surveillance.aspx#blank).
63. See New Zealand Law Commission, [www.lawcom.govt.nz/ProjectGeneral.aspx?ProjectID=129](http://www.lawcom.govt.nz/ProjectGeneral.aspx?ProjectID=129).
64. See “A Face Is Exposed for AOL Searcher No. 4417749”, [www.nytimes.com/2006/08/09/technology/09aol.html](http://www.nytimes.com/2006/08/09/technology/09aol.html); Latanya Sweeney, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy Working Paper, LIDAP-WP4 (2000); Arvind Narayanan and Vitaly Shmatikov, How to Break the Anonymity of the Netflix Prize Dataset, 16 October, 2006, <http://arxiv.org/abs/cs/0610105>.
65. See Paul Ohm, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation,” *University of Colorado Law Legal Studies Research Paper No. 09-12*, for a detailed discussion on the limits of anonymisation and the use of it to balance privacy interests with innovation and research. [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1450006](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006).
66. See OECD (2009), *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, OECD, Paris [www.oecd.org/dataoecd/55/48/43091476.pdf](http://www.oecd.org/dataoecd/55/48/43091476.pdf).
67. See Article 29 Working Party Opinion 1/2010 on the concepts of “controller” and “processor”, 16 February 2010

68. See Privacy Commissioner of Canada *Report of Findings into the Complaint filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*, 15 July 2009; [www.priv.gc.ca/cf-dc/2009/2009\\_008\\_0716\\_e.cfm](http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm).
69. See OECD (2010), *Consumer Policy Toolkit*, OECD, Paris
70. Many non-OECD countries' privacy legislation contain restrictions on transborder transfers of personal information. Some examples include Senegal, Malaysia, Argentina.
71. See [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf).
72. See OECD (2006), *Report on the Cross-Border Enforcement of Privacy Laws*, OECD, Paris [www.oecd.org/dataoecd/17/43/37558845.pdf](http://www.oecd.org/dataoecd/17/43/37558845.pdf).
73. See [www.oecd.org/dataoecd/63/28/36494147.pdf](http://www.oecd.org/dataoecd/63/28/36494147.pdf).
74. See Adam Warren *et al*, "Privacy Impact Assessments: International experience as a basis for UK Guidance", *Computer Law & Security Report*, Vol. 24, Issue 3 (2008), pp 233 – 242  
[www.sciencedirect.com/science?\\_ob=PublicationURL&\\_tockey=%23TOC%235915%232008%23999759996%23690573%23FLA%23&\\_cdi=5915&\\_pubType=J&\\_auth=y&\\_acct=C000049020&\\_version=1&\\_urlVersion=0&\\_userid=946274&md5=ae2c4bce46405355bbbd67da8451e6b5](http://www.sciencedirect.com/science?_ob=PublicationURL&_tockey=%23TOC%235915%232008%23999759996%23690573%23FLA%23&_cdi=5915&_pubType=J&_auth=y&_acct=C000049020&_version=1&_urlVersion=0&_userid=946274&md5=ae2c4bce46405355bbbd67da8451e6b5).
75. See [www.archives.gov/about/laws/egov-act-section-207.html](http://www.archives.gov/about/laws/egov-act-section-207.html).
76. See [www.assembly.ab.ca/HIARReview/Health Information Act.pdf](http://www.assembly.ab.ca/HIARReview/Health%20Information%20Act.pdf).
77. See [http://ec.europa.eu/information\\_society/policy/rfid/documents/recommendationonrfid2009.pdf](http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf).
78. *Ibid*, p. 235
79. A resolution on Privacy by Design was passed at the 32nd International Data Protection and Privacy Commissioners Conference (27-29 October 2010) in Jerusalem, Israel.
80. See Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles", [www.privacybydesign.ca/background.htm](http://www.privacybydesign.ca/background.htm).
81. See OECD, *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, OECD, Paris. [www.oecd.org/dataoecd/55/48/43091476.pdf](http://www.oecd.org/dataoecd/55/48/43091476.pdf). There is, however, the potential to allow for increased tracking and profiling by linking previously separate identities.
82. See *Annual Report to Parliament 2004-2005*, Office of the Privacy Commissioner of Canada [www.priv.gc.ca/information/ar/200405/200405\\_pa\\_e.cfm](http://www.priv.gc.ca/information/ar/200405/200405_pa_e.cfm).



83. See Paula J. Bruening et al, "Strategic Information Management," Privacy and Security Law Report, Vol. 07, No. 36 ( 15 Sept 2008), pp. 1361-1363, [www.hunton.com/files/tbl\\_s47Details/FileUpload265/2310/SIM\\_9.15.08.pdf](http://www.hunton.com/files/tbl_s47Details/FileUpload265/2310/SIM_9.15.08.pdf).
84. See OECD (2002), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD, Paris [www.oecd.org/document/42/0,3343,en\\_2649\\_34255\\_15582250\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html).
85. Various examples include layered privacy notices and a privacy "nutrition" label approach. For more information on the latter, see, [www.cylab.cmu.edu/files/pdfs/tech\\_reports/CMUCyLab09014.pdf](http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf)
86. For example, the IdM Policy Audit System, a project jointly developed by the Internet Society and the Department of Computer Science at the University of Colorado, with participation by the Electronic Frontier Foundation and the Center for Democracy and Technology. See [www.isoc.org/projects/idm\\_policy\\_audit\\_system/](http://www.isoc.org/projects/idm_policy_audit_system/).
87. See "Safe Harbour Overview", Export.gov; <http://export.gov/safeharbor>.
88. See "Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers", Article 29 Data Protection Working Party, adopted 3 June, 2003 [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2003/wp74\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf).
89. See "APEC Cross-Border Privacy Rules", Australian Government [www.dpnc.gov.au/privacy/apec/cross-border.cfm](http://www.dpnc.gov.au/privacy/apec/cross-border.cfm) .
90. See "Data Protection Accountability: The Essential Elements A Document for Discussion", Centre for Information Policy Leadership as Secretariat to the Galway Project, October 2009 [www.huntonfiles.com/files/webupload/CIPL\\_Galway\\_Accountability\\_Paper.pdf](http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf).
91. See [www.cbpweb.nl/downloads\\_int/wp173\\_en.pdf](http://www.cbpweb.nl/downloads_int/wp173_en.pdf).
92. The PrivacyMark System, <http://privacymark.org/> is operated by the Japan Information Processing Development Corporation, [www.jipdec.or.jp/eng](http://www.jipdec.or.jp/eng).
93. See Chris Connelly, "Trustmark schemes struggle to protect privacy," Galexia.com.au, 2008 [www.galexia.com/public/research/assets/trustmarks\\_struggle\\_20080926/trustmarks\\_struggle\\_public.pdf](http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf).
94. See OECD (2007) *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD, Paris [www.oecd.org/dataoecd/43/28/38770483.pdf](http://www.oecd.org/dataoecd/43/28/38770483.pdf).
95. From the Joint Statement made at the 21st APEC Ministerial Meeting, November 11 and 12, 2009, [www.apec.org/apec/ministerial\\_statements/annual\\_ministerial/2009\\_21th\\_apec\\_ministerial.htm.l](http://www.apec.org/apec/ministerial_statements/annual_ministerial/2009_21th_apec_ministerial.htm.l)

96. See [http://useu.usmission.gov/Dossiers/Data\\_Privacy/Oct2809\\_SLCG\\_principles.asp](http://useu.usmission.gov/Dossiers/Data_Privacy/Oct2809_SLCG_principles.asp).
97. Paul Schwartz, “Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment, 2009”, A Report from the Privacy Projects.org, para. 77 <http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf>.
98. See [www.capa.ca/Main%20certification.html](http://www.capa.ca/Main%20certification.html).
99. See Hunton & Williams, European Privacy Officers Forum web site; [www.hunton.com/Resources/Sites/general.aspx?id=441](http://www.hunton.com/Resources/Sites/general.aspx?id=441).
100. See [www.privacylaws.com/templates/Events.aspx?id=364](http://www.privacylaws.com/templates/Events.aspx?id=364).
101. See <http://thepublicvoice.org/madrid-declaration/>.
102. See <http://thepublicvoice.org/>.
103. See [www.tacd.org/](http://www.tacd.org/).
104. See Data Privacy Day web site; <http://dataprivacyday2010.org/history/> and Council of Europe web site; [www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/data\\_protection/Default\\_DP\\_Day\\_en.asp#TopOfPage](http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/Default_DP_Day_en.asp#TopOfPage).
105. See Privacy Awareness Week web site; [www.privacyawarenessweek.org](http://www.privacyawarenessweek.org).
106. See *Annual Report 2006/07*, UK Information Commissioner’s Office; chapter 4 [www.ico.gov.uk/upload/documents/annual\\_report\\_2007\\_html/4\\_protecting-information.html](http://www.ico.gov.uk/upload/documents/annual_report_2007_html/4_protecting-information.html).
107. See [www.oecd.org/document/42/0,2340,en\\_2649\\_34255\\_28863271\\_1\\_1\\_1\\_1,00.html#whatis](http://www.oecd.org/document/42/0,2340,en_2649_34255_28863271_1_1_1_1,00.html#whatis).
108. See [www.datenschutz.de/privo/partner/regeln/](http://www.datenschutz.de/privo/partner/regeln/).
109. See [www.worldlii.org/int/special/privacy/#about](http://www.worldlii.org/int/special/privacy/#about).
110. See “Resolution on International Standards of Privacy” 31st International Conference of Data Protection and Privacy Commissioners, 2009
111. See [www.privacyconference2005.org/fileadmin/PDF/montreux\\_declaration\\_e.pdf](http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf).
112. See [www.itu.int/wsis/index.html](http://www.itu.int/wsis/index.html).
113. See [www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdp](http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdp).
114. See [www.redipd.org/la\\_red/Historia/index-iden-idphp.php](http://www.redipd.org/la_red/Historia/index-iden-idphp.php).
115. See [www.privacy.gov.au/aboutus/international/appa](http://www.privacy.gov.au/aboutus/international/appa).
116. See [http://ec.europa.eu/justice\\_home/fsi/privacy/docs/wpdocs/tasks-art-29\\_en.pdf](http://ec.europa.eu/justice_home/fsi/privacy/docs/wpdocs/tasks-art-29_en.pdf).

