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

16-Oct-2006

English - Or. English

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

DSTI/ICCP/REG(2006)8/FINAL
Unclassified

Working Party on Information Security and Privacy

REPORT ON THE CROSS-BORDER ENFORCEMENT OF PRIVACY LAWS

JT03215940

English - Or. English

FOREWORD

More than 25 years after the adoption of the OECD 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 been evolving, elevating privacy risks, and raising cross-border enforcement challenges. This report describes the current attempts to address these challenges and highlights the need for a more global and systematic approach to cross-border privacy law enforcement co-operation.

The report was prepared by the Secretariat with the assistance of Francis Aldhouse, Malcolm Crompton, and Peter Ford, consultants. It was reviewed by a volunteer group of experts led by Jennifer Stoddart, Privacy Commissioner of Canada. 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 October 2006.

The report is published under the responsibility of the Secretary-General of the OECD and available online at: www.oecd.org/sti/security-privacy.

MAIN POINTS

The volume and characteristics of cross-border data flows are evolving, elevating privacy risks and the need for improved law enforcement co-operation

Developments in global communication networks and business processes have increased the volume of transborder data flows. Data transfers in areas like human resources, financial services, education, e-commerce and health research – to name a few – are now an integral part of the global economy. Advances in technology mean that data can be transferred quickly and stored indefinitely. Data transfers enable a globally distributed approach to tasks which takes advantage of expertise in multiple locations around the world and around the clock.

In addition to bringing business efficiencies and convenience for users, however, changes to global data flows have also elevated the risks to privacy. Wrong-doers seek to exploit technology to expose data, sometimes for financial gain. In particular, problems related to data security breaches have come into focus recently, sometimes in cases with a cross-border dimension. Given the ease with which information can be instantly transferred at anytime to any place, the cross-border aspect of data breaches is likely to increase. As with spam and cross-border fraud, protecting privacy in a global environment depends on cross-border co-operation. Although the need for effective enforcement co-operation has been noted over the years, there is now renewed interest in working at the international level to address the outstanding challenges to effective law enforcement in a world where global data flows are widespread and continuous.

Privacy enforcement authorities are now widespread in OECD countries, sharing commonalities in the types of powers they possess and the substantive scope of their jurisdiction

When the OECD Privacy Guidelines were adopted more than 25 years ago, only about one-third of member countries had privacy legislation. Today nearly all OECD members have laws – most of which follow the principles of the *Privacy Guidelines* – and have established authorities to carry out enforcement responsibilities.

If member country authorities share commonalities in terms of the powers they have and the scope of the laws they enforce, certain variations remain. Some authorities are charged with resolving individual complaints, others with supervising regulatory compliance, and many do both. Variations exist with respect to complaint handling processes, the authority to investigate or audit, and the available sanctions and remedies for a breach. Some are independent authorities, some housed within government departments. Some cover the public sphere, others only the private sector, and many cover both. A few authorities are mandated to enforce privacy laws covering a particular economic sector, for example, telecommunications or financial services.

Privacy enforcement authorities face challenges in addressing cross-border cases

Although almost all authorities can act against a domestic data controller for the benefit of a foreign individual, many are limited in or uncertain about their authority to protect their own citizens from privacy breaches by a foreign controller. A majority indicate that they would benefit from improved powers to exchange information and carry out investigations either jointly with or at the request of a foreign authority. Finally, efforts by authorities in the cross-border context are sometimes limited by insufficient preventive or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints.

A number of regional instruments and other less formal arrangements already exist to facilitate cross-border enforcement co-operation, but none with a global reach.

Work by the Council of Europe, the European Union, and APEC has helped establish frameworks for enforcement co-operation among enforcement authorities on a regional basis. One result has been a recent move towards joint audit activity in Europe. More informal networking and information exchange occurs at the International Conference of Data Protection and Privacy Commissioners, Asia Pacific Privacy Authorities Forum, the International Working Group on Data Protection in Telecommunications, and the Iberoamerican Network of Data Protection. Co-operation among privacy enforcement authorities can also occur under a recently adopted OECD Recommendation on anti-spam law enforcement co-operation. Existing arrangements are not, however, sufficiently comprehensive or globally co-ordinated to adequately address the cross-border enforcement challenges.

There is considerable scope for a more global and systematic approach to cross-border privacy law enforcement co-operation

Privacy is an area where public perceptions and fears can shift rapidly. The twin goals of the 1980 OECD *Guidelines* – protecting privacy and individual liberties, while avoiding the creation of unjustified obstacles to transborder flows of personal data – remain relevant today. Indeed, they may now be seen as more so given the growth in the volume of data crossing borders. An important element in maintaining that balance is having in place a framework allowing for co-operative enforcement actions to address problems when they do arise. In addition, greater transparency about how privacy enforcement works would be helpful for business compliance and user trust in global privacy protection. The overall goal of any effort to improve enforcement co-operation should be to safeguard the personal information of individuals, no matter where it is located.

TABLE OF CONTENTS

INTRODUCTION: TRANSBORDER DATA FLOWS, PRIVACY RISKS, AND LAW ENFORCEMENT CO-OPERATION

The challenge of ensuring the protection of personal information when it crosses national borders is by now well known. The history of efforts to address privacy protection at the international level dates back to at least the late 1970s when the OECD and Council of Europe launched their landmark work in the area. While much has been accomplished during the intervening years to increase privacy protection across the world, the growth of the Internet and related changes in the volume and characteristics of global flows of personal data have heightened privacy risks. These developments highlight the need for more structured enforcement co-operation globally to ensure privacy protection.

This report examines the law enforcement authorities and mechanisms that have been established to protect privacy, with a particular focus on how they operate in the cross-border context. It describes the current challenges to effective enforcement, as well as existing arrangements for addressing those challenges. It concludes by identifying a number of issues for further consideration, aimed at helping those charged with enforcing privacy laws to protect personal information wherever it may be located.

A. International frameworks for privacy protection

The OECD Privacy Guidelines were developed because of concerns about the consequences of competing national data protection laws. One aim was to ensure that the spread of national data protection laws should not cut off transborder data flows to the prejudice of economic growth. At the same time the *Guidelines* emphasised that OECD countries have a common interest in protecting privacy and individual liberties. Faced with the twin concerns about threats to personal privacy by the more intensive use of personal data and the risk to the global economy of restrictions on the flow of information, the OECD produced what has come to be recognised as one of the principal statements of the core privacy protection principles.

The adoption of the OECD *Privacy Guidelines* in 1980[1] represented a significant step in the international protection of personal privacy. The 1981 Council of Europe Convention[2] (Convention 108) and subsequently, the European Union Directive 95/46/EC (the EU Directive) marked further stages in the development of privacy law and policy. In particular, the EU Directive developed rules to ensure that the standard of privacy protection afforded within Europe was not weakened by the transfer of data between Europe and other countries. In 1990, the United Nations General Assembly adopted guidelines that reflect the principles to be found in the OECD *Guidelines* and Convention 108, but with a greater human rights emphasis.[3] More recently, the Asia Pacific Economic Cooperation economies (APEC) have finalised the APEC Privacy Framework. It introduces an approach focused on the prevention of harm from the misuse of personal information along with a principle of accountability where data moves across borders. The Framework was endorsed by APEC Ministers in 2004.[4]

B. Open economies and communications networks

Changes in global information flows

Continuous technical innovation and societal evolution in the Internet environment have changed the landscape for global communications and information flows. When the OECD *Privacy Guidelines* were adopted in 1980, cross-border flows of personal data could be considered discrete events, with data travelling in bulk between identified parties. Data transfers would occur, for example, in large batches by means of physical devices like tapes for processing. International data banks were just emerging, and the Internet was still in its infancy with commercial usages prohibited.

Precise estimates of today's volume of information flowing across borders are hard to come by, but related data is instructive. The overall number of Internet users is now approaching 1 billion, with the penetration of broadband subscribers having quadrupled between 2001 and 2005.[5] Capacity for international Internet traffic continues to grow, with, for example, capacity in hubs like San Francisco or Tokyo more than doubling between 2002 and 2003, and nearly doubling again in 2004.[6] Likewise, the prices for international transit have dropped dramatically, with some estimating that what might have cost USD 1 000 per Mbps per month in 1995 may cost USD 15 per Mbps per month in 2005.[7] Though not a direct measure of the volume of transborder data flows, these figures help illustrate an inter-connected world where information flows are fluid and decentralised, and cross-border data exchange is routine. Moving data around the world or across the corridor now requires the same "click".

This major feature of today's environment has been emphasised by several commentators. Information "flows more freely, knows fewer national attachments, and indeed represents one of the significant forces behind the processes of globalisation," according to one.[8] For another, information "has become the new raw material of the world economy."[9] Or, as described in the US-EU Safe Harbour materials, "[d]ata transfers are the life blood of many organizations and the underpinnings for all of electronic commerce. Multinational organisations routinely share among their different offices a vast array of personal information."[10] And indeed, more and more business, government and individual activities are migrating to the global "always on" broadband IP-based networks. Cross-border flows of personal data occur for any number of reasons: e-commerce, e-government, online banking, human resources management, distance education, online gambling, community activities or health research – to name a few areas.

Individuals routinely connect with others around the world, share profiles and preferences, blog, rate music and buy from other individuals on online auction sites.[11] They make purchases and travel arrangements with foreign businesses over the Internet. Sophisticated financial networks and messaging services facilitate the use of credit and debit cards throughout the world. Multinationals transfer personal information about their customers and employee records across borders. Governments increasingly provide for the electronic delivery of government services to both improve their internal operations and offer better services to the private sector and to citizens. Governments also exchange personal information for various reasons, such as border control.

Organisations have updated their businesses processes, managing their operations wherever it makes the most sense. A number of different agents may participate in the collection and transfer of data, sometimes on behalf of the company, sometimes in the name of another party. Formerly centralised functions like payment processing, credit verification, customer service, or technical support can be distributed globally to take advantage of expertise across multiple locations. The outsourced processing of credit card transactions, telephone bills, and medical records to offshore sites to take advantage of lower costs and specialised expertise is frequent. Many businesses have established offshore customer service centres to respond to the expectations of their customers that assistance should be available "real time." Responding to inquiries 24/7 may mean moving data to some place where it is normal working hours for support personnel, in line with a "follow the sun" model.

