OECD publishing

Please cite this paper as:

Kuner, C. (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", *OECD Digital Economy Papers*, No. 187, OECD Publishing.
http://dx.doi.org/10.1787/5kg0s2fk315f-en

OECD Digital Economy Papers
No. 187

Regulation of Transborder Data Flows under Data Protection and Privacy Law

PAST, PRESENT AND FUTURE

Christopher Kuner

Unclassified

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

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY

Unclassified

REGULATION OF TRANSBORDER DATA FLOWS UNDER DATA PROTECTION AND PRIVACY LAW: PAST, PRESENT AND FUTURE

OECD Digital Economy Paper no. 187

By Christopher Kuner, Tilburg University, The Netherlands

English - Or. English

OECD DIGITAL ECONOMY PAPERS

The OECD's Directorate for Science, Technology and Industry (STI) undertakes a wide range of activities to better understand how information and communication technologies (ICTs) contribute to sustainable economic growth, social well-being and the overall shift toward knowledge-based societies.

The OECD Digital Economy Papers series covers a broad range of ICT-related issues, both technical and analytical in nature, and makes selected studies available to a wider readership. It includes *policy reports*, which are officially declassified by an OECD committee, and occasionally *working papers*, which are meant to share early knowledge and elicit feedback. This document is a working paper.

Working papers are generally only available in their original language – English or French – with a brief summary in the other. The opinions expressed in these papers are the sole responsibility of the author(s) and do not necessarily reflect those of the OECD or of the governments of its member countries.

STI also publishes the OECD Science, Technology and Industry Working Paper series, which covers a broad range of themes related to OECD's research and policy work on knowledge-based sources of economic and social growth and, more specifically, on the translation of science and technology into innovation.

OECD Digital Economy Papers and
STI Working Papers are available at:
www.oecd.org/sti/working-papers

REGULATION OF TRANSBORDER DATA FLOWS UNDER DATA PROTECTION AND PRIVACY LAW

Christopher Kuner
Tilburg University, The Netherlands

ABSTRACT

Transborder data flows have become increasingly important in economic, political, and social terms over the 30 years since the adoption, in 1980, of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. A fundamental change in the business and technological environment for data processing is also taking place, driven by developments such as the increased globalisation of the world economy; the growing economic importance of data processing; the ubiquity of data transfers over the Internet; greater direct involvement of individuals in transborder data flows; the changing role of geography; and growing risks to the privacy of individuals. Despite these fundamental changes in the data processing landscape, and the growth in the regulation of transborder data flows in numerous countries, there has been little attempt so far to conduct a systematic inventory of such regulation at a global level; to examine the policies underlying it; and to consider whether those policies need to be re-evaluated. This study is designed to describe the present status of transborder data flow regulation, and to provoke reflection about its aims, operation, and effectiveness, now and in the future.

RÉSUMÉ

Les flux de données transfrontières ont pris une importance de plus en plus grande en termes économiques, politiques et sociaux au cours des trente dernières années, soit depuis l'adoption, en 1980, des Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel. L'environnement commercial et technologique du traitement des données connaît aussi de profonds bouleversements, déterminés par des évolutions comme la mondialisation croissante de l'économie, l'importance économique croissante du traitement des données, l'ubiquité des transferts de données sur l'Internet, l'implication plus directe des individus dans les flux de données transfrontières, l'évolution du rôle de la géographie et les risques croissants pour la vie privée des individus. En dépit de ces changements fondamentaux dans le paysage du traitement des données, et du développement de la réglementation des flux de données transfrontières dans de nombreux pays, il n'y guère eu jusqu'à présent de tentatives d'inventaire systématique de ces réglementations au niveau mondial, d'examen des politiques sur lesquelles elles reposent, ni de réflexion sur la nécessité ou non de réévaluer ces politiques. La présente étude a pour objet de décrire la situation actuelle en matière de réglementation des flux de données transfrontières et d'entamer une réflexion sur ses objectifs, son fonctionnement et son efficacité, maintenant et dans l'avenir.

ABOUT THE AUTHOR

Christopher Kuner is a partner in the Brussels office of Hunton & Williams, a visiting researcher at the Tilburg Institute for Law, Technology and Society (TILT) at Tilburg University, the Netherlands, and a research fellow at the law faculty of the University of Copenhagen, Denmark. Mr. Kuner is also chairman of the Task Force on Privacy and the Protection of Personal Data of the International Chamber of Commerce (ICC), and of the European Privacy Officers Forum (EPOF), He is author of the book *European Data Privacy Law: Corporate Compliance and Regulation* (2nd ed. Oxford University Press, 2007), and editor-in-chief of the journal *International Data Privacy Law* published by Oxford University Press. In 2012 he will be a visiting fellow at the Centre for European Legal Studies at the University of Cambridge.

TABLE OF CONTENTS

SUMMARY

Transborder data flows have become increasingly important in economic, political, and social terms over the thirty years since the adoption, in 1980, of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. A fundamental change in the business and technological environment for data processing is also taking place, driven by developments such as the increased globalisation of the world economy; the growing economic importance of data processing; the ubiquity of data transfers over the Internet; greater direct involvement of individuals in transborder data flows; the changing role of geography; and growing risks to the privacy of individuals. Despite these fundamental changes in the data processing landscape, and the growth in the regulation of transborder data flows in numerous countries, there has been little attempt so far to conduct a systematic inventory of such regulation at a global level; to examine the policies underlying it; and to consider whether those policies need to be re-evaluated.

This study is designed to describe the present status of transborder data flow regulation, and to provoke reflection about its aims, operation, and effectiveness, now and in the future. It considers only legal issues, in particular only those arising under data protection and privacy law; only examines rules that explicitly regulate the flow of data across national borders; takes a global approach; uses the terms 'data protection' and 'privacy' interchangeably; and covers transborder data flows in both the private and public sectors. The study defines 'regulation' broadly to include not only legal rules that specifically restrict transborder data flows, but also those that require parties exporting or importing personal data to take certain acts, such as putting a compliance framework in place to protect the data. Terms like 'personal data', 'transborder data flows', and 'data transfer' are also construed broadly. While reasonable effort has been made to consider the subject comprehensively, this study is not intended to be an exhaustive survey of the details of regulation in all jurisdictions.

The first examples of regulation of transborder data flows under data protection and privacy law can be found in data protection laws passed in various European countries in the 1970s. In the 1980s various international organisations enacted instruments dealing with the subject, most prominently the OECD Guidelines. The first relevant instrument enacted at the regional level was Convention 108 of the Council of Europe. The EU Data Protection Directive, which is the regional instrument containing the most detailed rules regulating transborder data flows, has been particularly influential. In 2004 APEC enacted its Privacy Framework, which member countries may enact voluntarily, and which provides protection for personal data transferred internationally based on the principle of accountability.

Over sixty countries have adopted data protection or privacy laws that regulate transborder data flows, most of which are largely based on one or more of these international and regional instruments. These national laws have been enacted in nearly all regions of the world, including North (Canada) and Latin (Argentina, Colombia, Mexico, Uruguay) America; the Caribbean (the Bahamas); all member states of the European Union and the European economic area, and several other European countries (Albania, Bosnia and Herzegovina, Switzerland, etc.); Africa (Benin, Burkina Faso, Mauritius, Morocco, South Africa, Tunisia, etc.); the Near and Middle East (the Dubai International Financial Centre and Israel); Eurasia (Armenia); and the Asia-Pacific region (Australia, Macau, New Zealand, South Korea, etc.). In addition to laws and legislation, a variety of voluntary and private-sector mechanisms may regulate transborder data flows. Initiatives are currently underway in many regions and countries to review national and regional approaches, and to consider whether an international instrument on data protection and privacy could be adopted.

Regulation of transborder data flows derives from various distinct legal traditions and cultures, depending on the originating country or region; for example, in some regions (like the EU) data protection and privacy laws may have the quality of legally-binding human rights instruments, while in others they may be based more on realising the benefits of electronic commerce (as in the APEC region). Regulation of transborder data flows performs a protective function designed to prevent the fundamental principles of data protection and privacy law from being circumvented, but it is not itself a fundamental principle of the law.