**126** – 4. THE EVOLVING PRIVACY LANDSCAPE: 30 YEARS AFTER THE OECD PRIVACY GUIDELINES

---

117. See [www.privacycommission.be/en/international/conferences/afapdp/](http://www.privacycommission.be/en/international/conferences/afapdp/).
118. See [www.intgovforum.org/cms/](http://www.intgovforum.org/cms/).
119. The key organisations include: IETF – Internet Engineering Task Force ([www.ietf.org/](http://www.ietf.org/)); W3C – World Wide Web Foundation ([www.w3.org/](http://www.w3.org/)); OASIS – Organization for the Advancement of Structured Information Standards ([www.oasis-open.org/](http://www.oasis-open.org/)); OpenID Foundation; Information Card Foundation (<http://informationcard.net/>); Kantara Initiative (<http://kantarainitiative.org/>).
120. Under Recommendations, the Guidelines state, “That Member countries endeavour to remove, or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data.”

*PART II.*  
*CROSS-BORDER PRIVACY LAW ENFORCEMENT*  
*CO-OPERATION*

*Chapter 5.***Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007)****[12 June 2007 – C(2007)67]****THE COUNCIL,**

**HAVING REGARD** to articles 1, 3, and 5 b) of the Convention on the Organisation for Economic Co-operation and Development of 14th 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.

## Chapter 6.

### Report on the Implementation of the 2007 OECD Recommendation on Privacy Law Enforcement Co-operation (2011)

#### Main points

In the 30 years since the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Privacy Guidelines) were adopted, the privacy landscape has undergone important changes, among which is a clear recognition of the need for improved privacy enforcement co-operation between privacy enforcement authorities.

On 12 June 2007, the OECD Council adopted a Recommendation<sup>1</sup> setting forth a framework for co-operation in the enforcement of privacy laws, based on the findings of a 2006 enforcement report.<sup>2</sup> As called for in the Recommendation, this report provides information on the progress in implementation measures, which are based in part on a survey of member country experiences.

The OECD has been actively supporting the implementation of the provisions of the Recommendation that relate to collective activities.

- One key implementation activity has been the launch in March 2010 of a new network for privacy enforcement co-operation – the Global Privacy Enforcement Network (GPEN). The OECD developed and hosts the website [www.privacyenforcement.net](http://www.privacyenforcement.net), which serves as the web platform for the GPEN.
- The list of national contact points for co-operation and mutual assistance under the Recommendation currently consists of 22 member countries and Estonia, and will be shared with authorities based outside the OECD.
- The ICCP Committee's Working Party on Information Security and Privacy (WPISP) developed a Request for Assistance Form for use by privacy enforcement authorities to help ensure that certain basic categories of information are provided to the authority receiving a request for assistance.

The Recommendation highlights that in order to improve cross-border privacy enforcement co-operation, governments need to develop and maintain a number of domestic measures. Some countries have reviewed or are in the process of reviewing their existing domestic frameworks, which might lead to adjustments of their legislation.

There are several key findings with respect to the domestic frameworks for co-operation.

- The importance of equipping privacy enforcement authorities with the necessary powers and authority to co-operate effectively across borders remains an issue.
- The powers to investigate generally seem to be adequate for most authorities, but further efforts may be needed to ensure that authorities have the power to administer significant sanctions, which could be of importance from the perspective of deterrence.
- Legal limitations on the ability of privacy enforcement authorities to share information with foreign authorities remain an issue in some countries, with some countries reporting either a legal barrier or a lack of clarity. There are fewer legal limitations regarding the sharing of non-case specific information, for example on technical expertise or investigation methods, but there are several authorities who are prohibited from doing so or whose legislation is unclear in this respect as well.
- Not all authorities are able to set their own priorities regarding for example the handling of complaints (some authorities are required to investigate each complaint they receive), which leaves them less time for possible cross-border co-operation. The resources allocated to the authorities generally remain an area of concern as well.
- Little information was reported in areas like redress for individuals in cross-border cases, or the ability to use evidence, judgments or court orders obtained abroad.

Looking at particular cases, cross-border co-operation appears to remain more the exception than the rule. There are however problems in obtaining good quantitative data about the volume and nature of cross-border complaints. There are some success stories in terms of bilateral co-operation between authorities on cross-border cases, many of which concern co-operation between EU member states.

The Recommendation recognises that cross-border co-operation can be improved by bilateral or multilateral enforcement arrangements or memoranda of understanding (MOU). An excellent example of a regional

multilateral arrangement is the 2009 Cooperation Arrangement for Cross-border Privacy Enforcement developed by Asia Pacific Economic Cooperation (APEC) economies.

The Recommendation calls for authorities to share information on enforcement outcomes. Members of GPEN and the International Conference of Data Protection and Privacy Commissioners recognise the importance of better sharing information and are working with their organisations to develop mechanisms to better share information.

Continued commitment by privacy enforcement authorities and their governments to implement the provisions of the Recommendation would help in fostering greater co-operation to ensure that the personal information of individuals is safeguarded no matter where it is located. At the moment locating reports and the results of cross-border cases remains a challenge.

## Background

As the OECD marks the 30<sup>th</sup> anniversary<sup>3</sup> of its 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Privacy Guidelines), virtually all OECD countries have enacted privacy laws and empowered authorities to enforce those laws. However, the volume and characteristics of cross-border data flows have brought important changes to the privacy landscape. In addition to bringing business efficiencies and conveniences for users, increases in global data flows have also elevated the risks to privacy and highlighted the need for improved privacy law enforcement co-operation. The importance of work in this area is recognised in the Seoul Ministerial Declaration, which calls for increased cross-border co-operation of governments and enforcement authorities in several areas, including the protection of privacy.<sup>4</sup>

The 1980 Guidelines are well known for their eight principles for the collection and handling of personal data, but they also call for member country co-operation through the establishment of procedures to facilitate mutual assistance in procedural and investigative matters. The need for effective privacy enforcement was highlighted in 1998 by Ministers in their Ottawa Declaration on the Protection of Privacy on Global Networks,<sup>5</sup> and emphasised again in 2003 in an OECD report calling for member countries to establish procedures to improve bilateral and multilateral mechanisms for cross-border co-operation by privacy authorities.<sup>6</sup>

The OECD began more in-depth work on privacy law enforcement co-operation in 2006, with an examination of challenges posed by cross-border aspects of this issue through a survey of OECD governments. Building on the results of a Questionnaire,<sup>7</sup> the OECD released a Report on the Cross-

border Enforcement of Privacy Laws in October 2006.<sup>8</sup> The report examined the law enforcement authorities and mechanisms that had been established with a particular focus on how they operated in the cross-border context. It described existing arrangements to address the challenges and identified a number of issues for further consideration.

Based on the findings of that report, on 12 June 2007, the OECD Council adopted a Recommendation<sup>9</sup> setting forth a framework for co-operation in the enforcement of privacy laws. The Recommendation was developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on Information Security and Privacy (WPISP). The work, conducted in close co-operation with privacy enforcement authorities, was led by Jennifer Stoddart, Privacy Commissioner of Canada. It built upon other OECD work on law enforcement co-operation in areas like spam<sup>10</sup> and cross-border fraud.<sup>11</sup>

The framework embodied in the Recommendation reflects a commitment by governments to improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities, as well as to provide mutual assistance to one another in the enforcement of privacy laws. It recognises that making co-operation commonplace cannot happen overnight. But a long-term commitment to implementing the principles in the recommendation can make enforcement co-operation effective among authorities rooted in varied domestic approaches.

The Recommendation calls for the ICCP Committee to exchange information on progress and experiences in implementing the principles, with a view to reporting back to Council within three years. At its meeting on 17-18 November 2008, the WPISP conducted a *tour de table* discussion of implementation activities and agreed to a proposal for preparing its implementation report. The preparatory work has been timed to permit the drafting of the report to Council in 2010. This report has been prepared with the assistance of an informal group of WPISP delegates. It includes a summary of member country implementation efforts, reflecting the replies to a written questionnaire circulated in November 2009.

### **Implementation activities supported by OECD**

Although primary responsibility for implementation of the Recommendation rests with member country governments and their privacy enforcement authorities, there is also a role for the OECD to facilitate some aspects of implementation. In particular, a number of the provisions of the Recommendation relate to collective activities, including the collection of contact points, sharing information on outcomes, and fostering the establishment of an informal network of privacy authorities. In addition there is a

section calling for consultation with other stakeholders, which is well-suited to a collective, multi-stakeholder approach. During the three years since the Recommendation was adopted, the OECD has been actively supporting the implementation of these provisions.

### *Contact points*

One of the most basic elements of cross-border enforcement co-operation is the need to know whom to contact when a cross-border enforcement issue arises. Although many enforcement officials will have existing contacts with colleagues from foreign authorities, a comprehensive contact list is an important complement.

The Recommendation calls for member countries to “designate a national contact point for co-operation and mutual assistance under this Recommendation” [para. 19]. The Recommendation further calls on the OECD Secretariat to maintain a record of the contact point information for the benefit of all member countries.

The process of collecting contact points with responsibility for distributing requests received to the appropriate domestic authority began in September 2007 through the circulation of a form [DSTI/ICCP/REG(2007)25]. To date, 22 member countries and Estonia have designated a contact point. Thus there remains room for progress in expanding the number of contacts on the list within the OECD, and as described below, beyond.

The current scope and scale of transborder data flows suggest that privacy law enforcement co-operation needs to extend well beyond the boundaries of the OECD to be effective. Indeed, the Recommendation itself specifically invites non-members to collaborate with OECD countries in its implementation. Fortunately, parallel work on contact points is being contemplated in other forums. For example, APEC economies are preparing a contact list as part of the newly endorsed APEC Cooperation Arrangement for Cross-border Privacy Enforcement. In the European context, the European Commission maintains a contact list of members and alternates for the Article 29 Data Protection Working Party. Within GPEN, the development of contact points is also a priority.

Recognising that contact list information is more valuable if it is shared among the various organisations that collect it, the WPISP agreed that the OECD Secretariat should share the internal contact list with authorities based outside the OECD through the other organisations or networks (absent objection from an individual on the contact list). Likewise, it would be welcome that other organisations share their lists with the OECD-based authorities. At some stage, it would be useful to have a single list of authorities around the world that could be prepared in collaboration with other organisations and kept up to date for maximum utility and convenience.