Looking ahead, cable, telecommunication and mobile networks are converging towards the Internet Protocol (IP) - next-generation networks (NGN) to enable voice, video and data to be carried over the same infrastructure. The deployment of networked RFIDs and sensors may soon make communications channels even more pervasive, fostering further exponential growth in round-the-clock data flows.[12]

Changes in privacy risks

As information and communications networks grow in size, sophistication and capabilities, and allow far greater business efficiencies and convenience for users, they also bring changes in privacy risks for individuals and organisations. One risk is related to the growth of transborder data flows in itself. Larger volumes of cross-border flows at higher speeds, reaching broader geographical areas, transferring alpha-numeric, voice and image data among an ever-greater multiplicity of actors is likely to increase the number and cost of privacy breaches borne by individuals and organisations. This change in scale could – should a "Tipping Point"[13] be reached – lead to a loss in individual user trust and a consequent change in behaviour.[14] According to a poll conducted for VISA of consumers in 12 countries, the single issue causing individuals the greatest fear is the loss or theft of personal or financial information, an issue selected from a list that included disease, natural disaster, terrorism, protecting the environment, and loss of employment.[15] Although in many cases reports of consumer fears do not seem to be accompanied by behavioural change, one should not underestimate the risk that elevated privacy breaches could jeopardise efforts to strengthen trust on line and hinder the continued growth of the digital economy. Already, studies suggest that consumer interest in online banking may be dropping because of concerns about misuse of personal information,[16] and that upon learning about a security breach many consumers will elect to take their business elsewhere.[17]

Beyond the scale-related risks, and more specifically, two categories of privacy risks tend to prevail, both the result of the evolving technological landscape: *i*) the risks related to secondary uses of personal data; and *ii*) the risks related to information security breaches. With respect to secondary usage, it has never been easy for individuals to monitor how organisations use their data, but the ease and frequency with which organisations process data today exacerbates the challenge. As Professor Peter Swire recently pointed out, we are now in an environment where unprecedented quantities of personal information are being instantly transferred between computers. If consumers cannot monitor the sale of their data effectively, then businesses have incentives to "over-use" the personal data, for example, by selling it for profit.[18] In March of 2006, an enforcement action was brought against an US-based Internet company for selling personal information obtained from millions of individuals despite a promise of confidentiality in the Web site's privacy policy.[19]

The second area of increased risk relates to the growing number of data security breaches which are publicly reported. In Japan, the Cabinet Office reported that the number of personal information breach cases publicly announced by organisations in 2005 exceeded 1 500.[20] Certainly, public attention to these breaches is increasing, in part because of an increase in mandatory reporting laws.[21] Not all data breach incidents result in financial or related losses to individuals, but in a number of cases the harm has been significant. One of the largest reported cases involved a US-based payment card processor, CardSystems Solutions, which settled charges by the US Federal Trade Commission (FTC) that its failure to take appropriate security measures to protect the sensitive information of tens of millions of consumers resulted in millions of dollars in fraudulent purchases.[22] The impacts of this breach spilled over into other countries, and in particular to Japan where tens of thousands of payment cards were compromised by the CardSystems breach, resulting in an estimated loss of JPY 110 million.[23] The CardSystems case followed on the heels of a breach involving consumer data broker ChoicePoint that resulted in the compromise of personal financial records of more than 163 000 individuals and at least 800 cases of identity theft.[24] An extensive catalogue of data breaches is maintained by the Privacy Rights Clearinghouse, which estimates that some 90 million records have been compromised since the ChoicePoint incident.[25] However, given that organisations do not usually find it advantageous to publicise their security breaches, the scale of the problem may not be known.[26]

Although it is likely that a number of privacy breach cases have impacts beyond the borders of the country in which the breach is reported, the cross-border dimensions are not often noted by the authorities

or in the press. Nevertheless, other cross-border breach incidents have been reported. One example involves a Canadian company that recently announced that it had lost a computer with the names and social security numbers of 1.3 million American students.[27] Other examples arise in the context of offshore outsourcing. In 2005, media reports indicated that the identities of customers could be easily bought from call centres operated for UK banks in India.[28] June 2006 brought reports of cross-border data breaches in the United Kingdom involving the data of 2 500 US employees.[29] In the same month, police in India arrested an employee of the customer service centre of a multinational financial institution for illegally accessing customer account information from UK customers that resulted in the theft of GBP 200 000.[30] Computer hackers can also cause breaches. In July 2006, a computer hacker located in Germany gained access to the computer system of a local government agency in the United States that contained personal information on 4 800 public housing residents.[31] Other cross-border risks include the fact that inadvertent disclosure of personal data on a public website opens the possibility of misuse in any country around the world.[32]

Privacy and data protection authorities do not report receiving cross-border complaints in significant number. It is certainly the case that few individual complaints have a cross-border element, with spam being a notable exception. Although this may suggest that there are not many privacy breaches with a cross-border dimension, it could just as well indicate that we lack good information on this topic. It may be illustrative to look at broader complaint trends. For example the proportion of fraud-related consumer complaints from the joint US-CAN-AUS Consumer Sentinel database that are cross-border is steadily increasing: 20% were cross-border in 2005, up from 16% in 2004 and 14% in 2003.[33]

Whether privacy complaints will follow the broader consumer fraud complaint trends is not clear. First of all individuals may not be aware of the use of their personal data beyond national borders. Sometimes, they may not even realise that their complaint would involve a foreign organisation. They may not know to whom to complain with a cross-border problem. Indeed, even in a purely domestic context, individuals may not know to whom they should complain. A recent study in Norway found that only 33% of Norwegians know that the Data Inspectorate is the authority responsible for the protection of personal data,[34] while in the United Kingdom public awareness of the role of the Information Commissioner's Office is only 15%.[35] On the whole, surveys of public attitudes suggest that a very small percentage of individuals would complain to the relevant privacy authority.[36] Recent efforts to improve privacy notices by organisations processing personal data may go some way to help inform individuals about how to exercise their privacy rights.[37]

More research, information and analysis would help obtain a clearer picture of the nature of the privacy risks brought about by the changing landscape for transborder data flows. But it is already clear that these risks have resulted in harm both to individuals and organisations and also threaten the climate of trust needed in a global economy dependent on freely flowing information. It is in this context that the OECD has embarked on new work on cross-border privacy law enforcement co-operation.

C. The current OECD initiative

The OECD *Privacy Guidelines* not only declare principles about the use of personal information, but also call for national implementing action (Part Four) and international co-operation to facilitate transborder flows of personal data which respect the protective principles declared in the *Guidelines* (Part Five). In particular, Part Five provides that:

> "Member countries should establish procedures to facilitate information exchange related to these Guidelines, and mutual assistance in the procedural and investigative matters involved."

The OECD has built on the platform established by the *Privacy Guidelines*, particularly in the area of electronic commerce. At their 1998 meeting in Ottawa, OECD Ministers declared their commitment to:

> "take the necessary steps, within the framework of their respective laws and practices, to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks, and in particular to . . . ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress."[38]

The importance of effective enforcement was again emphasised in the OECD's 2003 report "Privacy Online: Policy and Practical Guidance," which called on member countries to "endeavour to establish procedures to improve bilateral and multilateral mechanisms for cross-border co-operation between public enforcement agencies in the procedural and investigative matters involved or called for in the Guidelines."[39]

The OECD has in recent years addressed other aspects of global electronic commerce which might pose threats to individuals and thereby reduce trust on line. It has in particular worked to counter the phenomenon of spam e-mail messages,[40] and taken steps to encourage and facilitate co-operation between consumer protection authorities to prevent fraud on consumers.[41] Both these initiatives reflect the need for strengthened international law enforcement co-operation and illustrate the role which the OECD can play in facilitating that co-operation.

Against this background, the OECD's Working Party on Information Security and Privacy (WPISP) has undertaken this examination of the issues involved in cross-border enforcement of privacy laws. The intent is to consider the issue from the perspective of non-OECD countries as well as from that of OECD countries. Formal enforcement actions are usually considered as a last resort among the broad array of mechanisms for ensuring effective compliance. For example, prior OECD work has recognised the importance to compliance of market-based incentives, technical tools (*e.g.* PETS); third-party guarantees (*e.g.* trust mark or seal programmes) and organisational structures (*e.g.* chief privacy officers).[42] But law enforcement is at times necessary, and this project is aimed at assisting with the challenges of making it effective in the cross-border environment. This work should also serve the broader objective of strengthening user trust in the online environment and contributing to the development of a coherent policy approach to addressing concerns about the use of global networks. Enhanced co-operation in the enforcement of privacy laws may also help address current issues like identity theft, spam, and malware.

As the first step in this activity, and in order to understand the current environment for co-operation between enforcement authorities, the WPISP developed a questionnaire for member countries. The support of non-member economies was also sought in gathering responses to the questionnaire in order to provide a more complete picture of the world-wide situation. The questionnaire aimed to elicit sufficient information about the privacy enforcement authorities to: *i*) understand the legal context in which the authorities work, *ii*) identify current challenges present in cross-border co-operation, and *iii*) point towards promising directions for addressing those challenges. The focus of this project is efforts by governmental bodies to enforce public laws or regulations covering both the private and public sectors. Its scope does not include, for example, initiatives in the Asia Pacific region related to enforcement by non-governmental organisations or involving privacy principles other than those reflected in public laws.

The remainder of this report consists of two main sections and a conclusion. The first section of the report provides an overview of the basic mechanisms for privacy enforcement in the domestic context. The second section focuses on the cross-border aspects of privacy enforcement, looking at the particular challenges encountered by authorities as well as current arrangements for addressing them. It also includes a section examining recent OECD work on enforcement co-operation in the areas of spam and consumer

protection. The conclusion brings together the analysis with a list of topics for possible further consideration.

SECTION I. DOMESTIC ASPECTS OF PRIVACY LAW ENFORCEMENT

The survey questionnaire was circulated for response in February 2006. By mid-June, 21 member countries had responded namely: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, France, Germany, Hungary, Iceland, Italy, Japan, Korea, the Netherlands, New Zealand, Norway, Poland, Spain, Switzerland, the United Kingdom and the United States. In addition, a welcome response from a non-member economy – Albania – was received. A summary tabulation of the responses is attached as Annex A. In addition, a brief introduction to privacy laws outside the OECD is included as background information and attached as Annex B.