Some types of regulation are more geographically-based, while other types make data exporters accountable for ensuring the continued protection of personal data transferred to other organisations no matter what their geographic location. There are also significant differences in the mechanisms required under data protection and privacy law to provide a legal basis for transborder data flows. While it is questionable how widely such regulation is enforced, it can have an effect on important data processing decisions made by data controllers. The Internet has given individuals a greater direct involvement in the transborder transfer of their personal data than ever before, but at the same time transborder data flow regulation has become more complicated and less transparent, and thus less understandable for individuals.

Regulation also differs in the 'default position' that it takes regarding transborder data flows. Some instruments presume that data flows should generally be allowed, but give regulators the power to block or limit them in certain circumstances, while others proceed from the assumption that personal data may not flow outside the jurisdiction unless a legal basis is present. At the same time, many instruments on transborder data flows show the influence of multiple approaches.

Four policies seem to be the main motivations for regulation of transborder data flows, namely preventing circumvention of national data protection and privacy laws; guarding against data processing risks in other countries; addressing difficulties in asserting data protection and privacy rights abroad; and enhancing the confidence of consumers and individuals. Transborder data flows bring not only risks, but also benefits, and with the globalisation of the world economy, the ability to transfer personal data internationally is assuming ever-increasing importance in promoting economic and social development. The ability to conduct transborder data flows may also protect privacy, by allowing the exercise of fundamental rights beyond the control of authoritarian governments. However, little 'hard' research has been done to confirm the effects of transborder data flow regulation.

Since one of the main motivations for transborder data flow regulation is the possibility that personal data may be transferred across national borders in order to circumvent legal protections, the need for such regulation is reduced to the extent that data protection and privacy law is harmonised. Nevertheless, for a variety of reasons, the likelihood that a legally-binding data protection instrument of global application will be enacted in the foreseeable future appears slim. In practice, the subjects of transborder data flow regulation and applicable law are often intertwined, and countries may use rules on applicable law to protect data transferred beyond their borders. In particular, data protection and privacy law may be applied to the processing of data transferred outside the country, thus using rules on applicable law to serve the same purpose as regulation of transborder data flows. Rules on applicable law and jurisdiction with regard to data protection and privacy law are notoriously unclear, which can create problems in particular for individuals, who often may not be able to determine which law applies to the processing of their personal data, and to which national regulatory authorities they may turn if a problem arises.

The following are some important issues requiring further attention.

There is increasing tension between regulatory approaches based on geography (like those dependent on the 'adequacy' of data protection in foreign jurisdictions) and those that are more organisationally-based (such as under the accountability principle). What is needed is a way for the geographical and organisational approaches to co-exist. One solution could be a mixture of the two approaches, i.e. organisationally-based approaches that allow geography to be considered in making decisions about whether the transfer of personal data abroad is appropriate. Increased cooperation between data protection and privacy regulators can help minimize the problems caused by differences in the approaches to transborder data flow regulation.

There are two default positions in transborder data flow regulation, namely either presuming that data flows should be allowed, but leaving the possibility for regulators to block or limit them, or presuming that data flows should not take place unless a legal basis for the transfer is present. Neither of the two default positions seems inherently better than the other, each one has inherent advantages and disadvantages, and which one a country selects will largely depend on its own culture, history, and legal tradition. However, the position selected must be accompanied by measures to avoid its inherent disadvantages, otherwise the first position will tend to be too reactive, and the second one will be excessively bureaucratic.

Regulation of transborder data flows was originally designed to prevent the circumvention of national data protection law. As the volume of transborder data flows has dramatically increased, the policies behind such regulation have shifted. Policymakers need to consider the rationales behind regulation of transborder data flows more closely. Transborder data flows should also be seen as a phenomenon that may bring both risks and benefits: while the transfer of personal data to countries with lower standards of protection may produce risks, the transfer to countries with higher standards of protection may bring increased protection of privacy, it addition to economic benefits.

There is often a close connection between regulation of transborder data flows and rules dealing with applicable law and jurisdiction, and applicable law rules are sometimes used to protect data processed abroad in situations beyond the reach of transborder data flow regulation. Insufficient attention has been given to the interface between these two sets of issues, and they need to be studied in more detail by experts in both data protection law and private international law.

The growing popularity of phenomena like cloud computing will put increasing pressure on regulatory systems for transborder data flows, and make it imperative that they bring about a good level of compliance at a reasonable cost. Thus, it is crucial that efficiency be given priority in designing regulation of transborder data flows. Regulatory efficiency is also important so that compliance with legal requirements is affordable for the numerous small and medium-sized enterprises (SMEs) that transfer personal data across borders and cannot afford large compliance departments.

The economic, legal, and social importance of transborder data flows is not adequately recognised at the highest levels of government. Indeed, the topic is too often regarded as a niche area of interest only to data protection and privacy specialists. Thus, ministers and government officials at the highest levels should grant international data flows the same attention as they do international flows of capital and international trade.

Much more needs to be done by governments to seek transparency in transborder data flow regulation. In particular, it can be difficult to obtain reliable and timely information on such regulation, since many countries seem to view the subject as one of solely national importance, whereas in a globalised world there is often a need for persons and organisations outside the jurisdiction to obtain information about it. Countries should thus increase transparency about transborder data flow regulation by

making available on the Internet the current text of any national regulation of transborder data flows; providing regular updates in a timely fashion regarding any revised or new regulation; and designating a contact point in the government (for example, in a ministry or data protection authority) to which questions about transborder data flow regulation can be addressed. Greater transparency also needs to be created for individuals, such as by having privacy notices giving information about transborder data flows drafted in clearer language; limiting the use of consent to transfer data; increasing cross-border regulatory co-operation; and having data controllers provide greater transparency with regard to the location and identity of entities they use to process and store personal data.

Finally, much important research remains to be done in areas such as measuring the economic effects of transborder data flows; the benefits and costs of regulation; and the attitudes of individuals. Further policy instruments and practical tools could also be drafted. The various international organisations working in the field of transborder data flow regulation should co-operate in such initiatives.

INTRODUCTION

Transborder data flows have become increasingly important in economic, political, and social terms over the 30 years since the adoption, in 1980, of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (hereinafter the 'OECD Guidelines' or 'the Guidelines').[1] Personal data are now crucial raw materials of the global economy; data protection and privacy have emerged as issues of concern for individuals; and confidence in data processing and privacy protection have become important factors to enable the acceptance of electronic commerce. The international transfer of increasing amounts of personal data and the growth of electronic commerce have resulted in economic growth and efficiencies that have had a positive impact around the world, while at the same time subjecting the privacy of individuals to risks that could not have been imagined thirty years ago.

The legal protection of privacy on a global scale began with human rights instruments such as the Universal Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966, while data protection as a related area dates back to the first such laws that were enacted in the 1970s. Data protection law has now spread around the world, and legislation has been enacted by a wide variety of jurisdictions.

Data protection and privacy legislation often regulates the movement of personal data across national borders; while such movement may be designated by a variety of terms,[2] it will be referred to herein as 'transborder data flows', since this is the term used in the OECD Guidelines.[3] Despite the importance of such transfers, many governments still seem oblivious to their economic and social impact. Indeed, transborder data flows have too often been considered to be a 'niche' subject of interest only to data protection and privacy specialists.

The global economy is currently undergoing an 'information explosion', which can 'unlock new sources of economic value, provide fresh insights into science and hold governments to account'.[4] Another author refers to a 'massive growth in the complexity and volume' of global data flows, accompanied by a change in the nature of such transfers in that they no longer constitute point-to-point transmissions, but 'occur today as part of a networked series of processes made to deliver a business result'.[5]

These developments represent a fundamental change in the business and technological environment for data processing. At the time the OECD Guidelines were approved, transborder data flows were typically understood to refer to point-to-point transfers such as the 'exchange of internal company administrative information, response to requests for service by customers, and maintenance of records concerning or describing customers or subjects'.[6] By contrast, many transborder data flows today involve multiple computers communicating through a network in a distributed fashion (in particular via phenomena such as 'Web 2.0', online social networking, search engines, and cloud computing). The following are some of the main developments that have changed the data processing landscape since the Guidelines were adopted:

- **The increased globalisation of the world economy.** As described by the World Bank, 'over the last few decades, the pace of this global integration has become much faster and dramatic because of unprecedented advancements in technology, communications, science, transport and industry'.[7] This has included the wholesale reduction of capital controls (such as exchange controls, and controls on the international sale or purchase of various financial assets),[8] and the liberalization of international trade through the succession of General Agreement on Tariffs and Trade (GATT) trade rounds and the foundation of the World Trade Organization (WTO).

