OECD publishing

Please cite this paper as:

OECD (2011-04-27), "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, OECD Publishing, Paris.
http://dx.doi.org/10.1787/5kgdpm9wg9xs-en

OECD Digital Economy Papers No. 178

Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy

OECD

OECD Directorate for Science, Technology and Industry

Report on the Implementation of the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy

2011

FOREWORD

In 2007, the OECD Council adopted the *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (the Recommendation). The Recommendation instructs the Committee for Information, Computer and Communications Policy (ICCP) to exchange information on progress and experiences with respect to the implementation of the Recommendation, review that information, and report to Council within three years of its adoption

This report describes Members' progress in implementing the Recommendation. It was prepared by the ICCP Committee's Working Party on Information Security and Privacy (WPISP) for submission to the OECD Council, which agreed to declassify the report in April 2011. For ease of reference, the Recommendation is reproduced as an Appendix.

The report is published under the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

REPORT ON THE IMPLEMENTATION OF THE OECD RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY

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 law enforcement co-operation among privacy enforcement authorities.

In 2007, the OECD Council adopted a *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*[1] (the Recommendation; see Appendix II) setting forth a framework for co-operation in the enforcement of privacy laws. This report provides information on the progress in implementation measures, which is based in part on a survey of Members' experiences.

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

- One key implementation initiative has been the creation in March 2010 of a new network for privacy enforcement co-operation – the Global Privacy Enforcement Network (GPEN). Launched at a meeting at the OECD by the 11 founding members of the Network, GPEN has expanded quickly and now includes 22 authorities from 16 OECD Members, 2 non-members (Guernsey and Bulgaria), and the European Union. The OECD developed and hosts the website 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 23 Members, and will be shared with authorities based outside the OECD through other international organisations. As a first and important step, OECD and APEC have recently agreed to exchange their contact lists.

- 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 form as has also been adapted for use by authorities from Asia Pacific Economic Cooperation (APEC) economies under a 2009 APEC cooperation arrangement.

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 have recognised the importance of improvements in this area and are working to develop mechanisms to better share information.

Continued and strengthened 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.

I. Introduction

As the OECD marks the 30th anniversary[2] of its 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Privacy Guidelines), virtually all OECD Members 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.[3]

The 1980 Guidelines are well known for their eight principles for the collection and handling of personal data, but they also call for Members' 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,[4] and emphasised again in 2003 in an OECD report calling for Members to establish procedures to improve bilateral and multilateral mechanisms for cross-border co-operation by privacy authorities.[5]

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,[6] the OECD released a Report on the Cross-border Enforcement of Privacy Laws in October 2006.[7] 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 the Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy[8] (the Recommendation) 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[9] and cross-border fraud.[10]

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 Members' implementation efforts, reflecting the replies of 25 Members to a written questionnaire circulated in November 2009.

II. Implementation activities supported by OECD

Although primary responsibility for implementation of the Recommendation rests with Member 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 information on national 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, 23 Members 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 advanced 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 has also been identified as 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. As a first and important step, OECD and APEC recently agreed to exchange their contact lists. 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.[11] It was also recognised that the process of completing the Form can 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 Members 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."[12]

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 22 authorities from 17 countries, including Australia, Bulgaria, Canada, Czech Republic, France, Germany, Ireland, Israel, Italy, the Netherlands, New Zealand, Poland, Slovenia, Spain, Switzerland, the United Kingdom (including Guernsey), 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 OECD 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 a website, 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 report of the proceedings identified a number of key themes emerging from the Roundtable, including that by working together authorities and professionals can help make the application of privacy laws more predictable for organisations and beneficial to individuals.[13]

III. 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 co-operate 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. Japan reviewed its policy for international co-operation for personal information protection as part of a 2008 review of its "Basic Policy on the Protection of Personal Information (Cabinet Decision)."[14] Reviews of the privacy frameworks are currently underway in a number of other countries, including Australia, 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.[15] The importance of this co-operation is highlighted in a 2010 opinion on applicable law by the EU Article 29 Data Protection Working Party which notes that cross-border co-operation between national data protection authorities within Europe is particularly important in cases where the applicable law and the competence of the supervisory authorities do not coincide.[16]

While it is too early to know the final 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.[17]