The questionnaire focused on the enforcement of public privacy laws by government bodies. It defined the term 'enforcement' to include efforts by government authorities to *i*) secure legal remedies for individuals that have been harmed; *ii*) carry out regulatory audits and inspections; and *iii*) secure compliance by formal legal action of an administrative, civil, or criminal nature. This section of the report attempts to describe the picture of enforcement arrangements revealed by those answers to the questionnaire, supplemented to some degree by additional sources. The annexed tabulation of the responses includes two each for Korea and the Netherlands and a response limited to the private sector for Japan. There is just one entry for Germany describing the Federal German Commissioner although Germany provided a very comprehensive response reflecting its complex federal and local enforcement structure which the comments in this Report try to reflect.

As reflects the membership of OECD, the majority of countries that responded are members of the European Union or the European Economic Area (EEA), as well as the Council of Europe. They are consequently bound both by Convention 108 and EU Directive 95/46/EC. Accordingly there are considerable similarities in the responses from these countries. Taken as a whole, however, the responses also reveal diversity among the various enforcement authorities, some of which is described in this report. It is not obvious, however, that in practice this diversity creates a barrier to enforcement co-operation.

A. Basic mechanisms for enforcement

Authorities and their jurisdiction

The questionnaire asked countries to focus on national level enforcement authorities. Some responses provided additional information to explain the complexity of their national arrangements, either as a consequence of their federal structure or for other reasons such as a multiplicity of laws with a privacy impact or different enforcement arrangements in the public and private sectors. For example, as a consequence of the federal structure of Germany, data protection provisions governing the public and private sectors are predominantly enforced by the independent regional authorities.

The general impression from the responses is that member countries do have national level authorities responsible for enforcing privacy compliance, although in some countries, such as the United States, those functions might be considered as primarily consumer protection enforcement. In the majority – as a consequence of European Union membership – authorities have been set up under omnibus laws implementing the European Directive, to supervise both the public and private sectors with similar powers. This EU picture is broken, however, by Germany, one of the earliest countries to adopt data protection laws, in whose federal structure private sector enforcement is primarily a matter for the states. Canada, Australia and New Zealand also have systems of privacy commissioners enforcing privacy protection in both sectors.

Typically, an enforcement authority is a single commissioner independent of government, charged with the duties of considering complaints from individuals and of supervising the data processing activities of data controllers. Some countries, however, have commissions consisting of a body of commissioners, for example, France, Belgium and the United States. Those commissions may be small or large in number and either full or part-time. A second group to be found in Japan and Korea consists of groups of officials in government departments charged with privacy oversight. In Germany, there are data protection commissioners, charged with data protection oversight over public bodies, on the one hand, and independent data protection authorities for the private sector on the other. It is consequently no surprise to find that although the EU Directive imposes a certain degree of uniformity, the structure of the enforcement authorities is quite varied.

The following table sets out a list of the national level privacy enforcement authorities for OECD countries and sources of further information about them. It should be borne in mind that several countries, such as Australia, Canada, Germany and the United States, have regional level enforcement authorities which often play an important part in privacy enforcement and this list is therefore an incomplete picture.

Table 1. National Level Privacy Enforcement Authorities in OECD Countries

Australia	Privacy Commissioner	www.privacy.gov.au
Austria	Datenschutzkommission	www.dsk.gv.at
Belgium	Commission de la Vie Privée	www.privacycommission.be
Canada	Privacy Commissioner of Canada	www.privcom.gc.ca
Czech Republic	Office for Personal Data Protection	www.uoou.cz
Denmark	Datatilsynet	www.datatilsynet.dk
Finland	Office of the Data Protection Ombudsman	www.tietosuoja.fi
France	Commission Nationale de l'Informatique et des Libertés	www.cnil.fr
Germany	Federal Commissioner for Data Protection and Freedom of Information	www.bfdi.bund.de
Greece	Hellenic Data Protection Authority	www.dpa.gr
Hungary	Adatvédelmi Biztos	www.obh.hu
Iceland	Persónuvernd	www.personuvernd.is
Italy	Garante per la protezione dei dati personali	www.garanteprivacy.it
Japan	Cabinet Office	www5.cao.go.jp/seikatsu/kojin/index.html
	Competent Ministers (for the private sector)	
Korea	Ministry of Information and Communication	www.mic.go.kr
	Korea Information Security Agency	www.kisa.or.kr
Luxembourg	Commission nationale pour la protection des données	www.cnpd.lu
Netherlands	College Bescherming Persoonsgegevens	www.cbpweb.nl
	OPTA – Independent Post and Telecommunication Authority	www.opta.nl
New Zealand	Privacy Commissioner	www.privacy.org.nz
Norway	Datatilsynet	www.datatilsynet.no/
Poland	Inspecteur Général pour la protection des données personnelles	www.giodo.gov.pl
Portugal	Comissão Nacional de Protecção de Dados	www.cnpd.pt
Slovak Republic	Office for Personal Data Protection	www.dataprotection.gov.sk
Spain	Spanish Data Protection Authority	www.agpd.es
Sweden	Datainspektionen	www.datainspektionen.se
Switzerland	Préposé fédéral a la protection des données	www.edsb.ch
United Kingdom	Information Commissioner	www.ico.gov.uk
United States	Federal Trade Commission	www.ftc.gov
	Department of Heath and Human Services	www.hhs.gov
	Federal banking agencies	www.ffiec.gov
	Department of Justice	www.usdoj.gov

Distinctive features may be noted in the systems in the United States, Japan and Korea. In the United States, privacy protection in the private sector is partly treated as an aspect of consumer protection enforced by the Federal Trade Commission under long-standing powers which prohibit unfair and deceptive acts or practices in commerce. A parallel role is played by the Department of Justice for criminal proceedings. But in the common law legislative tradition, the United States also has specific sectoral and subject-matter legislation, for example in the financial services and health sectors, which provides for enforcement of privacy by other federal bodies as well. There is also privacy enforcement at a state level.

Japan and Korea reported on both the public and private sectors. In the public sector, privacy protection is enforced by government departments. In Korea, the Ministry of Government Administration and Home Affairs has general oversight of privacy protection in administrative bodies. In Japan, legislation applies privacy protection to the different types of administrative bodies and requires them to ensure compliance with privacy rules. Enforcement is through the legal system. Both countries have legislation applying to the private sector. In Japan, the Cabinet Office has general policy oversight of privacy protection, but complaints are dealt with by the National Consumer Affairs Center of Japan and other bodies. Relevant ministers can issue enforcement orders within the industry sectors over which they have oversight. In Korea, the principal enforcement authorities are the Ministry of Information and Communications which has a wide jurisdiction to protect privacy in electronic communications and KISA whose remit is not given by omnibus legislation, but is nevertheless extensive in that it also applies to personal data in electronic communications.

Complaints and complaint handling

Resolving the problems of individuals has always been seen as an important element of the work of data protection and privacy authorities. In some areas of regulation, the resolution of complaints is typically undertaken by ombudsmen or other services, whereas the enforcement authorities treat individual complainants more as informants providing evidence that could be used to support an enforcement action. In the European context, the EU Directive suggests but does not require that both functions will be carried out together. Another approach is adopted in Korea, which has established a Personal Information Dispute Mediation Committee within KISA to help resolve privacy disputes.

The survey enquired about the power of authorities to receive complaints from individuals about breaches of their privacy with the object of solving the problem for the individual. Each of the countries responding had at least one authority with the jurisdiction to consider privacy complaints. Germany provided information on more than 20 independent federal and state authorities. Most countries do not restrict the right to make complaints to citizens or residents. However, in Albania and Switzerland there are rules providing that a complainant has to be a citizen or legal resident of that country. In New Zealand, the authority cannot enforce a subject access request from a foreign national from abroad.

All authorities can receive complaints by conventional mail, and almost all by telephone and on-line. In Italy the law expressly provides that certain types of complaint must be made in writing, although ‘informal’ complaints, through which an individual acts in the role of informant, can be made by telephone and e-mail. Other exceptions include Australia, Belgium, Poland, Spain and the United Kingdom who do not accept complaints by telephone. That attitude to telephone complaints is reflected in several other responses. Even where such complaints are permitted, they are often discouraged as in the case of Austria or require written confirmation as in France. These variations in response are probably to be accounted for by the state of individual system development in different countries, the weight placed on demonstrating that a complaint is genuine, and the varying definitions of complaint.

A small majority of authorities reported having an obligation to investigate a complaint. The precise contours of what is entailed by this obligation may, however, vary. Canada’s Federal Commissioner is

under a duty to investigate, but may decline to issue a report on various grounds such as the availability of alternative remedies or the frivolous or vexatious nature of the complaint. Similarly, the Australian and New Zealand commissioners have a restricted discretion to discontinue or decline investigation. Belgium made the distinction between the duty of its authority to process a complaint, but not necessarily to conduct any enquiry.

Eighteen responses provided statistical information about complaints or referred to information published in reports of their authorities. Because of differences in categorisation practices, it is difficult to draw any internationally comparative conclusions. However, some observations can be made. Canada and Italy seem to be typical in that the financial sector features prominently in complaints about private sector organisations. More than a quarter of complaints in France, however, are about telecommunications or broadcasting. Telecommunications and the financial sector also predominate in Australia, Iceland, Poland and Spain. New Zealand and Hungary reported that complaints against the government are more common than against private sector organisations. The US FTC collects and analyses complaints on identity theft. In 2005, credit card fraud (26%) was the most common form of reported identity theft followed by phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%).

Investigations, audits and inspections

The survey also requested information about powers and activities more in the nature of regulatory supervision rather than complaint resolution. These may include studies or audits to generally examine compliance within a particular organisation or perhaps a business sector; as well as investigations of possible privacy breaches with a view to the imposition of appropriate sanctions. The powers of authorities in this area are quite varied. For example, the United Kingdom Commissioner can carry out audits only with the consent of the data controller, subject to a few exceptions; whereas many other authorities have power to conduct compulsory audits. On the other hand, the UK Commissioner is unusual in his power in certain criminal investigations to enter premises without notice if necessary under judicial warrant. In general, this is an area where the broader legal culture of a country is likely to impact the manner in which these powers are distributed to the enforcement authorities.