- **The growing economic importance of data processing.** The processing of personal data has assumed a growing economic importance in the past few years. The industry for data analytics alone has been estimated to be worth over USD 100 billion, and to be growing at almost 10% annually.[9]

- **The ubiquity of data transfers over the Internet.** In the past, transborder data flows often occurred when there was the explicit intent to transfer data internationally (*e.g.* when a computer file was deliberately sent to a specific location in another country). Nowadays, the architecture of the Internet means that even a transfer to a party in the same country may result in the message or file transiting via other countries, without the sender ever being aware of this.

- **Greater direct involvement of individuals in transborder data flows.** The development of new technologies and business models for processing personal data has led to a greater direct involvement of individuals in the way that their data are transferred across national borders. In particular, phenomena such as electronic commerce and online social networks have made it possible for individuals to initiate and control the transborder transfer of their personal data to a much greater extent than in the past. For example, online hotel reservation systems were already being used in the 1970s when the OECD Guidelines were drafted, but access was restricted to the companies participating in them, whereas nowadays individuals can make reservations via the Internet and thus input their personal data directly.

- **The changing role of geography.** While geography and territoriality are still the key factors for the application of data protection and privacy law, they have become less important from the business and technological points of view. Many companies structure their operations based on lines of business rather than geography, and technology allows the transfer of personal data without regard to national boundaries.

- **Growing risks to the privacy of individuals.** The above developments have all brought great economic and social benefits to individuals, but have also increased the risks of misuse of personal data, many instances of which involve transborder data flows. For example, there has been explosive growth in the scale and sophistication of attacks by criminals and hackers against users' personal data, which are often conducted across national borders via the Internet.

Despite these fundamental changes in the data processing landscape, and the growth in the regulation of transborder data flows in numerous countries, there has been little attempt to conduct a systematic inventory of such regulation; to examine the policies underlying it; and to consider whether those policies need to be re-evaluated.

This study is designed to describe the present status of transborder data flow regulation, and to provoke reflection about its aims, operation, and effectiveness, now and in the future. It was prepared in the context of the 30th anniversary of the OECD Guidelines, and is annexed to the report prepared by the OECD Secretariat to mark this occasion.

Before beginning, it is important to define the scope of the study:

- It only considers *legal* issues relevant to the regulation of transborder data flows. While other issues (such as economic and social ones) may be equally important, they require separate analysis.

- With a few exceptions, only issues that arise under data protection and privacy law are considered. Regulation of transborder data flows may arise in other areas of the law as well (e.g., under export control restrictions, financial services law, labour law, tax law, telecommunications law, etc.), but such issues are too specialised to be examined here.

- Many data protection laws regulate the transfer of personal data to third parties, in addition to any specific regulation of *transborder* data flows. For example, Japanese law restricts data transfers to third parties in general,[10] without containing a specific provision on international data transfers. While such general restrictions on data transfers may restrict international transfers as well, examining them would exceed the scope of this study. Thus, it is limited to examining rules that explicitly regulate the flow of data across national borders.

- It takes a global approach, and thus examines the relevant issues under the laws of many different countries and regions.

- There is no generally-accepted definition of the term 'privacy', but it will be used here in a broad sense to refer to protection of an individual's personal sphere. Data protection can be regarded as a specific aspect of privacy that gives rights to individuals in how data identifying them or pertaining to them are processed, and subjects such processing to a defined set of safeguards. While the terms 'data protection' and 'privacy' may not be synonymous, they are closely related, and will be used interchangeably here.

- This study defines 'regulation' broadly to include not only legal rules that specifically restrict transborder data flows, but also those that require parties exporting or importing personal data to take certain acts, such as putting a compliance framework in place to protect the data. For example, requiring data exporters to register transborder data flows with a regulatory authority before they are carried out may not seem to 'regulate' such flows under a strict interpretation of the term. However, registration of a database that will transfer personal data from numerous countries may involve considerable effort, and in some of those countries the regulatory authorities may have questions about the registration before they accept it (which may involve further cost, delay, and uncertainty), so that a registration requirement can impede or slow down implementation of data transfers. This broad definition of what constitutes 'regulation' is in line with modern regulatory scholarship.[11]

- Although reasonable effort has been made to consider the subject comprehensively, this study is not intended to be an exhaustive survey of the details of regulation in all jurisdictions. A document entitled 'Table of Data Protection and Privacy Law Instruments Regulating Transborder Data Flows', which contains citations to and excerpts from many such instruments from around the world, is being published separately.[12]

- It covers transborder data flows in both the private and public sectors. Certain types of data flows carried out by the public sector may give rise to special issues (e.g., those conducted for law enforcement purposes). However, already in the 1970s warnings were made about drawing a sharp boundary between data privacy rules in the public and private sectors,[13] which warnings are even more relevant today.

- The study is current up to 1 March 2011, and all hyperlinks have been checked as of that date.

Finally, the views expressed herein are solely those of the author, who is however greatly indebted to the following persons for their valuable assistance and suggestions: Marty Abrams; Amit Ashkenazi; Paula Bruening; Barbara Bucknell; Cédric Burton; Malcolm Crompton; Gary T. Davis; Michael Donohue; Anne-Marije Fontein-Bijnsdorp; Clarisse Girot; Paul De Hert; Jörg Hladjk; Yukiko Ko; John Kropf; Olivier Matter; Pablo Palazzi; Kenneth Propp; Olivier Proust; Anne Ruwet; Joan Scott; Blair Stewart; Jennifer Stoddart; Dan Jerker B. Svantesson; Micah Thorner; Mason Weisz; and my colleagues at the Tilburg Institute for Law, Technology, and Society.

HISTORY AND OVERVIEW OF TRANSBORDER DATA FLOW REGULATION

Definitions

Examination of transborder data flow regulation is plagued by a number of definitional uncertainties. For example, views as to whether certain types of data (such as Internet protocol (IP) addresses) constitute 'personal data' that are subject to data protection and privacy laws differ between the various data protection and privacy regimes.[14] There has also been controversy as to whether merely making personal data accessible on the Internet should be considered to result in an 'international data transfer'.[15]

For the purposes of this study, it seems best to consider terms such as 'personal data', 'transborder data flows', and 'data transfer' as broadly as possible. The rapid evolution of technologies and business models means that any definition of key terms that is too narrow is likely to be rapidly overtaken by events. Thus, such terms will be construed here widely to include most types of data and mechanisms that result in personal data flowing across national borders.

Early regulation

The first data protection law is generally considered to be that of the German federal state of Hessen, which was adopted in 1970 and did not contain any restriction on transborder data flows.[16] Shortly afterward, many European countries enacted data protection laws containing restrictions on transborder data flows; examples include the laws of Austria,[17] Finland,[18] France,[19] Ireland,[20] Luxembourg,[21] and Sweden.[22] The major motivation for regulation of transborder data flows in these early laws seems to have been avoiding the circumvention of legal protections on data processing by transferring personal data to countries without data protection laws.[23] The restrictions contained in these early laws range from a requirement to obtain an explicit authorisation from the data protection authority before transferring personal data outside the country (*e.g.* in Austrian and Swedish law); to adopting verbatim the provisions of Article 12 of Counsel of Europe Convention 108 (*e.g.* in Irish law); to a requirement that either the individual whose data were transferred had to consent to the transfer, or that the country of import had to have a data protection law with a similar level of protection (*e.g.* in Finnish law). However, despite these provisions, at the time the first data protection laws were drafted, the transborder flow of personal data seems to have been regarded as the exception rather than the rule.[24]

International instruments

The OECD Privacy Guidelines represent the first attempt to deal with transborder data flows from a global perspective. Adopted in 1980, the Guidelines are a non-binding set of principles that member countries may enact, and have the dual aim of achieving acceptance of certain minimum standards of privacy and personal data protection, and of eliminating, as far as possible, factors which might induce countries to restrict transborder data flows for reasons associated with such flows.[25] The Guidelines contain the following main provisions dealing with transborder data flows:

- Member countries are to consider in their legislation the implications for other member countries of domestic processing and the re-export of personal data (para. 15).