### ***Request for Assistance Form***

In addition to knowing whom to contact in a cross-border case, it can be useful to know what information will be needed to make that contact effective. Therefore the WPISP developed a Request for Assistance Form for use by privacy enforcement authorities to help ensure that certain basic categories of information are provided to the authority receiving the request for assistance.<sup>12</sup> It was also recognised that the process of completing the Form can also help ensure that the requesting authority has first conducted its own preliminary investigation or consideration of the matter, prior to seeking assistance.

The Request for Assistance Form is general enough for use in a variety of situations, including, for example, matters based on an individual complaint, matters arising out of media reports, or even industry-wide audits. The form is not burdensome to complete and each authority is perfectly free to adopt the form to suit the needs of a particular request.

The OECD form has been adapted for use by authorities from APEC economies under the APEC Cooperation Arrangement for Cross-border Privacy Enforcement. This is a useful step towards ensuring compatible processes between OECD and APEC, particularly for authorities from countries which are members of both organisations. Similar efforts to expand the use of the form more broadly could for example be pursued with the Council of Europe and the European Union.

### ***Fostering the establishment of an informal network of privacy enforcement authorities***

In a number of areas, informal networks have emerged to support cross-border regulatory enforcement co-operation. One example is the International Consumer Protection Enforcement Network (ICPEN), which has for many years provided an umbrella for the discussion and co-ordination of cross-border efforts in the consumer protection realm. Another initiative is the London Action Plan (LAP), which provides a forum to promote international enforcement co-operation against spam and other online threats.

In recognition of the utility such networks have had in other areas, the Recommendation calls for member countries to foster the establishment of an informal network of privacy enforcement authorities and other appropriate stakeholders [para. 21]. It further specifies a number of tasks for the network:

- 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 campaigns.

On 10 March 2010, representatives from several privacy enforcement authorities came together at a meeting hosted by the OECD and officially launched the Global Privacy Enforcement Network (GPEN). The Action Plan which serves as the basis of the network stresses that “it is important that government authorities charged with enforcing domestic privacy laws strengthen their understanding of different privacy enforcement regimes as well as their capacities for cross-border cooperation.”

GPEN is an informal network, open to public privacy enforcement authorities that are responsible for enforcing laws or regulations the enforcement of which has the effect of protecting personal data, and that have powers to conduct investigations or pursue enforcement proceedings. The network currently has as members 18 authorities from 15 jurisdictions, including Australia, Canada, France, Germany, Guernsey, Ireland, Israel, Italy, the Netherlands, New Zealand, Poland, Slovenia, Spain, the United Kingdom, and the United States, as well as the European Data Protection Supervisor. GPEN’s membership continues to expand.

GPEN is intended to focus on the practical aspects of privacy enforcement co-operation. Its mission is to share information about privacy enforcement issues, trends and experiences; participate in relevant training; co-operate on outreach activities; engage in dialogue with relevant private sector organisations on privacy enforcement and outreach issues; and facilitate effective cross-border privacy enforcement in specific matters by creating a contact list of privacy enforcement authorities interested in bilateral co-operation in cross-border investigations and enforcement matters. In line with the Recommendation, the focus of GPEN is primarily on facilitating co-operation in the enforcement of privacy laws governing the private sector. That however does not exclude co-operation on matters involving the processing of personal data in the public sector.

In order to provide further practical support to cross-border co-operation, the OECD has developed and hosts [www.privacyenforcement.net](http://www.privacyenforcement.net), which is being used by GPEN in order to support privacy enforcement co-operation between its members. In addition to providing a public face for GPEN, the site provides a restricted-access platform for the posting of documents and news items, and includes discussion forums, an events calendar and other functionalities to facilitate exchanges on privacy enforcement issues across borders.

*Fostering stakeholder dialogue*

Other examples of implementation activities supported by the OECD include fostering dialogue among key stakeholders. Section IV(C) of the Recommendation calls for a consultation between privacy authorities and privacy professionals on how best to resolve privacy complaints. On 27 May 2008, the OECD held a Roundtable bringing together some 50 participants, composed of privacy enforcement authorities and privacy professionals from many parts of the world. A full report of the proceedings is available on line at [www.oecd.org/sti/privacycooperation](http://www.oecd.org/sti/privacycooperation).

**Improving domestic measures to enable co-operation**

The Recommendation highlights that in order to improve cross-border privacy enforcement co-operation, governments need to develop and maintain a number of domestic measures (Section III). These include ensuring that authorities have the necessary authority to prevent and act in a timely manner against violations of laws protecting privacy, as well as the ability to share information and provide assistance to authorities in other countries. Responses to the implementation questionnaire highlight some of the initiatives taken at the domestic level to implement the Recommendation.

*Review of domestic frameworks*

The first step for some countries has been a review of existing domestic frameworks to determine whether it has sufficient authority to co-operate. The United States Federal Trade Commission (FTC) evaluates its ability to cooperate with international counterparts on an ongoing basis. A recent example is its 2009 Report to Congress on its experiences with the U.S. SAFE WEB Act, which provided the FTC expanded authority to co-operate with international authorities on enforcement matters. Reviews of the privacy frameworks are currently underway in a number of other countries, including Ireland, Korea, and New Zealand. For other countries, no formal review was considered necessary given the regular informal reviews.

More broadly, the EU has begun a review of its own data protection framework, Directive 95/46/EC. The European Commission recently issued a Communication on the review, which states that data protection authorities should be provided with the necessary powers and resources to properly exercise their tasks and calls for strengthened co-operation and co-ordination, particularly in the cross-border context.<sup>13</sup>

While it is too early to know the details of likely outcomes from all of these reviews, there are some interesting developments. For example, in August 2010 the Parliament of New Zealand enacted the Privacy (Cross-

border Information) Amendment Bill. This amendment empowers the Privacy Commissioner to refer a complaint to an overseas privacy enforcement authority – a term modelled on the OECD Recommendation. That will allow the Privacy Commissioner to work with privacy enforcement authorities in other countries to help New Zealanders protect their information wherever it is held, ensuring that New Zealand can take full advantage of the recent establishment of the APEC Cross-border Privacy Enforcement Arrangement (CPEA) and the Global Privacy Enforcement Network (GPEN). The bill also opens up the right of subject access to foreign individuals.<sup>14</sup>

### *Effective powers and authority*

The need for equipping privacy enforcement authorities with the necessary powers and authority to co-operate effectively across borders, as called for in the Recommendation, remains an issue.

Having authority to administer significant sanctions in appropriate cases can have an important deterrent value. This is particularly so in the cross-border context, where the likelihood of being subject to an enforcement action is more remote. The Canadian and Dutch authorities, for example, have no authority to directly impose sanctions for violations of privacy laws. Even for authorities with comparatively strong powers, some improvements have been called for. For example the U.S. FTC is seeking the authority to obtain civil penalties in data security cases for a number of reasons, including the deterrence value.

Consistent with the Recommendation, some improvements in this area were noted, for example in Germany, where administrative fines have been increased. Likewise, the Italian Garante has recently had its powers enhanced through increases in both the minimum and maximum fines it can issue. In 2008, the Korean Communications Commissioner received new powers to impose penalty surcharges for certain privacy-related violations. In 2010 the UK Information Commissioner's Office (ICO) has been given new powers to issue monetary penalties of up to GBP 500,000 for serious breaches. And the maximum penalties the Spanish data protection authority can issue have been increased to EUR 600,000 for major breaches of data protection legislation.

On the other hand powers to investigate generally seem to be adequate. Many authorities can compel testimony and the production of documents, enter premises, and obtain copies of records and other evidence. One exception had been the UK ICO, which prior to the Recommendation lacked a general power to conduct an audit without the consent of the organisation. In 2009, the legislation was updated to provide the commissioner with the power to issue an assessment notice to permit the inspection of an organisation's premises, albeit that this only extends initially to the auditing of government departments.

Not all privacy enforcement authorities are currently able to set their own priorities regarding, for example, the handling of complaints. Some are obliged to investigate all complaints received, and may not have sufficient flexibility to determine the way in which a complaint should be handled.<sup>15</sup> Having the ability to be selective in this respect gives privacy enforcement authorities the ability to decide to what activities they want to allocate their time and resources in order to be as effective as possible. This would also leave more time for possible cross-border enforcement actions.

A final issue relates to the resources allocated to enforcement authorities to accomplish their mission. Some authorities reported improvements in this area allowing for an increase in staffing. However, in other countries the economic difficulties facing governments are more likely to result in pressures to reduce budgets for government agencies, which may include privacy enforcement agencies

Little progress was reported in areas like redress for individuals in cross-border cases, or the ability to use evidence, judgments or orders obtained abroad. One exception in this respect was Korea, which in 2009 took steps to ratify the Hague Evidence Investigation Treaty.

#### ***Improving the ability to co-operate***

The Recommendation highlights that the ability of enforcement authorities to share information with each other is essential for the ability to co-operate. Legal limitations on the ability to share information with foreign authorities remain an issue in some countries. Although the Canadian Commissioner is still prohibited from sharing information with foreign authorities, this limitation would be removed under new legislation making its way through the process. For others who previously reported information-sharing limitations (e.g. Korea), the situation does not yet appear to have improved. For still others the power to share broadly with foreign authorities is not clear (e.g. Ireland). This uncertainty may be shared with other EU and EEA countries, for which the EU Data Protection Directive provides a legal basis for co-operation with other European authorities, but does not specifically address co-operation outside Europe.

There are fewer limitations on the sharing of information unrelated to specific cases. For example, many Member countries are able to share their technical expertise and investigation methods. However, not all privacy enforcement authorities have the authority to share such information with foreign authorities, or their legislation is unclear in this respect.

***Co-operating with other authorities and stakeholders***

The Recommendation calls for privacy enforcement authorities to consult with other types of criminal law enforcement authorities, private sector groups, and civil society [Section IV(C)]. Indications of the value of these consultations include work by UK ICO, which has now dedicated staff time to liaise with civil society groups. The ICO also reports that it has good working relations with its criminal enforcement colleagues. Another example is the Mexican data protection law that came into force in July of 2010. This law gives the Mexican Instituto Federal de Acceso a la Información y Protección de Datos the responsibility to co-operate with other domestic and international bodies and supervisory authorities, in order to assist in the area of data protection.<sup>16</sup>

**Examples of cross-border co-operation**

Cross-border co-operation in particular cases appears to remain more the exception than the rule. It is not fully clear the degree to which this simply reflects a lack of complaints/cases with a cross-border dimension or whether the challenges of cross-border co-operation by authorities remain a significant obstacle. An alternative explanation for the cases that have a cross-border dimension, most can be readily handled at a national level (i.e. without the need for co-operation).