The questionnaire enquired about the power of authorities to initiate investigations on their own initiative and to carry out audits and inspections. Only KISA reported that it did not have the power to investigate on its own initiative, but the Korean Ministry of Information and Communication (MIC) can do so. Accordingly, the general picture is that typically authorities combine the roles of complaint handling and regulator or enforcer. The survey does not enable us to reach conclusions about how authorities manage the sometimes difficult task of balancing these roles and the priority they each place on responding to individuals as opposed to securing regulatory compliance. This dual role has troubled some authorities.[43]

The powers available to many authorities when conducting investigations seem to be extensive. Most authorities can require a data controller to provide information and documents. Most authorities have similar powers in relation to third parties, but this is a smaller group than in the former case and excludes Japan, Korea, the United Kingdom and typically the German states. Again, most, but not all, authorities can enter premises without consent. This is a power which often requires judicial warrant, as is the case for Australia, France, Italy, the United Kingdom and the United States. It was also reported that the large majority of authorities could require the temporary or permanent cessation of processing, but the extent of the legal formalities required is not clear in those cases.

The point regarding the conduct of investigations concerns the ability of authorities to carry out on-site audits or inspections. This is a typical power of the enforcement authorities, but it is not universally available – the US FTC, KISA and the competent Japanese ministers do not have such powers. Where they do exist, the powers fall into two groups: the first group hedges the use of the powers with protections and

limitations. For example, the United Kingdom unusually requires the consent of the data controller, while authorities in Albania, Belgium, Canada, Hungary, Italy, and the Korean MIC are required to have reasonable grounds for believing that there has been non-compliance with the law. But these protections are not universal. A second group of authorities from the Czech Republic, France, Germany, Iceland, the Netherlands, and Poland appear to have little formal constraint on their powers. A number of respondents remarked that although it was not a formal requirement it was the usual practice to inform the data controller in advance of an audit unless there was some compelling reason not to.

Sanctions, remedies and outcomes[44]

The survey also asked about the sanctions which can be imposed by the enforcement authorities or sought by them through legal process. So far as remedies for individuals are concerned, only four respondents reported the power to help someone take their own legal proceedings; and still fewer, three, reported the power to undertake binding arbitration. In 11 cases, however, the survey responses indicated that mediation could be undertaken, and one German state authority pointed out that, in its view, voluntary measures such as mediation could always be undertaken.

Nineteen respondents reported the power to make a determination that the law has been violated, but in only ten cases does that decision have legal effect of itself. On the other hand, 15 authorities can issue warnings or reprimands, and all but 2, are entitled to publicise violations. All German authorities are able to publicise violations or give warnings or reprimands.

Only six authorities can negotiate fines or other settlements. The US FTC does so as part of the consent order process. The Canadian Federal Commissioner may attempt to resolve complaints through mediation and conciliation which could include a settlement. The Australian Commissioner sees negotiated settlements as the best way of resolving complaints. The Czech Republic, the Netherlands and Korean MIC are also part of this small group. France, however, noted that a regulatory authority that can impose a decision has no need to negotiate settlements – a response that may apply to other authorities with strong enforcement powers.

A majority – that is to say 16 of the 24 national authorities analysed - can issue legally enforceable orders. In Japan and Korea this action is taken by a minister rather than the complaint authority. German authorities can issue legally enforceable orders only with respect to the private sector.

Only three countries – Australia, Norway, and the United States – have authorities that can order compensation for individuals. Ten authorities can seek injunctions in the courts and in 16 can seek financial or other penalties. Seven authorities report that they can institute criminal proceedings. However, it would appear that others can submit a formal request to a public prosecutor to initiate proceedings. The United Kingdom Commissioner is a hybrid in that he can conduct his own prosecutions in the criminal courts of England, Wales and Northern Ireland, whereas in Scotland, he reports matters to the public prosecutor – which is the more general pattern in the OECD.

The second part of the survey on sanctions concerned the remedies available through the judicial process. The survey asked about order-making powers, compensation for individuals, civil penalties, criminal fines and imprisonment following conviction. All respondents provide some form of remedy through their courts or special tribunals. Sometimes the judicial remedies balance a limited range of sanctions which can be imposed by the authority. So, for example, KISA has rather limited powers, but a wide range of sanctions is available through the Korean courts including compensation for individuals and fines and imprisonment on criminal conviction. Sixteen of the 24 responses reported that their courts could impose civil penalties. Usually this is in addition to criminal penalties. The picture in Germany at the state

level is that in almost all cases the full range of sanctions is available through the courts, but at a federal level only injunctive orders can be sought.

The sanctions available in the case of non-compliance vary considerably. In the Czech Republic and Iceland, the authority can impose daily fines and in Denmark, the violator is referred to the police. Where the breach is of an order of the courts the typical response is that the usual mechanisms relating to the enforcement of judicial orders apply. Belgium and France responded that the normal methods of enforcing a court judgment would apply and that also applies to court decisions in New Zealand and Poland. Spain can use the tax system to recover unpaid penalties and Albania mentioned making a report to parliament as a further sanction. Australia, Canada and the United States specifically mention the use of contempt proceedings.

B. National privacy laws

Although the focus of this project is the ability of authorities charged with enforcing privacy laws to operate in a cross-border environment, the questionnaire did ask for basic information about the privacy laws enforced by these authorities. The survey asked whether laws were generally applicable or of a sectoral nature and whether they addressed the following sets of privacy principles:

- Openness/transparency.
- Data quality.
- Collection and use.
- Security safeguards.
- Subject access.
- Transborder data flows.

The EEA countries have laws of general application, with some exceptions. That is to say that, although the EU Directive does not apply to justice and home affairs and other matters outside the scope of community competence, EEA member states often cover in a single law both those sectors within the Directive and those outside. In any case, EU members are under other obligations to have legislation in place to provide data protection for justice and home affairs to the standard of Convention 108.[45] The Netherlands reported information about the laws enforced both by its general data protection authority and its telecommunications regulator. For the private sector, Germany has uniform substantive law at the federal level. The Federal Government and the states have their own provisions in place for the processing of personal data in the public administration. Similarly, Canada through its body of federal and provincial legislation has a set of laws of general application for the public and private sectors. On the other hand, although Australia has a fairly comprehensive scheme of legislation at the federal level, it is embodied in different sets of principles for the public and private sectors and the specific issues of credit reporting, tax file numbers and spent convictions. Japan and Korea deal differently with the public and private sectors and the focus of the survey analysis has been on their private sector legislation. The US FTC is primarily a consumer protection agency and privacy protection is part of its larger consumer protection mission.

Taken as a whole the laws in EU/EEA countries address all six sets of principles. The collection of sectoral laws enforced by the FTC is too complex to express through this framework. Japan and New Zealand seek to cover all matters except transborder data flows; Korea deals with all six matters. In Canada the federal Privacy Act, which applies to the public sector, does not address security or transborder data flow provisions.

Even where national laws set out to apply the same principles, differences of interpretation and emphasis to take account of historical, cultural and legal differences can hinder co-operation between authorities. A focus on the underlying facts of the complaints, however, may help overcome tensions between different legal categories.

SECTION II. CROSS-BORDER ASPECTS OF PRIVACY LAW ENFORCEMENT

The second part of the Questionnaire enquired about the "cross-border" aspects of enforcement, a term used in a broad sense to include cases in which "the data subject is located in a different country from the data controller, the data itself has passed to a third country, or simply where important evidence is located in a third country." OECD work on law enforcement in other areas (consumer protection, spam) has identified considerable challenges to be overcome to operate effectively in a cross-border context. The Questionnaire results suggest that the situation is similar for privacy, although there may be less practical enforcement experience upon which to judge.

The continued growth in the use of the Internet and changing nature of transborder data flows suggest that the need to address the cross-border challenges faced by enforcement authorities is only going to increase. Even now, the European Commission has identified transborder data flows as an area where the lack of enforcement action appears to be creating a gap between law and practice.[46] A similar sentiment is expressed by a practitioner who has observed that the global nature of the Internet means that "in many cases there is a gap between applicable data protection requirements and the possibility of the authorities to enforce those requirements."[47] This section of the report describes a number of cross-border enforcement activities, along with the legal and practical challenges that operating in a cross-border environment raises for enforcement authorities.

A. Examples of cross-border enforcement activity

Cross-border cases

While hardly commonplace, there have been a number of examples of cross-border enforcement activity. There were two separate cases in the United Kingdom where alleged criminal breaches of the prohibition on the deceitful obtaining of personal data required cross-border assistance. One case required advice from an expert in the law of a middle-eastern country and also the carrying out of investigations in France. In the second case the conduct of investigations in Norway was required for which the formal assistance of the Norwegian data protection authority was requested under both Convention 108 and the EEA Agreement which applies the EU Directive to Norway. Korea reported that in February 2006, 250 000 Koreans had their names and resident registration numbers stolen in a popular online computer game by hackers based in China. To date no financial damages has been suffered by the victims, but there remains a risk of harm because the registration number can be used to acquire other private data, and authorities in Korea have had difficulty establishing co-operation with the appropriate Chinese authorities. Naturally, rules on transborder data flows have also generated some cases. For example, in 2005 Iceland reported on a case in which the Data Protection Authority concluded that the sending of blood samples to the United States amounted to the overseas transfer of personal data and therefore required that the transborder dataflow rules be applied.

Other examples of cross-border cases can be drawn from the Canada-US experiences. The Office of the Privacy Commissioner of Canada has launched an investigation as a result of a Canadian magazine obtaining the telephone records of the Privacy Commissioner and another staff member from a US-based data broker. The data broker obtained the records from at least two different Canadian telecommunications companies. Other examples include a case involving a US-based website (Abika.com) that provided psychological profiles and criminal records searches on Canadian individuals without their consent. The

Privacy Commissioner of Canada determined that she could not proceed with the complaint on the basis that there was not sufficient jurisdiction to investigate. The US FTC has brought an enforcement action against the operators of the same website alleging a privacy invasion in violation of US law.[48] Other US-Canadian examples include complaints related to the transfer of credit card information to the United States for third-party processing.