- Member countries should take 'all reasonable and appropriate steps' to ensure that transborder flows of personal data (including transit of data) are uninterrupted and secure (para. 16).

- Member countries should refrain from restricting transborder flows of personal data between themselves, except where the recipient country 'does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation'. A member country is also allowed to impose restrictions 'in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection' (para. 17).

- Member countries are to 'avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection' (para. 18).

In 1990 the United Nations issued its Guidelines concerning Computerized Personal Files, which take the form of a non-binding guidance document.[26] The UN General Assembly has requested 'governmental, intergovernmental and non-governmental organisations to respect those guidelines in carrying out the activities within their field of competence'.[27] The Guidelines state in paragraph 9 that 'when the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands'.

Regulation of transborder data flows may restrict the provision of services across borders, which may give rise to questions under the General Agreement on Trade in Services (GATS), a treaty of the World Trade Organization (WTO) that entered into force in 1995.[28] Data protection regulation (including regulation of transborder data flows) is exempted from scrutiny under the GATS, but only as long as it does not represent a disguised restriction on trade.[29]

Governments have also concluded international agreements providing privacy protections for personal data transferred between jurisdictions for law enforcement purposes. For example, such agreements have been concluded between the EU and the United States covering the transfer of passenger name record (PNR) data of airline passengers[30] and of financial messaging data.[31] The 'High Level Contact Group', which is comprised of officials from various entities of the EU and the United States government, has also agreed on a set of high-level principles to provide data protection and privacy protections for data transferred between the two for law enforcement purposes.[32]

Regional instruments

In 1981 the Council of Europe enacted its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (referred to here as 'Convention 108').[33] The Convention entered into force on 1 October 1985, and at the time this study was finalised had been ratified and acceded to by forty-two countries (mainly in Europe). Significantly, the Convention is open also for signature by countries that are not member states of the Council of Europe, though no non-member has so far enacted it.

Article 12 of Convention 108 provides that 'a Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party' (Article 12(2)). However, the Convention goes on to say that a Party may derogate from these provisions 'insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection', or 'when the transfer is made from its territory to the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph' (Articles 13(3)(a)-(b)).

In 2001 the Council of Europe adopted an Additional Protocol to the Convention, which provides that each party shall allow the transfer of personal data to a non-party only if an 'adequate level of data protection' is assured (Article 2(1) of the Additional Protocol). However, by way of derogation, such transfers are also allowed if 'domestic law provides for it because of specific interests of the data subject or legitimate prevailing interests, especially important public interests' (Article 2(2)(a)), or 'if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law' (Article 2(2)(b)). At the time this study was finalised, the Convention had been ratified or acceded to by forty-two countries, and the Additional Protocol by twenty-nine countries.

The Council of Europe has also adopted a Recommendation regulating the use of personal data in the police sector, which contains rules for the international transfer of personal data. Under the Recommendation, the communication of personal data 'to foreign authorities should be restricted to police bodies', and should only be permissible 'if there exists a clear legal provision under national or international law', or 'if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law'.[34] In addition, the possibility of data transfer under the above provisions is without prejudice to the protections of domestic law.

Perhaps the most influential legal instrument regulating transborder data flows is the EU Data Protection Directive 95/46 (the 'Directive').[35] Adoption of the Directive was spurred by cases in which the free flow of data between the member states of the European Communities was threatened by the varying levels of data protection applicable in them. In one famous case that occurred in 1989, the French subsidiary of the Italian automobile company Fiat was only allowed by the French data protection authority to transfer employee data to Italy once a data transfer agreement between the two companies had been signed, owing to a lack of data protection legislation in Italy.[36]

Under the Directive, which is legally binding in the twenty-seven EU member states and the three EEA member countries (Iceland, Liechtenstein, and Norway), the transfer of personal data within the EU and EEA may not be restricted based on the level of data protection.[37] However, data transfers to other countries are prohibited unless such country provides 'an adequate level of data protection' as determined by the European Commission,[38] or unless certain other conditions are fulfilled. Besides formal adequacy decisions, the Directive foresees other possibilities as legal bases for the international transfer of personal data, such as the signature of EU-approved standard contractual clauses between the data exporter and data importer;[39] or the application of various exceptions, such as when consent of the individual has been obtained,[40] that the transfer is necessary for the performance of a contract between the data subject and the controller,[41] or that the transfer is necessary to protect the vital interests of the individual.[42] The possibility of relying on such exceptions is limited; for example, the Article 29 Working Party (a consultative body composed of the various EU Member State data protection authorities) has indicated that 'consent is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question'.[43]

Member state implementations of the Directive vary, and result in considerable differences in national legal approaches to international data transfers.[44] Member state data protection authorities have also authorised the use of mechanisms for the transborder transfer of personal data beyond those explicitly recognised in the Directive, such as intra-company compliance programmes known as binding corporate rules (BCRs).[45] The EU Directive has been influential in inspiring a number of other countries around the world to adopt regulations on transborder data flows; examples include a number of African countries, Argentina, the Dubai International Financial Centre, and Russia.

The EU has also enacted a decision to provide a common level of data protection in the processing of personal data by the police and judicial authorities. Under Article 13 of the Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, personal data may only be transferred from member state law enforcement authorities to third countries or international bodies if certain conditions are fulfilled, including that such country or international body ensures an adequate level of protection for the data processing (though a number of exceptions to this requirement are provided).[46]

In 2004, the twenty-one member economies of the Asia-Pacific Economic Cooperation (APEC) group agreed on the APEC Privacy Framework, which is a set of privacy principles that member economies may implement voluntarily.[47] The Framework protects personal data transferred outside the APEC member state where they were collected by recourse to the principle of 'accountability' (the accountability principle applies to data protection compliance in general, though discussion of it in this study will be limited to transborder data flows).[48] The accountability approach, which was first mentioned in the context of data protection in the OECD Guidelines,[49] 'ensures that the original collector of the personal information remains accountable for compliance with the original privacy framework that applied when and where the data was collected, regardless of the other organisations or countries to which the personal data travels subsequently'.[50] The APEC framework foresees that organisations (such as companies) may adopt Cross-Border Privacy Rules (CBPRs) as a way to apply protections across the organisation no matter where the data are processed.[51]

Some APEC member economies have implemented the accountability approach in their own data protection legislation. For example, accountability is used under the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), and the concept is also contained in the Australian Government's draft Privacy Principles that were released for consultation in June 2010.[52] Accountability does not specifically restrict transborder data flows, but imposes compliance responsibilities on parties that transfer personal data internationally. As the Office of the Privacy Commissioner of Canada has explained, 'PIPEDA does not prohibit organisations in Canada from transferring personal information to an organisation in another jurisdiction for processing. However under PIPEDA, organisations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement'.[53] On a practical level, accountability may require organisations to take steps such as implementing appropriate privacy policies which are approved by senior management and implemented by a sufficient number of staff; training employees to comply with these policies; adopting internal oversight and external verification programmes; providing transparency to individuals as to the policies and compliance with them; and adopting mechanisms to enforce compliance.[54]

However, the APEC Privacy Framework is not a monolithic or uniform approach. Because it is relatively new, there is little experience of how it will work in practice, besides the experience in those countries that have already implemented a similar system. Since the Framework is voluntary, it is also unclear how many members will implement it; in fact, at present APEC members have their own approaches to privacy protection, which cover a wide range of positions. Implementation of the Framework may not necessarily require legislation, but can also be accomplished through mechanisms like industry self-regulation,[55] meaning that divergence is likely to continue even between those countries that have implemented it. The APEC Framework does not have binding legal effect as would result, for example, from conclusion of an international treaty, and its provisions are subject to derogation by mandatory rules of national law.[56]

Certain formalities of national law may also have the practical effect of regulating the transborder transfer of personal data, even if they are not solely or specifically designed to do so. For example, the laws of a number of EU Member States,[57] and of some non-EU countries,[58] require data controllers to notify the processing of personal data, including transborder data flows, to data protection authorities,

which may then have powers to block the transfers or impose conditions on them.[59] Even if the data flow is not blocked, such requirements can lead to significant delays in carrying out the transfers.