***Number of cross-border complaints***

Evidence indicates that there are problems in obtaining good quantitative data about the volume and nature of cross-border complaints. Some authorities report that they are not easily able to identify or collate this type of information.

The Canadian authority reports that it has investigated 10-15 complaints with a cross-border dimension in nearly 10 years. New Zealand had two cross-border complaints last year.

***Referral of cross-border complaints***

Available data is limited, but what there is suggests that the referral of cross-border privacy complaints is not a prevalent practice. The U.S. FTC reports having referred cross-border complaints regarding data breaches and spyware to foreign authorities on several occasions. Japan reports that it has never been asked to provide assistance and has not referred any complaints to a foreign authority. One possible exception is the UK, which reports receiving complaints with a cross-border dimension, usually involving another European country, more regularly.

### ***Bilateral co-operation on cross-border cases***

A number of success stories can be reported in terms of bilateral co-operation. The US FTC provided assistance to the Office of the Canadian Privacy Commissioner (OPC) in connection with the OPC's investigation which enabled the OPC to determine that a company had violated several provisions of Canadian law.<sup>17</sup> The FTC had already brought an enforcement action against this company for violations of the FTC Act.<sup>18</sup> Another good example of co-operation involved a case in which a website hosted by a Brazilian university network published personal information about a number of Dutch politicians and civil servants. The Dutch DPA worked with the Portuguese privacy authority to have the university block access to the site. The Dutch DPA also reports providing assistance to the privacy authority in Guernsey in a case involving illegal content on a Dutch-hosted website. Other examples include co-operation between the UK and Spain involving unwanted solicitations regarding timeshares that resulted in the imposition of a EUR 60 000 fine by the Spanish DPA. Bilateral co-operation is a core element of the EU Privacy Directive, and occurs on a comparatively regular basis among EU member states.

### ***Multilateral enforcement co-operation***

Examples of multilateral co-operation can be seen at the European level, primarily through the enforcement subgroup of the Article 29 Working Party. Two investigations have been co-ordinated through the subgroup, the first of which involved a number of European DPAs investigating the processing of personal data by insurance companies for the health sector.<sup>19</sup> The second investigation concerned traffic data retention.<sup>20</sup> In 2010 the Article 29 Working Party has also sent collective letters to search engines regarding their compliance with European law.<sup>21</sup>

Other recent examples of multilateral enforcement co-operation are beginning to emerge. For example in April 2010, the Privacy authorities in Canada, France, Germany, Israel, Italy, Ireland, the Netherlands, New Zealand, Spain and the United Kingdom issued a joint letter to a company to highlight the importance of taking adequate account of privacy considerations prior to launching new services.<sup>22</sup>

Besides joint investigations, the Article 29 Working Party also plays a role in the process of co-ordinating separate national investigations that are being conducted in the same period of time and focus on the same or similar activities. Supporting and facilitating the sharing of information, including technical expertise and investigation methods, between the privacy enforcement authorities performing these investigations (as far as their legislation allows for it) is one of its mechanisms. That can contribute to having co-ordinated outcomes of these individual national investigations, reducing the burdens on the investigated organisations.

## Other international initiatives

### *Bilateral or regional co-operation arrangements*

The Recommendation recognises that one way to improve co-operation across-borders is through bilateral or multilateral enforcement arrangements or memoranda of understanding (MOU) (para. 13).

In 2006, the OECD already noted a number of bilateral co-operation arrangements: a 2005 MOU between the Spanish Data Protection Authority and the U.S. Federal Trade Commission on spam; and a 2006 MOU between the privacy commissioners of Australia and New Zealand. New Zealand and Australia recently updated their MOU to reflect the OECD Recommendation.<sup>23</sup> There do not appear to be any new examples.

In terms of regional arrangements, in November 2009, APEC ministers endorsed a Cooperation Arrangement for Cross-border Privacy Enforcement, referred to as CPEA.<sup>24</sup> This instrument provides a framework for cross-border privacy enforcement co-operation among authorities in the APEC member economies. Its goals are to facilitate information sharing among authorities; establish mechanisms to promote effective co-operation, for example, by referring matters to, or conducting parallel or joint investigations or enforcement actions with, other authorities; facilitate co-operation in enforcing Cross-Border Privacy Rules (the rules guide businesses on internal privacy procedures and informing customers about their practices); and encourage information sharing and co-operation with privacy enforcement authorities outside of APEC. Prior to the endorsement of APEC's Cooperation Arrangement there has been close co-ordination between OECD and APEC in order to ensure consistency in the definitions in their respective enforcement instruments.

Another regional arrangement, aimed amongst others at enforcement co-operation, is the Asia Pacific Privacy Authorities Forum (APPA). The purpose of APPA is to facilitate the sharing of knowledge and resources between privacy authorities within the region; foster co-operation in privacy and data protection; promote best practice amongst privacy authorities; and work to continuously improve its performance to achieve the important objectives set out in the members' respective privacy laws. Under the auspices of this forum Australia, Korea, New Zealand, New South Wales, Victoria (Australia), Canada, British Columbia and Hong Kong, China meet two times every year. In 2010 they were joined by a new member, the US Federal Trade Commission. This is the first authority that joined APPA after it broadened its membership rules to enable privacy enforcement authorities from across APEC economies (which participate in the CPEA) to join the forum.



Other examples of co-operation arrangements include arrangements related to European co-operation on privacy issues related to the Eurojust, Schengen, Europol and Customs Information Systems. There are also regular contacts between an Article 29 Working Party subgroup that participates in the “Privacy Contact Group” along with the U.S. Department of Commerce and the FTC to discuss Safe Harbor issues.

### *Information sharing on enforcement outcomes*

The Recommendation calls for privacy enforcement authorities to “share information on enforcement outcomes to improve their collective understanding of how privacy law enforcement is conducted” [para. 20]. The motivation for working on this topic is highlighted in the “Report on Cross-border Enforcement Co-operation in the Enforcement of Privacy Laws,” which noted how difficult it is to locate reports of cross-border cases.<sup>25</sup> In some respects, researching the results of privacy enforcement activities is challenging even in a purely domestic setting. Many privacy enforcement arrangements promote early resolution of complaints through conciliation, the outcomes of which are not routinely accessible beyond the parties and the enforcement authority. Privacy cases only rarely go before the courts and there are, therefore, often no accessible reports of enforcement outcomes.

The Recommendation recognised that one way to help improve this situation is through encouraging enforcement authorities to create instructive case reports in a format that facilitates access and use by other authorities. Sharing information on enforcement outcomes can promote understanding of the operation of privacy laws in other countries and may also contribute to more consistent interpretations through exposure to well-reasoned approaches from elsewhere.

A number of privacy enforcement authorities already publish case reports on their websites and/or via annual reports.<sup>26</sup> The Privacy Commissioner of New Zealand, for example, has published more than 230 case notes on completed complaints and investigations. The Privacy Commissioner of Canada regularly posts summaries of noteworthy investigations. The US FTC routinely issues press releases relating to its enforcement actions. Among European authorities, the Case Handling Workshop set up by the European Data Protection Conference provides a platform to share information and experiences.

There is still considerable scope for improvements in this area. Even where authorities do publish cases notes, the results are not always easy to access. The Asia Pacific Privacy Authorities Forum (APPA) has taken steps to address this issue, agreeing on a common case note citation format. Each

case note from an APPA authority should include: *i)* a descriptor of the case; *ii)* the year of publication; *iii)* a standard abbreviation for the privacy authority; and *iv)* a sequential number. Similar proposals have been considered by the International Working Group on Data Protection in Telecommunications. A citation system like that of the APPA might have to be adjusted somewhat to account for the greater variety in practices across the OECD, but could serve as a useful starting point.

Closely linked is the issue of disseminating case notes. Once again the APPA has taken the lead, agreeing on steps for actively disseminating case notes. Having a central access point or points on the Internet can assist transborder accessibility and the APPA has selected the WorldLII Privacy Law Library ([www.worldlii.org/int/special/privacy/](http://www.worldlii.org/int/special/privacy/)) for that purpose. Other suitable web repositories may exist for other languages.

Disseminating information on cases and outcomes is also a priority among the members of GPEN. GPEN's privacy enforcement website discussed above might be a useful place to make these reports available.

In November 2009, the International Conference of Data Protection and Privacy Commissioners adopted a resolution on case reporting calling upon authorities to disseminate information on cases and outcomes, complementing the parallel provisions in the OECD Recommendation.<sup>27</sup>

## Conclusion

In today's globalised world, occasional transborder transfers of personal data have evolved into a continuous, multipoint data flow. The important benefits of this evolution for organisational efficiency and user convenience are accompanied by new challenges and concerns with respect to the protection of privacy. In this context, OECD governments have committed to improved co-operation among privacy enforcement authorities, as reflected in the 2007 OECD recommendation.

All available indications suggest that the Recommendation is stimulating improvements in member countries to co-operate across borders in the enforcement of laws protecting privacy. None of the responses to the questionnaire indicated that disputes had arisen in the context of co-operation. There do not appear to have been any adverse consequences to the increased co-operation. There seems to be a willingness to co-operate, however actual instances of co-operation are still limited.

The review of implementation activities suggests that there are a number of areas that would require continued efforts by member countries and their privacy enforcement authorities. These would include additional efforts to:

- Designate a contact point in order to be able to be contacted for cross-border issues.
- Share case-related information in individual cross-border cases and information on technical expertise and investigative methods.
- Share information on enforcement outcomes by publishing case reports, possibly in a common format that would make comparisons easier.
- Consult with other types of criminal law enforcement authorities, private sector groups and civil society.
- Consider becoming a member of regional or global enforcement arrangements or develop bilateral memoranda of understanding with other authorities.

Renewed efforts by member countries are necessary in order to address legal impediments to effective cross-border privacy enforcement co-operation. Of particular concern are restrictions on sharing information with foreign authorities which is a core element of successful co-operation, but which remains an issue for some authorities. Likewise there remain considerable variations in the powers and resources put at the disposal of privacy authorities by their governments. Progress is still needed to equip authorities with the tools and resources to effectively address privacy violations occurring across borders.

Continued co-operation among international organisations working to improve privacy law enforcement co-operation will remain a key element going forward. For example, the close co-ordination between OECD and APEC to ensure consistency in definitions in their respective instruments in this area is particularly noteworthy, and such co-operation should be expanded more broadly.