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 United Kingdom 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.[18] 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 to their ability to co-operate. Legal limitations on the ability to share information with foreign authorities remain an issue in some countries. The limitations for the Canadian Commissioner to share information with foreign authorities have been removed under the new Canadian Fighting Internet and Wireless Spam Act (FISA), which passed into law on 15 December 2010.[19] For others who previously reported information-sharing limitations the situation however 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 Members 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.[20] The Canadian FISA requires that the Privacy Commissioner, the Commissioner of Competition and the Canadian Radio-television and Telecommunications Commission (CRTC) consult with each other to ensure that activities such as spamming are controlled under the complimentary provisions in the Acts for which each of them has responsibility.[21] There is however also the need to define how the co-operation between privacy enforcement authorities and accountability agents can be improved, since their role in compliance is becoming increasingly important (see for example the APEC Privacy Framework).

IV. 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, for example, reports that it has only investigated 10-15 complaints with a cross-border dimension in nearly 10 years. New Zealand had only two cross-border complaints last year. The US FTC reports that in its 2009 econsumer.gov cross-border e-commerce complaints database, more than 900 instances of unauthorized use of identity/account information were reported.[22]

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.[23] The FTC had already brought an enforcement action against this company for violations of the FTC Act.[24] 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.[25] The second investigation concerned traffic data retention.[26] In 2010 the Article 29 Working Party has also sent collective letters to search engines regarding their compliance with European law.[27]

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.[28]

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.

V. 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.[29] 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.[30] 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 (Australia), Victoria (Australia), Canada, British Columbia (Canada) 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.[31] 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.[32] 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 trans-border accessibility and the APPA has selected the WorldLII Privacy Law Library (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.[33]

VI. 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 Members 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 Members 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 Members 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

[2] See www.oecd.org/sti/privacyanniversary

[3] See www.oecd.org/futureinternet

[4] Declaration on the Protection of Privacy on Global Networks, 7-9 October 1998, Ottawa Canada. See www.oecd.org/dataoecd/39/13/1840065.pdf

[5] OECD, "Privacy Online: OECD Guidance on Policy and Practice, p. 18-19, available at: www.olis.oecd.org/olis/2002doc.nsf/LinkTo/NT000029C6/$FILE/JT00137976.PDF

[6] Available at www.oecd.org/dataoecd/5/30/37572050.pdf

[7] Available at www.oecd.org/dataoecd/17/43/37558845.pdf

[8] Available at www.oecd.org/dataoecd/43/28/38770483.pdf

[9] See www.oecd.org/document/24/0,3343,en_2649_34255_34804568_1_1_1_1,00.html

[10] See www.oecd.org/dataoecd/24/33/2956464.pdf

[11] Available at: www.oecd.org/dataoecd/43/58/38772442.doc

[12] See https://www.privacyenforcement.net/public/activities

[13] www.oecd.org/dataoecd/37/21/41246826.pdf

[14] See www.caa.go.jp/seikatsu/kojin/foreign/basic-policy-tentver.pdf.

[15] 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.

[16] See http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf, p.10.

[17] See www.privacy.org.nz/updated-media-release-30-8-10-privacy-amendment-important-for-trade-and-consumer-protection/.

[18] 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.

[19] See http://www2.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c28-e.pdf, p.13.

[20] 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.

[21] See http://www2.parl.gc.ca/Content/LOP/LegislativeSummaries/40/3/c28-e.pdf, p.13.

[22] Econsumer.gov is an initiative managed by the FTC that enables government agencies around the world to gather and share cross-border e-commerce complaints. Currently 25 countries participate. The public website of econsumer.gov allows consumers to lodge cross-border complaints, and to try to resolve their complaints through means other than formal legal action. Using the Consumer Sentinel network (a database of consumer complaint data and other investigative information operated by the U.S. Federal Trade Commission), the incoming complaints are shared with participating consumer protection law enforcers. See www.econsumer.gov.

[23] See www.priv.gc.ca/cf-dc/2009/2009_009_*rep_0731_e.cfm*

[24] 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)

[25] 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.

[26] 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 .

[27] http://ec.europa.eu/justice/policies/privacy/news/docs/pr_26_05_10_en.pdf.

[28] See www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm.

[29] See www.privacy.gov.au/aboutus/international/nz

[30] See www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce/cpea.html.

[31] See www.oecd.org/dataoecd/17/43/37558845.pdf

[32] 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.

[33] See www.privacyconference2010.org/upload/2009-4.pdf.

APPENDIX

RECOMMENDATION OF THE COUNCIL ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY [C(2007)67/FINAL]

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.