National legislation

In the course of the last few decades over 60 countries have adopted data protection or privacy laws that regulate transborder data flows, most of which are largely based on one or more of the international and regional instruments discussed earlier. Beginning in Europe, such laws have spread to all regions of the world, including North (Canada) and Latin (Argentina, Colombia, Mexico, Uruguay) America; the Caribbean (the Bahamas); all Member States of the European Union and the European Economic Area, and several other European countries (Albania, Bosnia and Herzegovina, Switzerland, etc.); Africa (Benin, Burkina Faso, Mauritius, Morocco, South Africa, Tunisia, etc.); the Near and Middle East (the Dubai International Financial Centre and Israel); Eurasia (Armenia); and the Asia-Pacific region (Australia, Macau, New Zealand, South Korea, etc.). Some countries are also currently in the process of adopting data protection and privacy legislation which includes regulation of transborder data flows (*e.g.* in Barbados, Malaysia, and South Africa), or of amending their existing regulation of transborder data flows (*e.g.* in Australia). In Hong Kong, privacy legislation is in force, but the specific provision dealing with transborder data flows is not.

The above list does not include those countries which are bound by international legal instruments like the Additional Protocol to Council of Europe Convention 108, and those that are eligible to participate in voluntary systems such as the APEC Privacy Framework (which by itself covers twenty-one countries). In addition, transborder data flow regulation exists not only at the national level, but also at the state level in a number of federal countries.[60] If one includes all such instruments, then the number of countries regulating transborder data flows in some form, or that have the possibility of doing so, is close to 100.

Conspicuous by their absence from the list of countries with transborder data flow regulation are some of the major world economies like Brazil, China, India, Japan, and the United States. However, economic growth over the long term is likely to be higher in developing countries than in the more developed economies,[61] and many developing countries have adopted regulatory frameworks for transborder data flows. Taking African countries as an example, their motivations for enacting such frameworks include the promotion of electronic commerce,[62] the protection of private life,[63] and the protection of privacy in connection with large-scale government data collection projects (*e.g.* digitalisation of the electoral rolls).[64] This demonstrates that the motivations for enacting regulation of transborder data flows in the developing world are similar to those in the more developed countries, and that such regulation is a global phenomenon.

Voluntary and private sector mechanisms

In addition to laws and legislation, a variety of voluntary and private-sector mechanisms may regulate transborder data flows. For example, the US-EU Safe Harbor framework can be adopted voluntarily by organisations based in the United States that import personal data from the EU,[65] and gives rise to legally-binding obligations, among which are protections for 'onward transfers' of personal data.[66] The EU also recognises data transfer mechanisms such as binding corporate rules[67] and standard contractual clauses,[68] which can be entered into voluntarily but then become legally-binding.

Codes of practice and standards may also contain restrictions on transborder data flows. For example, the Voluntary Model Data Protection Code for the Private Sector of the Infocomm Development Authority of Singapore (IDA) and the National Trust Council of Singapore (NTC) provides that where data are to be transferred to someone (other than the individual or the organisation or its employees) inside or outside of Singapore, the organisation shall take reasonable steps to ensure that the data will not be processed

inconsistently with the Code.[69] The Treasury Board of Canada has adopted guidance setting certain data processing standards for public bodies that contract for services (including situations where this will result in personal data being transferred outside of Canada).[70] And the International Organization for Standardization (ISO) is presently working on privacy standards, although it is unclear if they will contain rules on transborder data flows.

While such instruments are not obligatory in the same way that legislation is, some of them can become legally binding on the parties that adopt them. Even when not legally-binding, they may become widely used by parties that transfer personal data across national borders, thus creating a 'web' of data transfer regulation that applies across organisations as well as between countries. Data transfer restrictions that are applied either as private-sector instruments or as guidelines or codes of practice will likely assume increasing importance in coming years.

Future directions

The regulation of transborder data flows has gradually evolved over the last several decades. The first laws enacted in the 1970s tended to make transborder data flows contingent on strict conditions being fulfilled, such as that the transfer was approved by the local data protection authority. Later instruments added further options for legalizing transborder data flows (such as the use of standard contractual clauses). Recently more sophisticated instruments have been developed to provide protection for transborder data flows across organisations, such as binding corporate rules (BCRs) in the European Union and cross-border privacy rules (CBPRs) under the APEC Framework.

Some important regional data protection instruments (*e.g*. the EU Data Protection Directive) are currently being reviewed, with a view to making the legal regime for transborder data flows under them more effective and efficient. Discussions are also ongoing between data protection regulators, civil society groups, international organisations, and multinational companies about how the principle of accountability could be used as a way both to facilitate data flows in a globalised world and to protect the personal data and privacy of individuals. While the details of an accountability approach are still being worked out, it seems that the concept may prove useful in helping to bridge the various approaches to the governance of transborder data flows.

Because of the diversity of national data protection and privacy legislation, there have been growing calls for a global legal instrument on data protection, resulting in the publication in November 2009 of the 'The Madrid Resolution', a set of international standards for data protection and privacy.[71] The Resolution contains a provision dealing with international data transfers, which provides that international data transfers may be carried out when the country of data import affords the level of protection provided in the Resolution.[72] In addition, the document allows protection to be afforded by other means, such as contractual clauses or binding corporate rules.[73] The Resolution further allows countries to authorise data transfers in situations similar to those covered in the exceptions in Article 26(1) of the EU Directive (*e.g*. when the data subject consents, etc.).[74] Finally, national data protection authorities are empowered to make data transfers subject to authorisations before being carried out.[75]

ISSUES AND ANALYSIS

Legal nature of the various approaches

Regulation of transborder data flows derives from a number of distinct legal traditions and cultures, depending on the originating country or region. For example, some regional legal instruments (*e.g*. Council of Europe Convention 108,[76] the European Convention on Human Rights,[77] and the Charter of Fundamental Rights of the European Union[78]) view data protection as a fundamental human right. Other instruments may not be based on human rights law, and may not be legally binding. For example, a scan of the APEC Privacy Framework reveals that the terms 'fundamental right' and 'human right' are not used at all in the document, and the purpose of the Framework is defined in terms of realising the benefits of electronic commerce.[79]

Even when data protection is considered to be a human right, the regulation of transborder data flows is generally not considered to be a 'core' principle of the law. For example, in the Madrid Resolution, regulation of transborder data flows is not included in Part II which lists 'basic principles' of data protection (lawfulness and fairness, purpose specification, proportionality, data quality, openness, and accountability), but is contained in a separate section (section 15). Similarly, in the EU Directive, the provisions on transborder data flows are not included in the section containing the core rules of data processing ('Chapter II: General Rules on the Lawfulness of the Processing of Personal Data'), but in a separate section ('Chapter IV: Transfer of Personal Data to Third Countries'). This view is supported by the decision of the European Court of Justice in the case *Bodil Lindqvist*, where the Court referred to Article 25 of the EU Directive (which regulates international data transfers) as a 'regime of special application', contrasting it with the 'general regime' under Chapter II of the Directive that sets forth the conditions for the lawful processing of personal data.[80]

Regulation of transborder data flows focuses on policies like preventing circumvention of the law and guarding against data processing risks where the data are received, and if these policies are not implicated (for example, because the law of the countries of export and import have been harmonised), then the necessity of regulating transborder data flows is lessened or eliminated. Such regulation thus performs a protective function designed to prevent the fundamental principles of data protection and privacy law from being circumvented, but regulation of transborder data flows is not itself one of those fundamental principles.

Geographically-based versus organisationally-based regulation

The geographically-based approach aims to protect against risks posed by the country or location to which the data are to be transferred, while the organisationally-based approach targets risks posed by the organisations which receive the data. Many countries have adopted the geographically-based approach, including all the EU member states, and other countries such as Argentina, Morocco, and Russia. Various tests for the permissibility of data transfers are contained in national legislation following the geographically-based approach, such as whether the legal regime in the country of data import is 'adequate' (EU Directive), 'comparable' (Canadian federal law), or 'equivalent' (Convention 108) to that of the country of data export.