Renewed efforts by privacy enforcement authorities and their governments to implement the provisions of the Recommendation would help in building a global framework for co-operation to ensure that the personal information of individuals is safeguarded no matter where it is located.

## Notes

1. Available at [www.oecd.org/dataoecd/43/28/38770483.pdf](http://www.oecd.org/dataoecd/43/28/38770483.pdf).
2. See [www.oecd.org/dataoecd/17/43/37558845.pdf](http://www.oecd.org/dataoecd/17/43/37558845.pdf).
3. See [www.oecd.org/sti/privacyanniversary](http://www.oecd.org/sti/privacyanniversary).
4. See [www.oecd.org/futureinternet](http://www.oecd.org/futureinternet).
5. Declaration on the Protection of Privacy on Global Networks, 7-9 October 1998, Ottawa Canada. See [www.oecd.org/dataoecd/39/13/1840065.pdf](http://www.oecd.org/dataoecd/39/13/1840065.pdf).
6. OECD, "Privacy Online: OECD Guidance on Policy and Practice, p. 18-19, available at: [www.ois.oecd.org/olis/2002doc.nsf/LinkTo/NT000029C6/\\$FILE/JT00137976.PDF](http://www.ois.oecd.org/olis/2002doc.nsf/LinkTo/NT000029C6/$FILE/JT00137976.PDF)
7. Available at [www.oecd.org/dataoecd/5/30/37572050.pdf](http://www.oecd.org/dataoecd/5/30/37572050.pdf).
8. Available at [www.oecd.org/dataoecd/17/43/37558845.pdf](http://www.oecd.org/dataoecd/17/43/37558845.pdf).
9. Available at [www.oecd.org/dataoecd/43/28/38770483.pdf](http://www.oecd.org/dataoecd/43/28/38770483.pdf).
10. See [www.oecd.org/document/24/0,3343,en\\_2649\\_34255\\_34804568\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/24/0,3343,en_2649_34255_34804568_1_1_1_1,00.html).
11. See [www.oecd.org/dataoecd/24/33/2956464.pdf](http://www.oecd.org/dataoecd/24/33/2956464.pdf).
12. Available at: [www.oecd.org/dataoecd/43/58/38772442.doc](http://www.oecd.org/dataoecd/43/58/38772442.doc).
13. See the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – a comprehensive approach on personal data protection in the European Union, available at: [http://ec.europa.eu/justice/news/consulting\\_public/0006/com\\_2010\\_609\\_en.pdf](http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf).
14. See [www.privacy.org.nz/updated-media-release-30-8-10-privacy-amendment-important-for-trade-and-consumer-protection/](http://www.privacy.org.nz/updated-media-release-30-8-10-privacy-amendment-important-for-trade-and-consumer-protection/).
15. See WP 168 (The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data), available at: [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf).
16. See article 39 under VII of the Ley Federal de Protección de Datos Personales en Posesión de los Particulares. An English translation of the law can be

found on [https://www.privacyassociation.org/images/uploads/Mexico%20Federal%20Data%20Protection%20Act%20\(July%202010\).pdf](https://www.privacyassociation.org/images/uploads/Mexico%20Federal%20Data%20Protection%20Act%20(July%202010).pdf).

17. See [www.priv.gc.ca/cf-dc/2009/2009\\_009\\_rep\\_0731\\_e.cfm](http://www.priv.gc.ca/cf-dc/2009/2009_009_rep_0731_e.cfm).
18. See *Federal Trade Commission v. Accusearch, Inc., d/b/a Abika.com, and Jay Patel*, United States District Court for the District of Wyoming Civil Action No. 06-CV-105-D FTC File No. 052 3126 (D. Wy., September 28, 2007).
19. See WP 137 (Report on the first joint enforcement action, adopted on 20 June 2007), available at [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2007/wp137\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp137_en.pdf).
20. See WP 172 (Report on the second joint enforcement action, adopted on 13 July 2010), available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf).
21. [http://ec.europa.eu/justice/policies/privacy/news/docs/pr\\_26\\_05\\_10\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/news/docs/pr_26_05_10_en.pdf).
22. See [www.priv.gc.ca/media/nr-c/2010/let\\_100420\\_e.cfm](http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm).
23. See [www.privacy.gov.au/aboutus/international/nz](http://www.privacy.gov.au/aboutus/international/nz).
24. See [www.apec.org/apec/apec\\_groups/committee\\_on\\_trade/electronic\\_commerce/cpea.html](http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce/cpea.html).
25. See [www.oecd.org/dataoecd/17/43/37558845.pdf](http://www.oecd.org/dataoecd/17/43/37558845.pdf).
26. For a survey of Asia Pacific privacy case reporting practices see G. Greenleaf, "Reforming Reporting of Privacy Cases: A Proposal for Improving Accountability of Asia-Pacific Privacy Commissioners," (2004), available at: <http://ssrn.com/abstract=512782>. In addition, many authorities produce annual reports which include information about cases outcomes and statistics, and the EU's Article 29 Working Party produces an annual report that includes country by country highlights.
27. See [www.privacyconference2010.org/upload/2009-4.pdf](http://www.privacyconference2010.org/upload/2009-4.pdf).

## Chapter 1.

### Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)

[C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79]

#### 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 *Ministerial Declaration on the Protection of Privacy on Global Networks* [Annex 1 to C(98)177]; the *Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks* [C(2002)131/FINAL], the *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* [C(2007)67], the *Declaration for the Future of the Internet Economy (The Seoul Declaration)* [C(2008)99], the *Recommendation of the Council on Principles for Internet Policy Making* [C(2011)154], the *Recommendation of the Council on the Protection of Children Online* [C(2011)155] and the *Recommendation of the Council on Regulatory Policy and Governance* [C(2012)37];

**RECOGNISING** that Member countries have a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information;

**RECOGNISING** that more extensive and innovative uses of personal data bring greater economic and social benefits, but also increase privacy risks;

**RECOGNISING** that the continuous flows of personal data across global networks amplify the need for improved interoperability among privacy frameworks as well as strengthened cross-border co-operation among privacy enforcement authorities;

**12** – I. OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

**RECOGNISING** the importance of risk assessment in the development of policies and safeguards to protect privacy;

**RECOGNISING** the challenges to the security of personal data in an open, interconnected environment in which personal data is increasingly a valuable asset;

**DETERMINED** to further 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 them;

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

- I. **RECOMMENDS** that Member countries:
  - Demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest levels of government;
  - Implement the Guidelines contained in the Annex to this Recommendation, and of which they form an integral part, through processes that include all relevant stakeholders;
  - Disseminate this Recommendation throughout the public and private sectors;
- II. **INVITES** non-Members to adhere to this Recommendation and to collaborate with Member countries in its implementation across borders.
- III. **INSTRUCTS** the Committee for Information, Computer and Communication Policy to monitor the implementation of this Recommendation, review that information, and report to the Council within five years of its adoption and thereafter as appropriate.

This Recommendation revises 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].

## 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 national 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) “Laws protecting privacy” means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines.
  - d) “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.
  - e) “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 risk to privacy and individual liberties.
3. The principles in these Guidelines are complementary and should be read as a whole. They should not be interpreted:
  - a) as preventing the application of different protective measures to different categories of personal data, depending upon their nature and the context in which they are collected, stored, processed or disseminated; or



**14** – 1. OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

- b) in a manner which unduly limits the freedom of expression.
- 4. Exceptions to 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 can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data.

**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. Individuals 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 them;
  - b) to have communicated to them, data relating to them
    - 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 them;
  - 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 them 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. IMPLEMENTING ACCOUNTABILITY**

15. A data controller should:
- a) Have in place a privacy management programme that:
    - i. gives effect to these Guidelines for all personal data under its control;
    - ii. is tailored to the structure, scale, volume and sensitivity of its operations;
    - iii. provides for appropriate safeguards based on privacy risk assessment;
    - iv. is integrated into its governance structure and establishes internal oversight mechanisms;
    - v. includes plans for responding to inquiries and incidents;
    - vi. is updated in light of ongoing monitoring and periodic assessment;
  - b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and
  - c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

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

16. A data controller remains accountable for personal data under its control without regard to the location of the data.
17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.
18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

**PART FIVE. NATIONAL IMPLEMENTATION**

19. In implementing these Guidelines, Member countries should:
- a) develop national privacy strategies that reflect a co-ordinated approach across governmental bodies;
  - b) adopt laws protecting privacy;
  - c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;
  - d) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
  - e) provide for reasonable means for individuals to exercise their rights;
  - f) provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;
  - g) consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy;
  - h) consider the role of actors other than data controllers, in a manner appropriate to their individual role; and
  - i) ensure that there is no unfair discrimination against data subjects.

**PART SIX. INTERNATIONAL CO-OPERATION AND INTEROPERABILITY**

20. Member countries should take appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.
21. Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines.
22. Member countries should encourage the development of internationally comparable metrics to inform the policy making process related to privacy and transborder flows of personal data.
23. Member countries should make public the details of their observance of these Guidelines.

## *Chapter 2.*

### **Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)**

#### **Introduction**

In 1980, the OECD adopted the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (“1980 Guidelines”) to address concerns arising from the increased use of personal data and the risk to global economies resulting from restrictions to the flow of information across borders. The 1980 Guidelines, which contained the first internationally agreed-upon set of privacy principles, have influenced legislation and policy in OECD Member countries and beyond. Framed in concise, technology-neutral language, they have proven remarkably adaptable to technological and societal changes. Nevertheless, changes in personal data usage, as well as new approaches to privacy protection, have left the 1980 Guidelines in need of updating in a number of important respects. The Honourable Michael Kirby chaired the original OECD expert group that drafted the Guidelines. In reflecting on that achievement on the occasion of the Guideline’s 30th anniversary Justice Kirby observed: “In the field of information policy, the technology is such that no international expression of principles can be immune from the forces of change.”<sup>1</sup>

#### **Context of the review**

Over the last three decades, personal data have come to play an increasingly important role in our economies, societies and everyday lives. Innovations, particularly in information and communication technologies, have impacted business operation, government administration, and the personal activities of individuals. New technologies and responsible data uses are yielding great societal and economic benefits. The volume of

personal data being collected, used and stored is vast and continues to grow. Modern communications networks support global accessibility and continuous, multipoint data flows. The potential uses of personal data have increased tremendously as a result of the wide range of analytics that can provide comprehensive insights into individuals' movements, interests, and activities.