While the small sampling of cases identified above may not be representative, it provides some indication of the situations being encountered by authorities. A wider enquiry might uncover other cross-border cases – perhaps small in number – but important and challenging. Conducting research in this area is made difficult by the fact that in many countries privacy cases only rarely go before the courts and there are often no accessible reports of privacy dispute outcomes unless created by the enforcement authorities themselves. Identifying cases with a cross-border element is even more difficult, as this factor is not often mentioned in a short report or relevant news story.

Audits or inspections with a cross-border dimension

There is a growing trend to co-operate at an international level in regulatory investigations. The European advisory body for data protection, known as the "Article 29 Working Party,"[49] set out criteria for selecting enforcement targets and agreed that in 2005 and 2006 it would undertake synchronised national investigations. That declaration has been followed by the identification of the private health insurance sector for this first round of activity and the development of a questionnaire for eliciting information from companies in the sector. The Article 29 Working Party has also conducted joint audits of the arrangements surrounding the exchange of Passenger Name Records (PNR) data between European airlines and customers and border authorities in Australia, Canada,[50] and the United States.[51]

Another cross-border example involved consideration of the privacy implications of the Microsoft "Passport" web services, over which a number of European authorities were faced with similar complaints. A joint analysis was organised through the Article 29 Working Party.[52] It is a particularly noteworthy example because the US FTC was also faced with complaints, examined related issues, and settled an enforcement action with Microsoft.[53] Within the limits of their powers both the FTC and the European authorities tried to keep each other informed of their progress, their decisions and their reasoning.

B. Legal and practical challenges to effective cross-border enforcement

Foreign data controllers or data subjects

The Questionnaire sought information about whether an authority could take action against foreign data controllers or to protect foreign data subjects. Fourteen respondents said that their authorities could take action against foreign data controllers. Denmark, France, Italy, Norway, Poland, Spain and the United Kingdom clearly referred to the provisions of their national laws reflecting the European Union Directive which require them to apply their jurisdiction to data controllers established on their territory or using equipment on their territory for processing personal data otherwise than for the purpose of transit. This is a requirement which would apply to all EU member states and the additional EEA members. Australia, Japan and Switzerland reported that they cannot act against a foreign data controller; New Zealand reported that its authority in this situation is unclear; and Canada and the US FTC can act provided that the data controller has a sufficient connection with their country. Further information may be needed to determine whether the limitations relate to legal jurisdiction or to the practical ability to act against a data controller based abroad. On the other hand, everyone except the Korean authorities can act against a domestic data controller to protect a foreign data subject.

Notification and information sharing

The survey enquired whether authorities could notify authorities abroad of investigations which might concern them and whether they could share information with those authorities. Eighteen responses reported that their authorities could both notify foreign authorities and share information with them. Fourteen of the 18 are authorities from EEA countries and a number of them pointed out that Convention 108 and the EU Directive require them to co-operate with other authorities and in particular to share information with them.

Outside Europe, Canada reports that it does not, except in prescribed circumstances, have authority to inform foreign authorities or share information. The US FTC can notify others and share information, but it has been sufficiently concerned about the restrictions on its powers in this respect that it has sought additional powers through legislative changes. New Zealand is doubtful whether it can share information. In Japan, the law covering the private sector does not provide for notification, information sharing, and investigative assistance. In Korea, KISA cannot notify foreign authorities, but can in some circumstances provide information about cases where the privacy of a domestic data subject has been violated by a foreign data controller.

Broadly it would seem that although many authorities do have the power to share information, those powers are specially regulated and restricted and they seem to work most comfortably between members of groups such as parties to Convention 108. The powers to share information outside any formal grouping are uncertain and that uncertainty is a concern to enforcement authorities. Overcoming information sharing restrictions would in some cases require a review of relevant legislation or regulation, but is critical to effective international co-operation.

Other challenges

Sixteen of the 24 tabulated responses clearly said that the lack of powers was an obstacle and 15 said that the restrictions on information sharing were a specific obstacle. Sixteen authorities cited the incompatibility of legal regimes; 11 noted inadequate resources; but only 3 thought that language was an obstacle.

In the area of privacy enforcement as in other areas of cross-border legal co-operation, it should be noted that where formal orders have been issued or sanctions imposed, there arises the issue of cross-border judgment recognition and enforcement.[54] This is a problem in relation to the enforcement of court orders whether on behalf of an individual or an authority, and perhaps an even greater problem for sanctions imposed as a matter of administrative process.

Other issues include the difficulty of identifying a contact point and differing enforcement priorities. With respect to the contact point issue, virtually every country indicated that it had or could set up a single point of contact.[55] Only one-half of the responses reported that authorities have formal enforcement priorities. In one case, those priorities were described by reference to the sectors chosen as targets for regulatory action. Where an authority has enforcement priorities they would seem typically to be described in general terms. From the limited information available, recidivist behaviour, the seriousness of the harm and the number of individuals affected seem to be common criteria. France is unusual in giving priority to cases of current policy concern such as biometrics and video surveillance

C. Existing arrangements for cross-border cooperation in privacy law enforcement

It is clear from the activities and reports of privacy and data protection authorities that they attach considerable importance to international and regional co-operation arrangements. It is also clear from the survey results that authorities do have concerns about their legal ability to take part in these joint activities.

Where a legal framework exists permitting or requiring co-operation as in Europe, those arrangements are used in a small number of individual cases and to facilitate wider joint regulatory action. Given the overlapping membership among OECD, EU, Council of Europe, and APEC, continued information exchange and co-ordination of ongoing work will certainly be beneficial.

International Instruments for Privacy Co-operation

Council of Europe

The importance of co-operation on enforcement has been recognised by the other international institutions that have developed data protection instruments. The Council of Europe worked in parallel with OECD during the late 1970s and in January 1981 opened for signature its Convention 108 on the protection of personal data.[56] The model chosen by the Council of Europe was the adoption of a standard set of principles. There are also special rules on transborder data flows (TBDF) and mutual assistance mechanisms. The 'common core' principles were drawn from the earlier resolutions of the Committee of Ministers and member state legislation. Those principles were the now familiar rules on quality of data (*e.g.* fair and lawful obtaining and processing), sensitive data, security, and rights for individuals and they closely mirrored the principles in the OECD *Guidelines*. Limited rights to derogate were modelled on Article 8 of the European Convention on Human Rights,[57] and provisions were included restricting the right of parties to prohibit or restrict transborder data flows on the grounds of data protection. The Convention provides that non-members of the Council of Europe can accede to it. The Convention proved to be the principal international driving force for data protection in Europe throughout the 1980s and early 90s. A subsequent protocol has modified the Convention to align its provisions on TBDF and supervisory authorities with those of the European Union Directive.

Chapter IV of Convention 108 includes extensive provisions on Mutual Assistance and for ease of reference they are set out in Annex D. Article 13 contains the general duty to render mutual assistance including the requirement to nominate at least one authority for these co-operative purposes. It need not be a special data protection authority. The primary duty is to provide information. Article 14 requires the provision of assistance to foreign data subjects. Article 15 imposes restrictions on the use to be made of information obtained in the course of rendering assistance and Article 16 provides an exhaustive set of grounds on which assistance can be refused. Article 17 makes provision for the costs and procedures of rendering assistance. In addition, Chapter V of the Convention sets us a Consultative Committee (the T-PD) that acts as a forum for exchanges on privacy challenges and developments. Although not well recorded in public documents, the experience of regulators is that these provisions have been used, perhaps not extensively and frequently, but regularly over the years.

This chapter of the Convention was the basis for co-operation between many European States until the adoption of Directive 95/46/EC by the European Union. It still provides for co-operation in areas outside the scope of the Directive, such as policing, and in cases where one country is outside the European Economic Area (EEA), but has ratified the Convention.

European Union

Perhaps the most rigorous requirements to co-operate are to be found in the European Union Directive adopted in October 1995 (Directive 95/46/EC).[58] The Directive required the establishment of national supervisory authorities, imposed on them duties to co-operate, and created a co-operation mechanism. Those provisions have come to dominate the co-operation arrangements within Europe. Article 28 of the EU Directive expressly requires the establishment of national supervisory authorities. Those authorities are to be given investigative powers, 'effective powers of intervention,' and 'the power to engage in legal proceedings.' The authorities have the power to consider complaints and carry out checks on personal data

processing. Of particular interest in the current context, are the parts providing that authorities can be asked to exercise their powers by authorities in other EEA states, and the requirement that authorities shall co-operate with one another. Article 29 of the EU Directive goes on to set up a Working Party whose membership is largely drawn from the supervisory authorities of Member States established pursuant to Article 28. The role of the Working Party is largely to advise the European Commission, but it has become a principal means of establishing both common views between European data protection authorities and more recently joint enforcement operations.

Although these CoE and EU instruments are an important basis for co-operation within Europe and are referred to by respondents to the questionnaire, it is unclear about the extent to which information could be shared outside those groupings. It is possible that such sharing is not permissible at all or only to assist the investigation of one's own case. This is especially likely within the EEA because the data protection supervisory authorities in those countries are subject to a duty of "professional secrecy" imposed by article 28.7 of the EU Directive. The provisions of Directive 95/46/EC related to enforcement co-operation are reproduced in Annex C.

In 2002 the European Commission convened a conference to consider its First Report on the transposition of the European Directive.[59] As a consequence of that review an action plan was adopted by the Commission which included the encouragement of more systematic enforcement of the Directive across the EU. In November 2004, the Article 29 Working Party declared that "enforcement is an important instrument in the compliance 'toolbox,'" as well as its intention to take a more pro-active stance towards enforcement of data protection legislation within the European Union.[60]

Asia Pacific Economic Co-operation

In November 2004, Ministers of the Asia-Pacific Economic Co-operation endorsed the APEC Privacy Framework, developed by its Electronic Commerce Steering Group:

> "Consistent with the Organization for Economic Cooperation and Development's 1980 Privacy Guidelines, the Framework's privacy principles and implementation guidance are focused on the achievement of four main goals:
>
> - To develop appropriate privacy protections for personal information.
> - To prevent the creation of unnecessary barriers to information flows.
> - To enable multinational businesses to implement uniform approaches to the collection, use, and processing of data; and
> - To facilitate both domestic and international efforts to promote and enforce information privacy protections."[61]

One of the four objectives includes the facilitation of international efforts to enforce information privacy protections. The Guidance for Domestic Implementation of the APEC Principles provides that "A Member Economy's system of privacy protections should include an appropriate array of remedies for privacy protection violations."[62] The document also annexes a future work agenda that includes the following:

> "Member Economies should cooperate in relation to making remedies available against privacy infringements where there is a cross-border dimension. In order to contribute to this goal, Member Economies will endeavor to develop cooperative arrangements between privacy investigation and enforcement agencies of Member Economies"

To further this future agenda APEC's privacy sub-group is working to the develop cross-border privacy rules along with information and co-operation among privacy regulators in the area of investigation and enforcement.