The organisationally-based approach is exemplified by the APEC Privacy Framework, which makes data exporters accountable for ensuring the continued protection of personal data transferred to other organisations no matter what their geographic location, and is also followed at the national level in some other countries (*e.g*. in Canada). However, there is often a certain degree of overlap between the two approaches; for example, the EU legal framework also recognizes particular instruments that legitimise

transborder data flows within organisations, like binding corporate rules[81] and standard contractual clauses.[82]

Compliance in practice

There are significant differences in the mechanisms required under data protection and privacy law to provide a legal basis for transborder data flows. Some countries (particularly those subject to the EU Directive) require that certain formalities be observed before the transfer takes place, such as that the transfer be registered with the data protection regulator before personal data may be transferred.[83] Other countries that do not specifically restrict transborder data flows may impose compliance responsibilities on entities that transfer personal data outside the country's borders. For example, under Canadian law data controllers are expected to take steps so that data transferred outside of Canada will receive protection in the country of import, *e.g*. by confirming that the data importer provides training to its staff on privacy protection, has adopted effective data security measures, and grants the data controller rights of audit and inspection.[84]

Despite the large number of laws regulating transborder data flows, it is questionable how widely such regulation is enforced. In its first report on transposition of the Data Protection Directive published in 2003, the European Commission noted with regard to compliance with the Directive's provisions on international data transfers that 'many unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection. Yet there is little or no sign of enforcement action by the supervisory authorities'.[85] The fact that some of the largest economies in the world (such as China and Japan) have not been the subject of a formal EU adequacy decision means that there must be substantial non-compliance at least with regard to data flows from the EU to those countries.

In many cases the authorities may not have sufficient resources or personnel to properly monitor compliance with transborder data flow regulation. For example, one study revealed that eleven out of twenty-seven national data protection authorities in the EU member states were unable to carry out the entirety of their tasks because of a lack of financial and human resources.[86] This suggests that the authorities are only able to enforce data transfer requirements on a piecemeal basis.

At the same time, regulation can have an effect on important data processing decisions made by data controllers, notwithstanding the relative lack of enforcement. For example, on 15 June 2007, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), a co-operative association located in Belgium owned by thousands of financial institutions and providing worldwide secure message and payment services, announced that it would change the architecture of its data processing system so that data flowing between European countries would be stored only in Europe (rather than being mirrored in the US as was previously the case), based on considerations of data protection.[87] The author is aware from his experience as a practicing lawyer of many other cases in which transborder data flow regulation played a significant role in business decisions, such as in deciding whether a particular project involving the international transfer of personal data should proceed, and in determining where to locate data processing operations.

The increasing complexity of regulation governing transborder data flows also creates difficulties for individuals. On the one hand, the Internet has given individuals a greater direct involvement in the transborder transfer of their personal data than ever before. On the other hand, regulation has become more complicated and less transparent, and thus less understandable for individuals. For example, many transborder data flows are conducted based on the consent of the individual, but there is growing concern that individuals may not understand what they are consenting to, and that they may not have a meaningful opportunity to refuse consent.[88] The greater use of cloud computing technologies also means that it will

become increasingly difficult for individuals to exercise their rights with regard to data stored in other countries.

Differences in the 'default position'

The laws and instruments also differ in the 'default position' that they take regarding transborder data flows. Some instruments (*e.g.*, the OECD Guidelines and the new legislation in New Zealand[89]) presume that data flows should generally be allowed, but give regulators the power to block or limit them in certain circumstances, while others (most notably the EU Directive) proceed from the assumption that personal data may not flow outside the jurisdiction unless a particular legal basis is present.

Many instruments on transborder data flows show the influence of multiple approaches, and even those as seemingly divergent as the EU's 'adequacy' approach and the 'accountability' approach used in the APEC Privacy Framework are likely to grow closer over time. For example, the Article 29 Working Party has called for the principle of accountability to be explicitly incorporated into EU data protection law,[90] and some national DPAs in Europe have also expressed interest in it.[91] Some jurisdictions using the accountability approach also recognise that the flow of personal data across national borders may raise concerns about the level of privacy protection.[92] Moreover, at least one of the APEC countries (namely Russia) has adopted a data protection law which is heavily influenced by the EU Directive.

Risks and underlying policies

The policies underlying regulation of transborder data flows are based on the perceived risks that can arise from transferring personal information across national borders. These risks have been articulated as follows by the State Services Commission of New Zealand:[93]

- non-compliance with national law;
- unauthorised release of personal information;
- inability to provide individuals with access to their personal information;
- inability to co-operate with national regulators regarding complaints;
- inability of the national regulator to investigate or enforce the law;
- inability to guarantee the protection of personal information in countries without privacy or data protection laws;
- conflicts between foreign laws and national law;
- possible access to data by foreign governments;
- overseas judicial decisions that might require the disclosure of data;
- problems with recovery or secure disposal of data;
- loss of trust if data are transferred and misused.

These risks can be associated with the following four policies, which seem to be the main motivations for regulation of transborder data flows, even if they are often not explicitly articulated:

- **Preventing circumvention of national data protection and privacy laws.** Perhaps the most frequently-cited motivation for regulation of transborder data flows has been to avoid circumvention of national data protection law. At the time the first legislation was passed, there were only a few laws protecting privacy and data protection rights, and so circumvention of the law was a real concern. However, the number of laws has increased dramatically, thus reducing the chances that data can be transferred to a jurisdiction where no privacy protection applies. It is also unclear what constitutes 'circumvention' of the law in this context: the term could be used in a subjective sense, such as when a party transfers data with the primary purpose of evading application of the law, or in an objective sense, such as when the primary purpose of transferring the data is a business factor (*e.g.* optimisation of business processes, cost considerations, factors relating to IT infrastructure, etc.) other than evasion of the law.

- **Guarding against data processing risks in other countries.** In some cases, transborder data flow regulation has been enacted because of concerns about data processing risks in other countries. For example, some Canadian provinces have enacted such regulation specifically because of concerns that the United States government would use the 'Patriot Act' to gain access to data of Canadian citizens and residents if such data were outsourced for data processing in the United States or to 'United States-linked' companies in Canada.[94] Service providers doing business in China have also been compelled to reveal data to Chinese law enforcement authorities,[95] which has given rise to fears about access to data stored in cloud computing services in China.[96]

- **Difficulties in asserting data protection and privacy rights abroad.** The difficulty of asserting data protection rights outside the country of export has been cited as an important policy rationale underlying regulation of transborder data flows.[97] The OECD has recognised that individuals and regulators may have increased difficulties in enforcing their data protection and privacy rights across national borders.[98] For example, in the European Union, various legal instruments and obligations provide individuals and regulators with a framework that allows the assertion of rights with regard to EU-based data processing. Thus, EU data protection authorities are obliged to co-operate with each other,[99] and often do so in practice.[100] Court decisions from one EU member state can also be enforced in another member state with relative ease.[101] However, the same legal instruments do not apply to situations where a non-EU country is involved, meaning that such enhanced regulatory co-operation and ease of enforcement may not be possible. The difficulty of asserting legal rights abroad is not unique to data protection and privacy law, but results from the fact that there is no global legal framework for the assertion of consumer rights, or for the recognition and enforcement of court decisions in other countries. However, the assertion of privacy rights is increasingly based on formal or informal co-operation between regulators outside of traditional legal assistance channels;[102] examples are provided by the Global Privacy Enforcement Network[103] and the APEC Cross-border Privacy Enforcement Arrangement.[104] There is also ever-increasing use of internal dispute resolution mechanisms in both the private and public sectors,[105] which may enhance the ability of individuals to assert their rights in other countries.

- **Enhancing the confidence of consumers and individuals.** Regulation of transborder data flows may help increase the confidence of individuals in the processing of their personal data. Data protection authorities have received complaints from individuals regarding data transfers abroad,[106] though the number does not seem to be large.[107] The increasing complexity of data processing on the Internet caused by phenomena such as cloud computing and outsourcing can make it difficult for individuals to obtain information as to where their personal data are

being processed and stored, which may lead to a loss of confidence. On the other hand, some studies demonstrate a lack of interest by individuals in the regulation of transborder data flows.[108] Parties that export personal data across national borders may also not comprehend the ubiquity of transborder data flows: for example, in a study by the European Commission published in 2008, only a small percentage (10%) of data controllers stated that their companies transferred personal data outside the European Union,[109] a figure that must be too low given the widespread use by companies of e-mail and the Internet.