At the same time, the abundance and persistence of personal data have elevated the risks to individuals' privacy. Personal data is increasingly used in ways not anticipated at the time of collection. Almost every human activity leaves behind some form of digital data trail, rendering it increasingly easy to monitor individuals' behaviour. Personal data security breaches are common. These increased risks signal the need for more effective safeguards in order to protect privacy.

In recent years, several initiatives have been undertaken to address new and elevated privacy risks, particularly in the context of transborder data flows. The work is ongoing and examples include the European Union's system of Binding Corporate Rules (BCRs)<sup>2</sup>; the global discussion on the commonly accepted elements of privacy accountability<sup>3</sup>; and the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules System (APEC CBPR).<sup>4</sup> At the OECD, cross-border co-operation among privacy enforcement authorities has been a priority, resulting in the adoption of the 2007 Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (the "2007 Recommendation", [OECD, 2007]).

The *Seoul Declaration for the Future of the Internet Economy* (2008) recommended that the OECD assess the application of certain OECD instruments, including the 1980 Guidelines, in light of "changing technologies, markets and user behaviour and the growing importance of digital identities." This Declaration triggered the launch of a formal review of the 1980 Guidelines.

The OECD Recommendation on Principles for Internet Policy Making (OECD, 2011a) called for a strengthening of consistency and effectiveness in privacy protection at a global level. While the OECD Privacy Guidelines have a broader scope than Internet policies, the 2011 Recommendation is nevertheless instructive. The Communiqué attached to the 2011 Recommendation for information purposes explains that current privacy challenges are likely to become more acute "as the economy and society depends more heavily on broadened and innovative uses of personal information that can be more easily gathered, stored, and analysed" (OECD, 2011b).

Privacy frameworks around the world are being examined and refined. Three of the primary frameworks with an international dimension (OECD, European Union, and Council of Europe) have been under review simultaneously, and a fourth (APEC) is implementing new cross-border arrangements. Work on domestic privacy frameworks is likewise underway across the globe, from Australia to Brazil to China to the United States. In light of all of these developments, the OECD concluded that it was an appropriate time to engage in a substantive review of the 1980 Guidelines.

### **Process of the review**

Preparations for the review began in 2010, in the context of the 30<sup>th</sup> anniversary of the 1980 Guidelines. As part of the process, the OECD organised three thematic events. These events addressed (1) the impact of the 1980 Guidelines; (2) the evolving role of the individual; and (3) the economic dimensions of personal data and privacy. It also produced two reports, “The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines” (OECD, 2011c), and “Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation” (OECD, 2011d).

Building on this preparatory work, the Working Party for Information Security and Privacy (WPISP) developed Terms of Reference (OECD, 2011e) to serve as a roadmap for the review. The Terms of Reference articulated a shared view of current issues and approaches, and provided the rationale for further work. In addition to highlighting the changes in the environment, the Terms of Reference identified those elements which Member countries considered essential to improving the effectiveness of privacy protections.

A Volunteer Group of Privacy Experts (“Expert Group”) was formed to assist the WPISP in the review process. This group included experts from governments, privacy enforcement authorities, academics, business, civil society, and the Internet technical community. Participants also included representatives of the Council of Europe and the European Union, as well as experts active in APEC. This multi-stakeholder group was chaired by Jennifer Stoddart, Privacy Commissioner of Canada. Omer Tene served as the Rapporteur to the group. The Expert Group collaborated through a series of meetings and a virtual workspace during 2011 and 2012. During these meetings, the Expert Group focused on three main themes identified by the Terms of Reference, namely: (1) the roles and responsibilities of key actors; (2) geographic restrictions on transborder data flows; and (3) proactive implementation and enforcement.

The approach that emerged from the work of the Expert Group suggested that, although the environment for privacy and transborder data flows has changed significantly, an update to the 1980 Guidelines was preferred rather than a fundamental rethinking of its core principles. The Expert Group took the view that the balance reflected in the eight basic principles of Part Two of the 1980 Guidelines remains generally sound and should be maintained. The Expert Group introduced a number of new concepts to the OECD privacy framework, such as privacy management programmes, security breach notification, national privacy strategies, education and awareness, and global interoperability. Other aspects of the 1980 Guidelines were expanded or updated, such as accountability, transborder data flows and privacy enforcement.

The 1980 Guidelines were accompanied by an Explanatory Memorandum, which described the environment that led to their development, as well as their underlying rationale. The Explanatory Memorandum provides insight into the competing priorities of the time, as well as a detailed interpretation of various provisions in the 1980 Guidelines, some of which have not been modified (in particular those of Part Two). These insights remain relevant today. This Supplementary Explanatory Memorandum has been prepared as part of the review process to complement the revised Guidelines. It is intended to supplement – not replace – the original Explanatory Memorandum. Where there have been changes to the 1980 Guidelines, this Supplementary Explanatory Memorandum sheds light on the rationale and context of these changes to help understand and interpret them.



## Revisions to the Guidelines

### Privacy management programmes

Part Two of the 1980 Guidelines sets forth the principle of accountability, which places the onus on the data controller to comply “with measures that give effect to the rest of the principles”. Recognition of the importance of the accountability principle has increased over time. Domestic privacy laws have come to introduce a variety of mechanisms designed to promote the accountability of both public and private data controllers. Obligations of transparency towards individuals and privacy enforcement authorities are clear examples of such mechanisms.

In recent years, the principle of accountability received renewed attention as a means to promote and define organisational responsibility for privacy protection. Building on this experience, the new Part Three of the Guidelines (“Implementing Accountability”) introduces the concept of a privacy management programme and articulates its essential elements.

Paragraph 15(a)(i) specifies that a data controller’s privacy management programme should give effect to the Guidelines “for all personal data under its control”. The term “control” refers back to the definition of a “data controller”, as defined in paragraph 1(a). This formulation emphasises that a privacy management programme should not only address the data controller’s own operations, but all operations for which it may be accountable - regardless of to whom data is transferred. For example, a privacy management programme should include mechanisms to ensure that agents of the data controller maintain appropriate safeguards when processing personal data on its behalf. Safeguards may also be necessary in relationships with other data controllers, particularly where the responsibility for giving effect to the Guidelines is shared. Appropriate safeguards may include: provisions in contracts that address compliance with the data controller’s privacy policies and practices; protocols for notifying the data controller in the event of a security breach; employee training and education; provisions for sub-contracting; and a process for conducting audits.

Paragraph 15(a)(i) refers only to the Guidelines as a source of rules or principles to be implemented through a privacy management programme. In practice, privacy management programmes may need to reflect other sources as well; including domestic law, international obligations, self-regulatory programmes, or contractual provisions.

Paragraph 15(a)(ii) underlines the need for flexibility when putting in place a privacy management programme. For example, large data controllers with locations in multiple jurisdictions may need to consider different internal oversight mechanisms than small or medium sized data controllers with a single establishment. At the same time, paragraph 15(a)(ii) also provides that privacy management programmes should be adapted to the volume and sensitivity of the controller's operations. Programmes for data controllers that deal with large volumes of personal data will need to be more comprehensive than those of data controllers who handle only limited amounts of personal data. The sensitivity of the data controller's operations may also impact the nature of a privacy management programme, as even a very small data controller may handle extremely sensitive personal data.

A recurring element in the discussions about privacy management programmes was the need for such programmes to develop appropriate safeguards based on privacy risk assessment. Paragraph 15(a)(iii) contemplates that the determination of the necessary safeguards should be made through a process of identifying, analysing and evaluating the risks to individuals' privacy. This process is sometimes accomplished by conducting a "privacy impact assessment" before a new programme or service is introduced or where the context of the data use changes significantly. "Risk" is intended to be a broad concept, taking into account a wide range of possible harms to individuals. A privacy management programme can also assist in the practical implementation of concepts such as "privacy by design", whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an afterthought.

Paragraph 15(a)(iv) indicates that privacy management programmes should be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms. Obtaining support and commitment from senior management is a key factor in ensuring the successful implementation of a privacy management programme. Ensuring the availability of sufficient resources and staff, as well as training programmes, may also improve the effectiveness of the programme. Privacy officers may play an important role in designing and implementing a privacy management programme.

Paragraph 15(a)(v) provides that a privacy management programme should also include plans for responding to incidents and inquiries. The increasing frequency of security breaches affecting personal data demonstrates the importance of developing an incident response plan, which includes breach notification (see below). To support the “Individual Participation Principle” in Part Two, data controllers should also be able to provide timely response to inquiries (either in the form of complaints or requests for information) by data subjects. Finally, paragraph 15(a)(vi) stipulates that privacy management programmes should be routinely reviewed and updated to ensure that they remain appropriate to the current risk environment.

Paragraph 15(b) provides that a data controller should be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines. Establishing the capacity and effectiveness of a privacy management programme, even in the absence of a personal data security breach or allegation of non-compliance, enhances the accountability of data controllers. The assessment of the programme may be carried out directly by the privacy enforcement authority or by an agent on its behalf.

Paragraph 15(b) includes the terms “appropriate” and “competent” to highlight that data controllers should be prepared to demonstrate their privacy management programmes at the request of a privacy enforcement authority provided that this authority has jurisdiction over the data controller. The Guidelines do not address legal issues related to jurisdiction, competence and conflicts of law.

A privacy management programme may also be demonstrated to an entity which is responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to Guidelines. Such arrangements may involve seal programmes or certification schemes, and may also concern transborder flows of personal data. In this regard it can be noted that paragraph 21 encourages the development of international arrangements that give practical effect to the Guidelines. The European Union’s Binding Corporate Rules (BCRs) and the APEC Cross-border Privacy Rules System provide two models for developing such an arrangement.

### **Data security breach notification**

The “Security Safeguards Principle” of Part Two states that “Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.” Numerous high-profile data breaches have demonstrated that personal data security continues to be a challenge.

Data breaches can result, for example, from actions by careless employees who fail to follow proper procedures; hackers who gain access to inadequately protected databases; or opportunistic thieves who steal unsecured portable devices. However, the underlying causes – lack of employee training and awareness, out-of-date security safeguards, inadequate rules governing access to personal data, over-collection of data and undefined retention periods, or a lack of adequate oversight – can often be attributed to the data controller.

The potential harm to individuals from the misuse of their personal data, whether accidentally lost or purposefully stolen, may be significant. Organisations experiencing a breach often incur significant costs responding to it, determining its cause, and implementing measures to prevent recurrence. The reputational impact can also be significant. A loss of trust or confidence can have serious consequences for organisations. As a result, the security of personal data has become an issue of great concern to governments, businesses and individuals.