Other privacy co-operative arrangements

Other co-operative arrangements include the US-EU Safe Harbor Agreement,[63] a 2005 MOU between the Spanish Data Protection Authority and the US Federal Trade Commission (on spam),[64] a 2006 MOU between the privacy commissioners of Australia and New Zealand,[65] the APEC Privacy Sub-Group, and the Eurojust, Schengen, Europol and Customs Information System arrangements for European co-operation in areas of law enforcement.

There are a number of less formal, but important co-operation arrangements (without primarily an enforcement focus). The International Conference of Data Protection and Privacy Commissioners meets annually to discuss a broad range of privacy issues. The International Working Group on Data Protection in Telecommunications (sometimes known as the Berlin Group) typically meets twice a year on a variety of topics. Australia; Korea; New Zealand; and Hong Kong, China meet biannually under the auspices of the Asia Pacific Privacy Authorities Forum (formerly PANZA+). In 2003, the Spanish Data Protection Authority founded the Iberoamerican Data Protection Network (IDPN) as an advisory forum for national data protection efforts in Latin America.[66] Other examples include the EU Case handling Workshop which meets twice a year and the arrangement for seeking assistance from other authorities and exchanging information through the European Commission's CIRCA website. Other co-operative arrangements exist in the form of regional group meetings to discuss not only general policy, but also specific cases: examples would be the annual spring conference of European Data Protection Authorities, the six-monthly British Isles meetings, meetings of Francophone countries, and the meetings of the Scandinavian authorities.

D. OECD Co-operation Instruments in other Areas

There is much that can be learned from work on law enforcement co-operation in other areas, whether civil, administrative or criminal.[67] The OECD has already been active in promoting cross-border law enforcement co-operation in two areas that are relevant for the work on privacy co-operation: consumer protection and spam.[68] In both areas the OECD has developed co-operation instruments that aim to address common cross-border enforcement challenges, including:

- Restrictions on the scope of enforcement authority.
- Limitations on information gathering and sharing.
- The limited enforceability of outcomes across borders; and
- Varied enforcement priorities among enforcement agencies.[69]

Both instruments articulate key policy principles, but leave the implementation responsibilities to member countries and their respective enforcement authorities. They contemplate that existing networks and bilateral arrangements for co-operation will continue to assist in cross-border cases.

Cross-border Fraud Guidelines

In 2003 the OECD governments agreed on new *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders* ("Cross-border Fraud Guidelines").[70] The Guidelines recognise that improved international co-operation begins with effective domestic systems that equip enforcement bodies with the appropriate authority and tools to investigate, obtain evidence, share evidence, and stop wrongful conduct.

The *Cross-border Fraud Guidelines* articulate principles for international co-operation, with specific attention to notification, information sharing, investigative assistance, confidentiality, and the jurisdiction of enforcement authorities. Member countries are called upon to establish a single point of contact to facilitate international co-operation. The *Guidelines* also highlight the important contribution that can be made by the private sector to successful cross-border enforcement. Finally, the *Guidelines* call for further study on some of the more challenging aspects of cross-border enforcement, including redress, the freezing of assets, and the mutual enforcement and recognition of judgments.

For some countries, implementation of the *Cross-border Fraud Guidelines* has required legislative change - indeed in some countries new authorities have been created.[71] For other countries, implementation efforts to date have been more at the operational level. For nearly all countries, the process of updating their enforcement authorities to address the realities of a global marketplace will be an ongoing process.

Spam Enforcement Recommendation

Building on the *Cross-border Fraud Guidelines*, the OECD council adopted a *Recommendation on Cross-border Co-operation in the Enforcement of Laws against Spam* ("Spam Recommendation") on 7 April 2006.[72] The problem of anti-spam law enforcement raises a similar need for global co-operation to overcome a number of challenges to information gathering and sharing, for identifying enforcement priorities and for developing effective international enforcement frameworks.

While the goal is enhanced co-operation, the Recommendation also makes clear that ultimately the decision on whether to provide assistance in any particular case rests with the enforcement authority receiving the request. Before making a request for assistance under the Recommendation, enforcement authorities are encouraged to conduct preliminary investigative work, attempt to prioritise the request, and utilise existing common resources.

The Spam Recommendation has particular relevance for privacy law enforcement co-operation, because many OECD countries have given responsibility for spam enforcement to their privacy enforcement authorities, who are therefore covered within its scope.

CONCLUSION

As was pointed out by one privacy enforcement official at an APEC Symposium in 2004, enforcement co-operation "seems instinctively to be a 'good thing.'"[73] We now have additional evidence to support the need for effective co-operation. As information and communications networks have grown in size and capabilities, the business and operational efficiencies they bring have been accompanied by increased privacy risks. Mitigating these risks while at the same time ensuring the trust needed in a global economy dependent on the free flow of information requires strong cross-border privacy law enforcement co-operation. The need for improved enforcement co-operation – initially recognised in the 1980 Privacy Guidelines – has now become a priority within and outside the OECD.

The OECD's Working Party on Information Security and Privacy plans continued work on topics addressed in this report, with the objective of furthering the ability of authorities to work together in cross-border cases. The findings in this report suggest a number of possible topics for further study and consideration, including:

- Examination of approaches to handling and classifying cross-border complaints.
- Work towards identifying common priorities for enforcement co-operation.
- Ways to improve co-operation between authorities with respect to notifications, information sharing, and investigative assistance.
- Consideration of the adequacy of sanctions and remedies available to privacy enforcement authorities in the context of cross-border cases.
- Work towards improving the prospects of international judgment recognition and enforcement of orders for monetary redress for individuals who suffer privacy breaches.[74]
- Examination of informal methods of international co-operation – often through regional networks – that allow for information exchange on current issues and best practices.
- Consideration of the need for practical tools, like contact lists, forms to request assistance from another authority, cross-border complaint forms, common approaches to reporting case results, etc.
- Work towards establishing a more complete and robust set of indicators about the dimensions of cross-border privacy problems.

Virtually every OECD country has established law enforcement authorities charged with enforcing privacy laws. Increased attention to the issues described above can help ensure that these authorities can successfully meet their responsibilities when cross-border challenges arise.

NOTES

[1] Recommendation of the Council concerning *Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980), OECD, Paris, ISBN 92-64-19719-2.

[2] Council of Europe (CoE) (1981) The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg, CoE. European Treaty Series No 108.

[3] United Nations *Guidelines Concerning Computerized Personal Data Files* adopted by the General Assembly on 14 December 1990.

[4] See, http://www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html.

[5] See OECD, Broadband Statistics, December 2005, available at: http://www.oecd.org/document/39/0,2340,en_2649_37441_36459431_1_1_1_37441,00.html.

[6] TeleGeography Research, Internation Internet Statistics" (2005) http://www.itu.int/dms_pub/itu-d/md/02/isap2b.1.1/c/D02-ISAP2B.1.1-C-0025!!PDF-E.pdf

[7] OECD, Internet Traffic Exchange: Market Developments and Measurement of Growth (2006), p.13 http://www.oecd.org/dataoecd/25/54/36462170.pdf.

[8] Colin Bennett and Charles Raab, *The Governance of Privacy* (MIT, Cambridge Mass 1996) p. xvi.

[9] Christopher Kuner, *European Data Privacy Law and Online Business* (Oxford U. Press 2003), p. ix.

[10] U.S. Dept. of Commerce, "Safe Harbor Workbook," available at: http://www.export.gov/safeharbor/sh_workbook.html

[11] According to one study, sixty-one percent (61%) of teens reveal their contact information on their blogs by disclosing their email address (44%), instant messenger name (44%), or a link to a personal home page (30%). Fifty-nine percent (59%) reveal their location in terms of a city or state. Thirty-nine percent (39%) of teen bloggers provide their birth date, and twenty percent (20%) disclose their full name. See David Huffaker, "Teen Blogs Exposed: The Private Lives of Teens Made Public" (2006), available at http://www.soc.northwestern.edu/gradstudents/huffaker/papers/Huffaker-2006-AAAS-Teen_Blogs.pdf.

[12] See, *e.g.*, Elliot Maxwell, "Some Reflections on The Future: Dipping A Toe in the Datastream;" presentation to the OECD Foresight Forum on Radio Frequency Identification (RFID) Applications and Public Policy Considerations, Paris, 5 October 2005, available at: http://www.oecd.org/dataoecd/60/20/35466861.pdf.

[13] *The Tipping Point*, Malcolm Gladwell, 2000-2002, Back Bay Books

[14] A growing majority of 5 257 US and Canadian households surveyed report that privacy concerns affect their behaviour on line . See, Forester Research, "The Consumer Privacy Bluff" (13 December 2005).

[15] See, Harris Interactive, "Global Consumer Perceptions towards Data Security," (January 2006), available at: http://corporate.visa.com/av/pdf/DataSecurityResearch.pdf.

[16] See, IPSOS "Interest in Online Banking Flattens", (6 September 2005) available at: http://www.ipsos-na.com/news/pressrelease.cfm?id=2765

[17] See, John Leydon, "Consumers punish firms over data security breaches", (15 November 2005), reporting on a study by the Ponemon Institute, available: http://www.theregister.co.uk/2005/11/15/data_security_breach_survey/ .

[18] See, Peter Swire, "The Internet and the Future of Consumer Protection," (24 July 2006) available at: http://www.americanprogress.org/atf/cf/%7BE9245FE4-9A2B-43C7-A521-5D6FF2E06E03%7D/SWIRE_CONSUMER_PROTECTION_REPORT.PDF

[19] The action was brought by the New York State Attorney General, who obtained a USD 1.1 million settlement from the company. See, http://www.oag.state.ny.us/press/2006/mar/mar23a_06.html .