Benefits of transborder data flows

The OECD Guidelines recognise the economic and social benefits of transborder data flows,[110] and with the globalisation of the world economy, the ability to transfer personal data internationally is assuming ever-increasing importance in promoting economic and social development. As the World Economic Forum has stated, the use of information and communication technologies, many of which operate via the Internet and thus rely on the ability to conduct transborder data flows, 'is a key element of infrastructure for efficient industries and a critical productivity enhancer' that 'is crucial for sustaining recovery and laying the foundations for economies that are competitive in the long term'.[111]

The ability to conduct transborder data flows may also protect privacy, by allowing the exercise of fundamental rights beyond the control of authoritarian governments. For example, in 2010 the government of the United Arab Emirates (UAE) threatened to ban use of the BlackBerry messaging service, since it results in messages being encrypted during transmission to the service's central servers in Canada, meaning that they cannot be accessed by UAE government agencies.[112] Since Canada has privacy laws at both the federal and provincial level, whereas the emirates making up the UAE seem to have no omnibus privacy laws, the transfer of data to the BlackBerry servers in Canada may result in a higher level of privacy protection than they would receive in the UAE.

Regulation of transborder data flows may bring economic benefits, as it may make other countries more willing to transfer personal data to a country with such legislation.[113] At the same time, the latter may also carry economic costs. For example, a study of the impact of Canadian provincial legislation restricting transborder data flows revealed that it caused 'fewer services available to Canadian public bodies and residents, increased bureaucracy and significantly reduced efficiency, higher financial costs, the threat of tangible harms to health and safety, and the undermining of competition for public bodies' business and of Canada's burgeoning services industry'.[114] However, little 'hard' economic or social research has been done to confirm the effects of transborder data flow regulation.

Role of legal harmonisation

Since one of the main motivations for transborder data flow regulation is the possibility that personal data may be transferred across national borders in order to circumvent legal protections, the need for such regulation is reduced to the extent that data protection and privacy law is harmonised.[115] For example, Article 1(1) of the EU Directive obligates all EU member states to protect the fundamental rights and freedoms of natural persons regarding their right to privacy with respect to the processing of personal data, and Article 1(2) then requires member states not to restrict the free flow of personal data between them for reasons relating to the level of protection. While the global harmonisation of data protection and privacy law is a subject beyond the scope of this study, the issue is thus relevant to the rationale for regulation of transborder data flows.

Most data protection legislation is based on the same international documents (like the OECD Guidelines, Council of Europe Convention 108, the APEC Privacy Framework, etc.), so that the fundamental, high-level principles of the law are similar across regions and legal systems. However, the

differences in the cultural, historical, and legal approaches to data protection mean that once one descends from the highest level of abstraction, there can be significant differences in detail. This is not surprising, since concepts such as 'data protection' and 'privacy' are derived from national legal culture and tradition, and thus vary considerably around the world, even in systems that accept the same fundamental principles.

The likelihood that a legally-binding data protection instrument of global application will be enacted in the foreseeable future appears slim for a variety of reasons, in particular because of the difficulty of agreeing on the form of the legal framework, selecting the standards on which such an instrument would be based, determining the scope of the instrument, and agreeing on an international organisation to co-ordinate the work.[116] However, the Madrid Resolution[117] represents a useful first step to define global data protection standards, and it is possible that harmonisation of the law may proceed gradually, in which case the rationale for regulation of transborder data flows would decrease.

Applicable law and jurisdiction

In practice, the subjects of transborder data flow regulation and applicable law are often intertwined, and countries may use rules on applicable law to protect data transferred beyond their borders.

For example, personal data may generally not be transferred outside the geographic boundaries of the EU without a legal basis, which may require the continued application of EU law to the processing of the data in other countries. Thus, under EU law, certain legal bases for international data transfers (*e.g.* signature of EU-approved standard contractual clauses between data exporter and data importer that impose data processing obligations based on EU law) result in the application of EU data protection standards in other countries where personal data are processed. Moreover, EU standards are then also applied to further transfers from the data importer to third parties (so-called 'onward transfers').[118]

In addition, rules on applicable law may mandate the application of EU data protection law in some cases involving the transfer of personal data outside the EU even when an 'international data transfer' under the rules on transborder data flows is not considered to take place. For example, when an individual in the EU enters data in an Internet search engine or uploads data onto an online social network operated from a server outside the EU, this is not generally considered to result in an 'international data transfer', but it does result in the direct applicability of EU law to the data processing based on Article 4(1)(c) of the EU Directive.[119] Application of Article 4(1)(c) is designed to avoid the circumvention of EU law,[120] which, as explained above, is also the main justification given for regulation of transborder data flows. Thus, the EU rules on applicable law and those concerning the regulation of transborder data flows may both serve the same purpose.

Regulation in other regions may also apply data protection and privacy law to the processing of data transferred outside the country. The APEC Privacy Framework seems to provide that the protections of the law of the place from which the data were transferred 'attach to' the data and continue to be applicable as they are transferred abroad.[121] Further examples are provided by the Privacy Act of New Zealand, certain provisions of which apply to information held outside that country,[122] and the draft Privacy Principles of the Australian government, which make the entity transferring data abroad liable for breaches of the Principles committed outside Australia by the data importer.[123]

In addition, rules on applicable law and jurisdiction with regard to data protection and privacy law are notoriously unclear,[124] which can create problems in particular for individuals, who often may not be able to determine which law applies to the processing of their personal data, and to which national regulatory authorities they may turn if a problem arises.

CONCLUSIONS AND RECOMMENDATIONS

This study can only give a broad overview of the most important issues concerning regulation of transborder data flows and raise some questions requiring further attention, in particular the following:

Reconciling the geographical and organisational approaches

Countries show a diversity of approaches to transborder data flow regulation. One of the central themes in this regard is the increasing tension between approaches based on geography (such as those dependent on the 'adequacy' of data protection in foreign jurisdictions) and those that are more organisationally-based (such as under the accountability principle). This tension is a feature not only of data protection and privacy regulation, but of any regulation that is territorially-based, as most data protection and privacy law is. In a globalised world, geographically-based regulation will naturally come into conflict with the fact that geography matters less in a business and technological sense than it used to. And while regulation of capital flows and international trade has been liberalised in the last few decades, regulation of transborder data flows has been tightened. Thus, there is an inherent tension between the liberalisation of restrictions on the flow of capital and the use of transborder services on the one hand, and the regulation of transborder data flows on the other hand.

The first regulation of transborder data flows enacted in the 1970s was based mainly on geography, but there has been a gradual trend toward regulation that focuses on the organisation processing the data. One reason for this is the difficulty of determining whether a particular privacy regime is 'adequate', 'comparable', or 'equivalent' based on the standards of the country of export; indeed, it is not clear exactly what these terms mean or whether there is any meaningful distinction between them. The procedures used in the EU to reach decisions on adequacy are widely viewed as overly burdensome and inefficient,[125] and since the Directive was adopted only a relatively small number of 'adequacy' decisions has been issued by the European Commission.[126] Political considerations may also come into play when determining the adequacy of data protection and privacy regimes in other countries.[127]

However, geography will continue to play a role in the regulation of transborder data flows, since 'human beings tend to cluster geographically, based on shared cultures, languages, tastes, wealth, and values'.[128] There will always be cases where individuals become concerned about the processing of their personal data outside the borders of their country, based, for example, on a perceived risk of access to the data by foreign law enforcement, the chance of a breach of data security, or some other potential danger. Data controllers may also prefer to keep data within a particular region, and some cloud computing service providers already grant customers the option of keeping data within a national or regional 'cloud'. Thus, the market for data processing services, driven by demand from both data controllers and individuals, will increasingly allow them to choose whether to restrict the transborder transfer of their personal data. Geography will also remain important with regard to law enforcement access to data, since more and more governments are likely to demand that entities offering communications in their countries also maintain communications equipment there, in order to facilitate such access.[129]

What is needed is a way for the geographical and organisational approaches to co-exist. One solution could be a mixture of the two approaches, *i.e.* organisationally-based approaches that allow geography to be considered in making decisions about whether the transfer of personal data abroad is appropriate. An example is provided by the Guidance Document on contracting decisions published by the Treasury Board of Canada, which applies the principle of accountability,[130] but also allows the locations to which the data are to be transferred to be considered as a factor in the analysis. Under this approach, the location to which the data are exported is not the sole consideration in determining whether data export is appropriate, but is

one factor to be considered in a risk analysis based on *i*) the sensitivity of the personal information, *ii*) the expectations of the individuals to whom the information relate, and *iii*) the potential injury if personal information is wrongly disclosed or misused.[131] The draft Australian Privacy Principles also seek to blend the geographical and organisational approaches.[132] A risk analysis that takes geography into account could be carried out by the organisation seeking to export the data, and by a regulatory authority if so required by the applicable law.