Breach notification laws requiring data controllers to inform individuals and/or authorities when a security breach has occurred have been passed or proposed in many countries. These laws are usually justified on the grounds that data controllers have little incentive to disclose breaches voluntarily, given the possible harm this can cause to their reputation. Requiring notification may enable individuals to take measures to protect themselves against the consequences of identity theft or other harms. Notification requirements may also provide privacy enforcement authorities or other authorities with information to determine whether to investigate the incident or take other action. Ideally, breach notification laws also help to create an incentive for data controllers to adopt appropriate security safeguards for the personal data they hold.

In addition to contributing to data security, data breach notification enhances other basic principles set forth in Part Two of the Guidelines, including accountability, individual participation and openness. Furthermore, mandatory security breach notification may improve the evidence base for privacy and information security policies by generating information about the number, severity and causes of security breaches.

---

2. SUPPLEMENTARY EXPLANATORY MEMORANDUM TO THE REVISED OECD PRIVACY GUIDELINES - 27

Security breaches not only raise privacy concerns, but also intersect with other issues, including criminal law enforcement and cybersecurity. When an organisation suffers a security breach, particularly one resulting from an external attack, notification of the breach to authorities other than privacy enforcement authorities (e.g. computer incident response teams, criminal law enforcement entities, other entities responsible for cybersecurity oversight) may be appropriate or required.

Requiring notification for every data security breach, no matter how minor, may impose an undue burden on data controllers and enforcement authorities, for limited corresponding benefit. Additionally, excessive notification to data subjects may cause them to disregard notices. Accordingly, the new provision that has been added to the Guidelines [paragraph 15(c)] reflects a risk-based approach to notification. Notice to an authority is called for where there is a “significant security breach affecting personal data”, a concept intended to capture a breach that puts privacy and individual liberties at risk. Where such a breach is also likely to adversely affect individuals, notification to individuals would be appropriate as well. To determine whether individuals are likely to be “adversely affected” by a breach, the term “adverse effect” should be interpreted broadly to include factors other than just financial loss. Notification requirements should be flexible to allow for prevention and mitigation of further damage. There may be circumstances where notification to data subjects would be inappropriate, for example when it would increase the risk to data subjects or impede a law enforcement investigation.

Existing breach notification laws differ in terms of the thresholds for notification, the parties to be notified, the timing of the notification, as well as the role of privacy enforcement and other authorities. Further experience may be needed to determine which modalities of breach notification are most effective in practice.

Security breaches may affect the personal data of individuals residing in different jurisdictions. When designing, implementing or revising breach notification requirements, special consideration may be given to the interests of affected individuals who may live outside their jurisdiction. In particular, the notification of privacy enforcement authorities in other jurisdictions where a significant number of individuals are known or likely to have been affected, can be beneficial. Cross-border enforcement cooperation mechanisms are one way to foster arrangements that might support or disseminate breach notifications of importance to multiple jurisdictions. Such arrangements may also help to address issues arising from conflicting legal requirements.

### Privacy enforcement authorities

Neither the 1980 Guidelines nor the 2007 Recommendation explicitly call for the establishment of privacy enforcement authorities, although the latter instrument assumes their existence and recommends their endowment with effective powers and authority. The revised Guidelines define and make explicit the need to establish and maintain “privacy enforcement authorities”. They also incorporate a definition of “laws protecting privacy”, to refer to “national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines”. Both definitions mirror those agreed in the 2007 Recommendation.

The definitions of “laws protecting privacy” and “privacy enforcement authorities” allow for flexibility in application. “Laws protecting privacy” can refer not only to horizontal privacy laws that are common in Member countries, but also to sectoral privacy legislation (e.g. credit reporting or telecommunications laws) or other types of legislation that contain provisions which protect personal data so as to give effect to the Guidelines in practice (e.g. consumer protection laws). Likewise, a “privacy enforcement authority” refers not only to those public sector entities whose primary mission is the enforcement of national privacy laws, but may for example also extend to regulators with a consumer protection mission, provided they have the powers to conduct investigations or bring proceedings in the context of enforcing “laws protecting privacy”.

A new provision in Part Five (“National Implementation”) calls on Member countries to establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an “objective, impartial and consistent basis” [paragraph 19(c)]. This formulation has been adapted from the 2012 OECD Recommendation on Regulatory Policy and Governance (OECD, 2012a). In the context of the Guidelines, it refers to the need for privacy enforcement authorities to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy. There exist a variety of mechanisms across Member countries for ensuring the necessary impartiality of privacy enforcement authorities in the exercise of their privacy protection functions. Paragraph 19(c) focuses on the practical impact of such mechanisms, which should ensure that these authorities can take decisions free from influences that could compromise their professional judgment, objectivity or integrity.

In some countries, the term “privacy enforcement authority” can also refer to a group of bodies that collectively enforce laws protecting privacy. For example, oversight of public sector data controllers may involve multiple bodies from different branches of government, who may also have the authority to issue guidelines or other data usage requirements. The “governance, resources, and technical expertise” called for in paragraph 19(c) may not, in such a case, be embodied in a single entity, but rather be found in the enforcement system as a whole.

The 2007 Recommendation underlined the need for privacy enforcement authorities to be endowed with the resources and authority necessary 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; and (c) permit corrective action to be taken against data controllers engaged in violations of laws protecting privacy. The resources of privacy enforcement authorities should be commensurate with the scale and complexity of data processing operations subject to their oversight. The new provision also calls for empowering privacy enforcement authorities with sufficient technical expertise, which has become crucial in light of the increasing complexity of data uses. This reinforces the emerging trend within privacy enforcement authorities to retain staff with a technical background.

### **Transborder flows of personal data**

When the 1980 Guidelines were drafted, data flows largely constituted discrete point-to-point transmissions between businesses or governments. Today, data can be processed simultaneously in multiple locations; dispersed for storage around the globe; re-combined instantaneously; and moved across borders by individuals carrying mobile devices. Services, such as “cloud computing”, allow organisations and individuals to access data that may be stored anywhere in the world.

The 1980 Guidelines presumed that data flows should generally be allowed, but recognised the ability of governments to restrict them in certain circumstances, namely where the receiving country “does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation.” Since then, Member countries have instituted a range of mechanisms to ensure the protection of individuals in the context of transborder data flows. Some of these mechanisms include a country-specific assessment, such as the “adequacy model” adopted within the European Union. Other mechanisms are not based on a country-specific assessment, but are instead based on the safeguards put in place by data controllers. Such mechanisms include, for example, Binding Corporate Rules, model contracts, and Cross-Border Privacy Rules.

The revisions reflected in Part Four attempt to simplify and consolidate the OECD approach to transborder flows of personal data. It begins by recalling that a data controller remains accountable for personal data under its control without regard to the location of the data [paragraph 16]. This paragraph restates the basic principle of accountability contained in Part Two in the context of transborder data flows. Transborder flows of personal data, to Member countries or non-Member countries, present risks, which data controllers must address. Some data flows may require close attention because of the sensitivity of the data or because the receiving jurisdiction may lack either the willingness or capacity to enforce privacy safeguards.

Without precluding the application of paragraph 6, paragraph 17 specifies two circumstances in which a Member country should refrain from imposing restrictions on transborder flows of personal data. Paragraph 17(a) retains the general approach from the 1980 Guidelines, by providing that Member countries should refrain from restricting transborder data flows between itself and another country where the other country substantially observes these Guidelines. Paragraph 17(b) discourages restrictions where sufficient safeguards exist to ensure a continuing level of protection consistent with these Guidelines. It gives recognition to the measures which a data controller can put in place to ensure a continuing level of protection, which may result from a combination of measures, such as technical and organisational security safeguards, contracts, complaint handling processes, audits, etc. However, the measures provided by the data controller need to be sufficient and supplemented by mechanisms that can ensure effective enforcement in the event these measures prove ineffective. Paragraph 17(b) therefore includes as a consideration the availability of effective enforcement mechanisms which support measures adopted by the data controller. Such enforcement mechanisms may take a variety of forms, including for example, administrative and judicial oversight, as well as cross-border co-operation among privacy enforcement authorities.

Paragraphs 16 and 17 operate independently. The existence or absence of country restrictions on data flows adopted pursuant to paragraph 17 does not, as such, affect the operation of the principle embodied by paragraph 16, namely that data controllers remain accountable for personal data under their control, including in the context of transborder flows.

Paragraph 18 updates the language in the 1980 Guidelines to refer to “risk” and “proportionality”, indicating that any restrictions upon transborder data flows imposed by Member countries should be proportionate to the risks presented (i.e. not exceed the requirements necessary for the protection of personal data), taking into account the sensitivity of the data, the purpose and context the processing. In doing so, the text has been made more coherent with other provisions of the Guidelines, which implement a risk-based approach.



Paragraph 6 of the Guidelines acknowledges that Member countries have the ability to supplement the standards set forth by the Guidelines with additional measures necessary for the protection of privacy and individual liberties, which may impact transborder flows of personal data. Such measures should be implemented in a manner that least impacts the free flow of personal data.

### **National implementation**

Regarding national implementation, the 1980 Guidelines focused on the need for “legal, administrative and other procedures or institutions”. Although the 1980 Guidelines also highlighted non-regulatory measures, including self-regulation, it was recognised that there is a need for additional measures to help to protect privacy.

Paragraph 19(a) recommends that Member countries develop national privacy strategies that reflect a co-ordinated approach across governmental bodies. Elevating the importance of privacy protection to the highest levels within government helps improve the effectiveness of privacy protection. A further element of national privacy strategies concerns intra-governmental co-ordination. As highlighted in the OECD Recommendation on Regulatory Policy and Governance, Member countries should promote regulatory coherence between various levels of government. Where governments act as a policy maker for private sector activity, ensuring co-ordination across governmental departments is a necessary part of a national strategy. In addition, with many government departments making use of personal data, another dimension of co-ordination is to ensure a consistent level of protection across governmental bodies. Finally, national privacy strategies also offer a vehicle to ensure compatibility of policy development in related areas (e.g. national cybersecurity strategies).