[20] See, BNA, "Japan Sees Jump in Data Breach Reports in FY '05," Vol.5 No.28 (10 July 06). Although the fiscal year 2005 numbers are a three-fold increase from those reported in 2004, that jump may be due in part to a change in Japanese law which made such reporting mandatory.

[21] Many states in the US have now enacted provisions that make it mandatory to notify individuals of data breaches in certain circumstances. Such provisions are less common in Europe and elsewhere. See BNA, "Security Breaches: Legal Requirements in Europe, "(June 06) Vol. 6, No. 6, p. 26.

[22] See, http://www.ftc.gov/opa/2006/02/cardsystems_r.htm

[23] See, www.meti.go.jp/policy/commerce_distribution/kouhyouyou.htm .

[24] The US FTC obtained a fine of USD 10 million and USD 5 million in consumer redress. See, http://www.ftc.gov/opa/2006/01/choicepoint.htm

[25] For a list of data-breaches reported by US organisations, see, http://www.privacyrights.org/ar/ChronDataBreaches.htm.

[26] The recent CSI/FBI Computer Crime Survey concludes that negative publicity from reporting intrusions to law enforcement is still a major concern for most organisations. Even in an anonymous survey, only half of the 616 U.S companies surveyed were willing to share overall cost figures from financial losses resulting from security breaches. See, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

[27] See, http://www.hummingbird.com/press/2006/texas_guaranteed.html

[28] See, http://www.thisismoney.co.uk/saving-and-banking/article.html?in_article_id=401667&in_page_id=7

[29] See, Associated Press, "Equifax laptop with employee data stolen", (20 June 2006), available at: http://www.msnbc.msn.com/id/13437723/

[30] See, BNA, Privacy and Security Law Report, Vol. 5, No. 27 (3 July 2006) p.948.

[31] See, http://www.montereyherald.com/mld/montereyherald/news/15133805.htm

[32] The US Military recently reported that personal data including full name and social security numbers of 100 000 military personnel was inadvertently made publicly available on an official US government website. See, http://www.news.navy.mil/search/display.asp?story_id=24568.

[33] See http://www.ftc.gov/bcp/conline/edcams/crossborder/PDFs/Cross-BorderCY-2005.pdf.

[34] Inger-Anne Ravlum, "Pinning our faith on Big Brother" (2005). See, http://www.toi.no/article17922-29.html.

[35] See, ICO Communications and External Relations Strategy, Three year plan 2006-2009, p.4 available at: http://www.ico.gov.uk/cms/DocumentUploads/Communications_and_External_Relations_Strategy_2006-09_full_version

[36] See, Bennett and Rabb (2006), p.263 reporting on surveys in Canada and Australia.

[37] See, OECD, "Simplified Privacy Notices: An OECD Report and Recommendations" (2006), available at: http://appli1.oecd.org/olis/2006doc.nsf/linkto/dsti-iccp-reg(2006)5-final.

[38] Declaration on the Protection of Privacy on Global Networks made by Ministers at the Conference 'A Borderless World: Realising the Potential of Global Electronic Commerce', 7-9 October 1998, Ottawa, Canada.

[39] OECD, "Privacy Online: OECD Guidance on Policy and Practice", p. 29-31 (2003). Available at: http://www.oecd.org/document/49/0,2340,en_2649_34255_19216241_1_1_1_1,00.html.

[40] See, www.oecd-antispam.org.

[41] www.oecd.org/sti/crossborderfraud.

[42] See, OECD "Privacy Online" (2003), p. 19.

[43] See, for example, the report of and papers prepared for a conference in November 2005 by the United Kingdom Information Commissioner, available at: http://www.ico.gov.uk/eventual.aspx?id=16537.

[44] In this section of the report numbers of respondents have been calculated using the German Federal Commissioner alone. Separate comments are made on the position of German state authorities.

[45] See for example Article 14 Convention Based on Article K.3 of the Treaty on European Union, on the Establishment of a European Policy Office (Europol Convention) [Official Journal C 316 of 27.11.1995].

[46] First Report on the implementation of the Data Protection Directive, COM(2003)265 final, p. 20.

[47] Kuner, (2003), p. 37.

[48] See, http://www.ftc.gov/opa/2006/05/phonerecords.htm

[49] The Working Party on the Protection of Individuals with Regards to the Processing of Personal Data was set up under Article 29 of the EU Data Protection Directive, 95/46/EC.

[50] See, Art. 29 Working Party, "Opinion 1/2005 on the level of protection ensured in Canada for the transmission of Passenger Name Record and Advance Passenger Information from Airlines", (2005), available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp103_en.pdf

[51] See, Art. 29 Working Party, "Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP) available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp87_en.pdf

[52] See Art. 29 Working Party, "Working Document First orientations of the Article 29 Working Party concerning on-line authentication services" (2002) available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp60_en.pdf

[53] See, http://www.ftc.gov/opa/2002/08/microsoft.htm

[54] For a discussion of these issues in the context of consumer protection judgments, see OECD, "Consumer Dispute Resolution in the Global Marketplace" (2006), pp. 39-43, available at: http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/FRY%20DPL.asp#TopOfPage

[55] In Japan the Cabinet Office could probably provide information about private sector issues.

[56] See footnote 2 supra.

[57] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, European Treaty Series 5 Strasbourg, 1950.

[58] See footnote 3 supra.

[59] European Commission First Report on the transposition of the Data Protection Directive IP/03/697 Date: 16/05/20.

[60] Declaration of the Article 29 Working Party on Enforcement 12067/04/ENWP 101.

[61] See, www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.tml.

[62] See, http://203.127.220.112/content/apec/apec_groups/som_special_task_groups/electronic_commerce.downloadlinks.0004.LinkURL.Download.ver5.1.9

[63] See, http://www.export.gov/safeharbor/index.html. To date, the body established by EU data protection authorities to consider complaints from individuals under the US Safe Harbor Agreement has had no cases to consider.

[64] See, http://www.ftc.gov/os/2005/02/050224memounderstanding.pdf

[65] See, http://www.privacy.org.nz/filestore/docfiles/2072970.doc

[66] https://www.agpd.es/index.php?idSeccion=349

[67] For example, recent work in the area of cybercrime raises similar issues regarding information sharing, See *e.g,* Council of Europe, Convention on Cybercrime, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm or the EU "Council Framework Decision 2005/222/JHA" available at http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf#search=%22council%20framework%20decision%202005%2F222%2FJHA%22

[68] The OECD has also been active in promoting co-operation in the area of competition law enforcement. See, *Recommendation of the Council concerning Co-operation between Member Countries on Anticompetitive Practices Affecting International Trade*, C(95)130/FINAL, available at: http://www.oecd.org/competition .

[69] OECD, "Anti-Spam Law Enforcement Report," DSTI/CP/ICCP/SPAM(2004)3/FINAL, p.4.

[70] See, www.oecd.org/sti/crossborderfraud.

[71] OECD, "Report on the Implementation of the 2003 OECD Guidelines for Protecting Consumers From Fraudulent and Deceptive Commercial Practices Across Borders." (2006), available at: http://www.oecd.org/dataoecd/45/53/37125909.pdf

[72] See, http://www.oecd-antispam.org/article.php3?id_article=237v .

[73] Blair Stewart 'Cross Border Co-operation on Enforcement Matters', Apec Symposium On Data Privacy Implementation Mechanisms, Santiago, Chile, 23-24 February 2004.

[74] For a discussion of these issues, see OECD, "Consumer Dispute Resolution and Redress in the Global Marketplace", (2005), pp. 39-41. http://www.oecd.org/dataoecd/26/61/36456184.pdf

ANNEX A: TABULATION OF THE RESPONSES TO THE QUESTIONNAIRE

Questions:	Enforcement Authority				Complaint Handling							Investigation/Audits/Inspection										
	Date	Budget M Euros	Staff	Enforcement Staff	Receive complaints	Citizen	Resident	Mail	Phone	On-line	Inv. Duty	Own motion	Testimony	Documents	3rd Parties	Enter Premises	Stop Processing	On-site Audits	Grounds	Inform	Consent	Other
AUSTRALIA	1988	2,52	39	39	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y
AUSTRIA	1980		20	5	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
BELGIUM	1992	4,61	59	25	Y	N	N	Y	N	Y	N	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
CANADA	1983		86	30	Y	N	N	Y	N	N	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N
CZECH REPUBLIC	2000	3,2	80	50	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
DENMARK	1979	2	37	31	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y
FRANCE	1978	7	102	102	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	Y
GERMANY	1978	3,69	69	56	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
HUNGARY	1995	1,3	52	31	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y
ICELAND	2001	0,5	8	6	Y	N	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	N
ITALY	1997	16,5	105	5	Y	N	N	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
JAPAN - Private Sector[1]	2003	0,7	44	44	Y	N	Y	Y	Y	N	N	Y	Y	Y	N	N	Y	N	N	N	N	N
KOREA - MIC	1948		441	8	Y	N	N	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N
KOREA - KISA	1996			10	Y	N	N	Y	Y	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	N
NETHERLANDS - CBP	1989	5,46	71	12	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
NETHERLANDS - OPTA	1997	18	140	8	Y	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
NEW ZEALAND	1991	1,4	31	12	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	N	Y	Y	Y
NORWAY	1980	2,9	31	24	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
POLAND	1998	2,7	116	81	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
SPAIN	1993	9,45	115	77	Y	N	N	Y	N	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
SWITZERLAND	1993		19,6	19,6	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	N	N
UNITED KINGDOM	1984				Y	N	N	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N
UNITED STATES - FTC	1914	211 USD	varies	varies	Y	N	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N
ALBANIA (Non-member)	2000	0,575	45	2	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N

1. The budget figure is only for the cabinet office (excludes competent ministers) and the staff figure is for both cabinet office and competent ministers.