Paragraph 19(g) calls upon Member countries to consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy. While existing initiatives attempt to raise awareness, there is broad recognition that more needs to be done. The Terms of Reference for the review of the Guidelines called for the creation of a culture of privacy among organisations and individuals through implementation of privacy literacy initiatives. Recent OECD instruments in related areas include measures for education and awareness as part of their policy frameworks.<sup>5</sup> Such initiatives should involve a wide range of stakeholders, including governments, privacy enforcement authorities, self-regulatory bodies, civil society organisations, and educators. As children are a particularly vulnerable category of data subjects, Member countries are specifically

encouraged to consider privacy literacy initiatives which seek to equip children with the knowledge and skills necessary to stay safe online and use the Internet to their benefit.

Privacy professionals play an increasingly important role in the implementation and administration of privacy management programmes. Several Member countries have already undertaken initiatives to define the competencies of privacy professionals. Credential programmes in data protection and privacy, as well as specialised education and professional development services may contribute to the development of the necessary skills. Paragraph 19(g) explicitly encourages Member countries to consider the adoption of measures to support such skills development.

Technical measures also play an increasingly important role in complementing laws protecting privacy. Paragraph 19(g) encourages measures to foster the development and deployment of privacy-respecting and privacy-enhancing technologies (PETs). For example, Member countries may choose to support the development of technical standards which advance privacy principles. International standardisation initiatives may also advance technical interoperability among PETs, which may in turn help promote wider adoption of these technologies. Accreditation and seal programmes may further foster the adoption of technologies beneficial to privacy. Other measures include the promotion of research and development, exchange of best practices, and the issuance of regulatory guidance.

Paragraph 19(h) invites Member countries to consider the role of actors other than data controllers, “in a manner appropriate to their individual role”. When discussing the need for complementary measures, it was recognised that other actors who, while not covered by the concept of data controller, nevertheless play an important role in determining the level of protection of personal data. Over the past few years, individuals have transcended the role of passive “data subjects” to become actively involved in creating, posting and sharing personal data about themselves, friends, relatives and others, over a vast array of information outlets including social networking services, rating systems and geo-location based applications. When discussing this change, it was recognised that not every actor should necessarily be regulated in the same way. For example, individuals acting in the context of their private lives are generally perceived to fall outside the remit of the Guidelines, as relationships among individuals are usually fundamentally different from those between individuals and organisations. Non-legislative measures, including education and awareness raising, were considered more appropriate to address the privacy risks associated with the activities of individuals. Where an individual does cause damage to the privacy interests of others, tort or civil law may offer a possible remedy, but other measures may need to be considered as well.

### **International co-operation and interoperability**

The OECD Recommendation on Internet Policy Making calls for a strengthening of consistency and effectiveness in privacy protection at a global level. The Communiqué which is annexed to it for information purposes further recognises the objective of governments to pursue global interoperability in this area. The Terms of Reference similarly identified the value of globally interoperable privacy frameworks that ensure effective protection of privacy and support the free flow of personal information around the world. However, as outlined by the G8 Deauville Declaration, we still “face considerable challenges in promoting interoperability and convergence among our public policies on issues such as the protection of personal data” (G8, 2011).

Paragraph 21 expresses the general objective of Member countries to improve global interoperability of privacy frameworks through international arrangements that give practical effect to the Guidelines. There exists a range of approaches to interoperability among privacy frameworks. The US-EU Safe Harbour Framework<sup>6</sup>, which was adopted under the EU adequacy regime and implemented in 2000, was an early example. Since then, several initiatives have been undertaken to bring together different approaches and systems of protection, including work by the privacy enforcement authorities within the framework of the EU Binding Corporate Rules and the APEC Cross-Border Privacy Rules System within the Asia-Pacific region. At the time of publication of these revised Guidelines, the Council of Europe continues its deliberations on the modernisation of Convention 108 on the Automated Processing of Personal Data. Further work is needed at the policy level towards a more seamless approach to global privacy governance.

A strong global network of privacy enforcement authorities working together is a first important step towards global interoperability. In 2005, the OECD revisited the issue of global cooperation among privacy enforcement authorities, resulting in the adoption of a new framework for cross-border co-operation in the form of the 2007 Recommendation. The three-year implementation report for the 2007 Recommendation highlighted the need for further efforts to ensure that privacy enforcement authorities have sufficient powers to administer effective sanctions and resources to accomplish their mission.<sup>7</sup> The Terms of Reference for the review of the Guidelines called for a redoubling of efforts to develop a globally active network of privacy enforcement authorities. Paragraph 20 reiterates the commitment expressed by Member countries in the 2007 Recommendation to enhance co-operation between privacy enforcement authorities. In particular, Member countries are encouraged to address obstacles – be they

legal or practical – towards information sharing among privacy enforcement authorities to facilitate coordinated and effective enforcement. Reducing the barriers to information sharing has been a particular concern in this respect.

Improving the global interoperability of privacy frameworks raises challenges but has benefits beyond facilitating transborder data flows. Global interoperability can help simplify compliance by organisations and ensure that privacy requirements are maintained. It can also enhance individuals' awareness and understanding of their rights in a global environment.

### **Improving the evidence base for policy making**

The OECD Recommendation on Internet Policy Making calls for the development of capacities to bring publicly available, reliable data into the policy-making process. The Communiqué, annexed to it for information, specifically notes the value of internationally comparable metrics.

The evidence base which is currently available for policymaking in the area of privacy is uneven. Household surveys by national statistical agencies provide some insight into privacy issues on the basis of internationally comparable metrics. However, the scope of these surveys, which focus primarily on awareness issues among individuals, is limited. There are gaps, for example, related to the technical or economic dimensions of privacy, as well as the implementation of prevention measures. Privacy enforcement authorities gather considerable data that are made public through annual reports, but not in a format well-suited to international comparisons. For example, progress in understanding complaint data, data breach statistics, and how fines and other sanctions influence data controllers' behaviour could be a potentially rich source of insight for policy makers. The addition of paragraph 22 in Part Six identifies the need for Member countries' support for initiatives to improve the evidence base in this area.

### **Other updates**

In addition to the substantive changes discussed in the previous section, the revised Guidelines reflect several minor changes which were made either to enhance readability or otherwise update the language of the 1980 Guidelines.

As a general matter, all references to specific parts of the Guidelines, have been replaced by a more generic phrasing (“these Guidelines”).

Paragraph 2, which specifies the scope of the Guidelines, now refers to a “risk” rather than “danger” to privacy and individual liberties, reflecting the increased emphasis on risk within the revised Guidelines. This change should not be construed as preventing Member countries from extending the scope of laws protecting privacy or other privacy regimes to all forms of processing of personal data.

Former paragraph 3(b) has been deleted, as the ability for Member countries to exclude from the application of the Guidelines “personal data which do not pose any risk to privacy and individual liberties” is already reflected in paragraph 2.

Former paragraph 3(c) has been deleted, as Member countries have generally extended the scope of their domestic privacy laws to include the processing of personal data in general.

A new paragraph 3(b) has been added, to recognise the potential conflict between the protection of privacy and other fundamental rights arising from the now ubiquitous nature of personal data processing. It is also in line with the Communiqué on Principles for Internet Policy Making (OECD, 2011g) which underlines that “[p]rivacy rules should also consider the fundamental rights of others in society including rights to freedom of speech, freedom of the press, and an open and transparent government”.

Former paragraphs 15 and 16 of the 1980 Guidelines were removed in the interests of clarity and to avoid repetition, as the commitment of Member countries to the global free flow of information and security is already underlined elsewhere in the Recommendation.

### *Notes*

1. Remarks from Hon. Michael Kirby on the 30th anniversary of the OECD Privacy Guidelines, [www.oecd.org/internet/interneteconomy/49710223.pdf](http://www.oecd.org/internet/interneteconomy/49710223.pdf).
2. The system of BCRs is being further developed, see [http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm)
3. See [www.huntonfiles.com/files/webupload/CIPL\\_Galway\\_Conference\\_Summary.pdf](http://www.huntonfiles.com/files/webupload/CIPL_Galway_Conference_Summary.pdf).
4. APEC, APEC Cross-border Privacy Rules System – Policies, rules and guidelines, [www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx](http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx)
5. E.g., OECD (2002), OECD (2012b).
6. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, Official Journal of the European Communities, 25 August 2000, L-215, 7-47. See also [www.export.gov/safeharbor](http://www.export.gov/safeharbor).
7. See OECD (2011f).

### *References*

- G8 (2011), Deauville Declaration: Internet,  
[www.g8.utoronto.ca/summit/2011deauville/2011-internet-en.html](http://www.g8.utoronto.ca/summit/2011deauville/2011-internet-en.html)
- OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards A Culture Of Security,  
[www.oecd.org/internet/interneteconomy/15582260.pdf](http://www.oecd.org/internet/interneteconomy/15582260.pdf)
- OECD (2007), Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy,  
[www.oecd.org/internet/interneteconomy/38770483.pdf](http://www.oecd.org/internet/interneteconomy/38770483.pdf).
- OECD (2011a), Council Recommendation on Principles for Internet Policy Making [www.oecd.org/internet/interneteconomy/49258588.pdf](http://www.oecd.org/internet/interneteconomy/49258588.pdf).
- OECD (2011b), Communiqué on Principles for Internet Policy Making [www.oecd.org/internet/interneteconomy/49258588.pdf](http://www.oecd.org/internet/interneteconomy/49258588.pdf).
- OECD (2011c), “The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines”, *OECD Digital Economy Papers*, No.176,  
<http://dx.doi.org/10.1787/5kgf09z90c31-en>.
- OECD (2011d), “Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy”, *OECD Digital Economy Papers*, No. 178,  
<http://dx.doi.org/10.1787/5kgdpm9wg9xs-en>.
- OECD (2011e), “Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data,” [www.oecd.org/sti/interneteconomy/48975226.pdf](http://www.oecd.org/sti/interneteconomy/48975226.pdf)
- OECD (2011f), “Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy”, *OECD Digital Economy Papers*, No. 178,  
<http://dx.doi.org/10.1787/5kgdpm9wg9xs-en>
- OECD (2011g), Council Recommendation on Principles for Internet Policy Making, [www.oecd.org/internet/interneteconomy/49258588.pdf](http://www.oecd.org/internet/interneteconomy/49258588.pdf)
- OECD (2012a), Recommendation of the Council on Regulatory Policy and Governance, [www.oecd.org/gov/regulatorypolicy/49990817.pdf](http://www.oecd.org/gov/regulatorypolicy/49990817.pdf)
- OECD (2012b), Recommendation of the Council on the Protection of Children Online,  
<http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False>.