Questions:	Sanctions, remedies, etc. by the Authority														Sanctions through legal system					
	Mediation	Binding arbitration	Legal assistance	Legal decision	Binding decision	Publicity	Warning/ reprimand	Negotiate fine, etc	Legal order	Compensation	Court Injunctions	Penalties	Criminal case	Other	Orders	Compensation	Civil penalties	Criminal fines	Jail	Other
AUSTRALIA	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	N	N	Y	Y	N	Y	Y	N
AUSTRIA	Y	N	Y	Y	Y	N	Y	N	Y	N	N	N	Y	N	Y	Y	N	Y	Y	N
BELGIUM	Y	N	N	N	N	Y	N	N	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y
CANADA	Y	N	Y	Y	N	Y	Y	N	N	N	Y	N	N	N	Y	Y	Y	Y	N	N
CZECH REPUBLIC	N	Y	N	Y	Y	Y	N	Y	Y	N	N	Y	Y	N	N	Y	N	Y	Y	N
DENMARK	N	N	N	Y	Y	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y	Y	Y	Y	N
FRANCE	N	N	N	Y	Y	Y	Y	N	Y		N	Y	N	N	Y	Y	Y	Y	Y	N
GERMANY	Y	Y	N	Y	N	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N
HUNGARY	Y	N	N	Y	Y	Y	Y	N	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y	N
ICELAND	N	N	N	Y	Y	Y	N	N	Y	N	N	N	N	Y	N	Y	Y	Y	Y	N
ITALY	N	N	N	Y	Y	Y	Y	N	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N
JAPAN - Private Sector	N	N	N	Y	N	Y	Y	N	Y	N	N	Y	N	N	N	N	N	Y	Y	N
KOREA - MIC	N	N	N	Y	Y	Y	Y	Y	Y	N	N	Y	N	N	Y	Y	Y	Y	Y	N
KOREA - KISA	Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	N
NETHERLANDS - CBP	Y	N	Y	Y	N	Y	Y	Y	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	N
NETHERLANDS - OPTA	N	N	N	Y	Y	Y	Y	N	Y	N	N	N	N	Y	Y	Y	N	Y	Y	N
NEW ZEALAND	Y	N	Y	Y	N	Y	N	N	N	N	Y	Y	N	Y	Y	Y	N	N	N	Y
NORWAY	Y	N	N	Y	Y	Y	Y	N	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	N
POLAND	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	Y	Y	Y	Y	N
SPAIN	N	N	N	Y	Y	Y	N	N	Y	N	N	Y	N	N	Y	N	Y	Y	N	N
SWITZERLAND	N	N	N	Y	N	Y	N	N	Y	N	Y	Y	N	N	Y	Y	Y	Y	N	N
UNITED KINGDOM	N	N	N	Y	N	Y	Y	N	Y	N	Y	Y	Y	N	Y	Y	N	Y	N	N
UNITED STATES - FTC	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	N	N	N
ALBANIA (Non-member)	Y	N	N	Y	Y	Y	Y	N	N	N	N	N	Y	N	Y	Y	Y	Y	Y	N

Questions:	Cross-border Aspects							Obstacles to cross-border co-operation					
	Existing arrangements	Could have Contact Point	Enforcement priorities	Against foreign controller	Against domestic controller	Notify foreign authorities	Share info abroad	Lack of legal powers	Legal incompatibilities	Limits on info sharing	Resource limitations	Language barriers	Other
AUSTRALIA	Y	Y	N	N	Y	Y	Y	Y	Y	Y	N	Y	N
AUSTRIA	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	N
BELGIUM	N	Y	N	N	Y	Y	Y	Y	Y	N	Y	N	N
CANADA	N	Y	N	Y	N	N	N	Y	N	Y	N	N	Y
CZECH REPUBLIC	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
DENMARK	Y	Y	N	Y	Y	Y	Y	?	?	?	?	?	
FRANCE	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y
GERMANY	N	Y	N	N	Y	N	N	Y	N	Y	Y	N	N
HUNGARY	N	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
ICELAND	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	Y
ITALY	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N
JAPAN - Private Sector	N	N	N	N	Y	N	N						
KOREA - MIC	N	Y	Y	N	N	N	Y	Y	Y	N	N	N	N
KOREA - KISA	Y	Y	Y	N	N	N	Y	Y	Y	Y	N	N	
NETHERLANDS - CBP	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	Y	N
NETHERLANDS - OPTA	Y	?	Y	N	Y	Y	Y	Y	Y	Y	Y	N	
NEW ZEALAND	Y	Y	Y	?	Y	Y	?	Y	Y	Y	Y	Y	
NORWAY	Y	Y	N	Y	Y	Y	Y	N	N	N	N	N	
POLAND	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	
SPAIN	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N	N
SWITZERLAND	N	Y	Y	N	Y	Y	Y	N	Y	Y	Y	N	
UNITED KINGDOM	Y	Y	Y	Y	Y	Y	Y	?	?	N	N	N	
UNITED STATES - FTC	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	
ALBANIA (Non-member)	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N

ANNEX B: PRIVACY LAWS AND ENFORCEMENT AUTHORITIES OUTSIDE THE OECD

What follows below is a short overview of the situation outside OECD.[1] While the variety in approaches to privacy within the OECD is significant, it is even greater in non-member economies. There are a number of economies outside the OECD that have a privacy law and enforcement authority. A number of others' jurisdictions are currently in the process of developing or approving legislation. For example proposed legislation in South Africa would establish a data privacy of general application and create a new body to enforce the law, while India is considering amending its Information Technology Act to require improved data security.

Europe

Among the European countries that are not part of the OECD, a significant number have privacy laws, including: Albania,[2] Bosnia and Herzegovina,[3] Bulgaria,[4] Croatia,[5] Cyprus,[6] Estonia,[7] Gibraltar[8], Latvia,[9] Liechtenstein,[10] Lithuania,[11] Malta,[12] Monaco,[13] Romania,[14] Serbia,[15] and Slovenia.[16] Here the influence of the European Union and the Council of Europe has been substantial.

Asia Pacific

Non-members in the Asia-Pacific region with privacy laws include Hong Kong, China; Chinese Taipei; and Thailand.[17] The power of the Hong Kong, China authority[18] to investigate overseas breaches by local companies is uncertain. It would appear that their law would not allow them to share information with a body in another jurisdiction. On the other hand, the law in Chinese Taipei has limited coverage but allows the various sectoral enforcement bodies to restrict export of data in certain circumstances. Thailand has a law that includes principles and mechanisms to protect privacy of people related to personal information controlled or kept within state agencies or state enterprises. It is enforced by the Office of the Information Commissioner.[19]

Other countries in the region have privacy provisions inserted in other laws (for example, cybercrime laws) with limited means of enforcement. These include China, Indonesia, Philippines and Vietnam. A number of these countries are moving towards having more comprehensive privacy law.

Latin America

In Latin America, privacy rights have developed from the concept of “habeas data,” which permits individuals to know what information is archived about them by the government, and in some cases the private sectior.[20]Argentina established a comprehensive data protection law with an independent enforcement authority.[21] Chile’s constitution recognises a general right to privacy and it has comprehensive legislation - the Law for the Protection of Private Life - which regulates the processing of personal data in the public and private sectors, including human resources data. There is no independent data protection authority, with enforcement by means of individuals bringing private actions in the courts. Paraguay established a data protection law in 2000.[22]

Other Regions

Israel has a Data Protection Inspector and Registrar of Data Bases. Burkina Faso also has general data protection law.

ANNEX B: NOTES

[1] Member states of the Council of Europe and APEC economies were invited to participate in the work, including by completing the Questionnaire. Only one reply was received, that of Albania which has been incorporated into the broader analysis.

[2] The characteristics of the Albanian system have been incorporated in the body of this report, based on its response to the Questionnaire. An informal translation of the Albanian law is available here: http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/AlbaniaProtectionPersonalData.asp#TopOfPage

[3] See, http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/Bosnia&Herz.Data%20Protection%20eng%20received%20080402.asp#TopOfPage

[4] See, http://www.ceecprivacy.org/main.php?s=2&k=bulgaria

[5] See, http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/NATIONAlLAWS-EN.asp#TopOfPage

[6] For an unofficial translation, see http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/Cyprus%20-%20DP%20Law.asp#TopOfPage .

[7] See, http://www.dp.gov.ee/index.php?id=14

[8] The law is available at: http://www.gra.gi/legis/DATA%20PROTECTION%20ORDINANCE.pdf

[9] See, http://www.dvi.gov.lv

[10] See, http://www.sds.llv.li

[11] See, http://www.ada.lt/

[12] The website of the Data Protection Commissioner of Malta is here: http://www.dataprotection.gov.mt/

[13] See, http://www.ccin.mc/

[14] See, http://www.avp.ro

[15] See, http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/national_laws/FRY%20DPL.asp#TopOfPage.

[16] See, http://www.ip-rs.si/.

[17] The Web site of the Office of the Official Information Commission is here: http://www.oic.thaigov.go.th/content_eng/default_eng.asp.

[18] See, http://www.pco.org.hk/

[19] http://www.oic.thaigov.go.th/

[20] See, Pegg Eisenhauer, "Developments in Latin America Privacy Laws" in BNA Privacy and Security Law Report, Vol. 5, No. 15 (10 April 2006), pp521.

[21] See, http://www2.jus.gov.ar/dnpdp/

[22] http://www.alston.com/abResourceCenter/docs/ParaguayPrivateInfo.pdf

ANNEX C: EUROPEAN UNION DIRECTIVE 95/46/EC (excerpt)

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28 Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

ANNEX D: COUNCIL OF EUROPE CONVENTION 108 (excerpt)
Chapter IV – Mutual assistance, Article 13 – Co-operation between Parties

1 The Parties agree to render each other mutual assistance in order to implement this convention.

2 For that purpose:
- a each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;
- b each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.

3 An authority designated by a Party shall at the request of an authority designated by another Party:
- a furnish information on its law and administrative practice in the field of data protection;
- b take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

Article 14 – Assistance to data subjects resident abroad

1 Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

2 When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

3 The request for assistance shall contain all the necessary particulars, relating *inter alia* to:
- a the name, address and any other relevant particulars identifying the person making the request;
- b the automated personal data file to which the request pertains, or its controller;
- c the purpose of the request.

Article 15 – Safeguards concerning assistance rendered by designated authorities

1 An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.

2 Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

3 In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.