While harmonisation of the law could help reduce the friction between the geographical and organisational approaches, it is likely to take place slowly, with many fits and starts. In the meantime, increased co-operation between data protection and privacy regulators can help minimize the problems caused by differences in the approaches to transborder data flow regulation. Such co-operation already exists, but could be increased to provide enhanced possibilities for cross-border enforcement of the law. In some cases this may require governments to amend their laws in order to allow the cross-border sharing of information between regulatory authorities.[133]

Determining the default regulatory position

The two default positions either presume that data flows should be allowed, but leave the possibility for regulators to block or limit them, or presume that such flows should not take place unless a legal basis for the transfer is present.

Neither of the two default positions seems inherently better than the other, each one has inherent advantages and disadvantages, and which one a country selects will largely depend on its own culture, history, and legal tradition. The first position (allowing transborder data flows unless specific risks are present) may prove too reactive and allow enforcement only after data misuse has already occurred, whereas the second one (requiring a legal basis before transfers take place) may unduly restrict data flows and prove increasingly futile in light of developments such as cloud computing. In order to minimize these disadvantages, if the first position is adopted, it should be accompanied by the following measures:

- steps to encourage pro-active compliance with the law (such as the promotion of trustmarks and privacy audits);
- granting sufficient resources and enhanced enforcement powers to regulators;
- enactment of rules to ensure the legal accountability of parties transferring personal data.

If the second position is adopted, it should be accompanied by measures such as the following:

- minimisation of bureaucratic restrictions (such as requiring regulatory filings or approvals for individual data transfers);
- encouragement of organisationally-based data transfer mechanisms (such as binding corporate rules or cross-border privacy rules);
- prioritisation of enforcement to focus on those transborder data flows that carry the greatest risks for individuals.

Thus, either of the default positions can work, but only if it is accompanied by measures to avoid its inherent disadvantages, otherwise the first position will tend to be too reactive, and the second one will be excessively bureaucratic.

Evaluating underlying policies

Regulation of transborder data flows was originally designed to prevent the circumvention of national data protection law. As the volume of transborder data flows has dramatically increased, the policies behind such regulation have shifted. When the first regulations were enacted, few countries had data protection laws, whereas now many do. Informal co-operation between regulatory authorities is increasing, so that concerns about individuals not being able to exercise their rights outside their own countries may be lessening. As data protection and privacy laws become more harmonised, the rationale for restrictions on transborder data flows may also diminish. On the other hand, there may be greater concern at present about data access by foreign governments than there was when the first transborder data flow regulation was enacted.

Policymakers need to consider the rationales behind regulation of transborder data flows more closely. For example, there has never been a detailed explanation of what is considered to be 'circumvention' of national data protection laws in the context of transborder data flows. Preventing circumvention of the law is a policy that is recognised in other areas of the law as well (for example, in German conflict of laws doctrine[134]), and examples from other areas of law could be useful in determining the scope of the policy against circumvention in the context of transborder data flows, and in deciding the extent to which it is a policy still worth pursuing.

Transborder data flows should also be seen as a phenomenon that may bring both risks and benefits. While the transfer of personal data to countries with lower standards of protection may produce risks for the processing of personal data, the transfer to countries with higher standards may bring benefits.

Reconciling applicable law and data transfer issues

There is often a close connection between regulation of transborder data flows and rules dealing with applicable law and jurisdiction, and applicable law rules are sometimes used to protect data processed abroad in situations where the use of transborder data flow regulation is unavailable. Insufficient attention has been given to the interface between these two sets of issues; expert bodies (such as the Hague Conference on Privacy International Law) could help by clarifying issues of applicable law and jurisdiction as they relate to transborder data flows.[135] Further clarity would also benefit individuals by increasing transparency as to which law governs the processing of their data and which regulatory authorities have jurisdiction. Taking EU law as an example, it seems redundant and inefficient to use two sets of legal provisions (those concerning applicable law and transborder data flows) to fulfil the same purpose, namely protecting personal data processed outside the geographic boundaries of the EU. There is also an increasing trend (expressed for example in the APEC Privacy Framework) to apply local law to data processing in other countries, which may lead to conflicts with mandatory legal provisions of the country of import, and will make it necessary to 'tag' the data and indicate which 'home' data protection regime attaches to it.[136]

Countries seem to be using a combination of applicable law rules and transborder data flow regulation to strive for a watertight legal framework under which personal data processing can be protected no matter where the data are transferred. However, they should be careful not to over-extend the jurisdictional reach of their data protection and privacy laws, in order to avoid creating international friction. Countries have in the past refused opportunities to enact global legal instruments protecting consumers in electronic commerce,[137] and it is unrealistic to expect that seamless legal protection around the world can be achieved under data protection and privacy law when this has not been realised in any other area of consumer protection law.

Furthering regulatory efficiency

Technology and data transfer practices will become increasingly complex as time goes by. In particular, the growing popularity of phenomena like cloud computing will put increasing pressure on regulatory systems for transborder data flows, and make it imperative that they bring about a good level of compliance at a reasonable cost. Thus, it is crucial that efficiency be given priority in designing regulation of transborder data flows. Since regulators are likely to have limited resources, this means that labour-intensive mechanisms such as regulatory approvals and the filing of application and registration forms should be disfavoured; mechanisms like codes of practice and targeted audits should be encouraged; and regulators should be given enhanced enforcement powers. Certain compliance functions (*e.g.* the operation of codes of practice and privacy seal programmes) could also in effect be 'outsourced' to private parties, with proper regulatory oversight. This is the only way that the regulation of transborder data flows has a chance of keeping up with advances in technology and business processes. The governance of transborder data flows seems to have become increasingly bureaucratised, and it is important that compliance requirements actually serve the purpose of protecting personal data, rather than being enacted for their own sake.

Regulatory efficiency is also important so that compliance with legal requirements is affordable for the numerous small and medium-sized enterprises (SMEs) that transfer personal data across borders and cannot afford large compliance departments or outside lawyers. The cost advantage of data processing services like cloud computing that inherently involve transborder data flows is likely to prove increasingly attractive to smaller enterprises, and it is crucial that regulation allows them to comply with legal requirements in an efficient and cost-effective way.

Recognising the importance of transborder data flows

Anecdotal evidence suggests that the economic, legal, and social importance of transborder data flows is not adequately recognised at the highest levels of government. Indeed, the topic is too often regarded as a niche area of interest only to data protection and privacy specialists. Thus, ministers and government officials should grant international data flows the same attention as they do international flows of capital and international trade; indeed, these topics are in many ways inseparable, since the ability to transfer personal data internationally is a vital component of the globalised economy.

Increasing transparency

Despite pledges by OECD governments to 'seek transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows',[138] much more needs to be done to promote such transparency. It can be difficult to obtain reliable and timely information on transborder data flow regulation, since many countries seem to view the subject as one of solely national importance, whereas in a globalised world there is often a need for persons and organisations outside the jurisdiction to obtain information about it.

Countries should thus increase transparency about transborder data flow regulation by taking steps such as the following:

- making available on the Internet the current text of any national regulation of transborder data flows, in multiple languages;

- providing regular updates in a timely fashion regarding any new or revised regulation;

- designating a contact point in the government (for example, in a ministry or data protection authority) to which questions about transborder data flow regulation can be addressed.

Countries and other governmental entities should co-operate in disseminating information about transborder data flow regulation; this could be done, for example, by making information available in a central repository maintained on the web site of an international organisation.

Greater transparency also needs to be created for individuals. This means that privacy notices giving information about transborder data flows should be drafted in clearer language; that the use of consent to transfer data should be limited; and that cross-border regulatory co-operation should be increased, so that individuals can more easily assert their rights with regard to data that have been transferred to other countries. Data controllers also need to provide greater transparency with regard to the location and identity of entities they use to process and store personal data.

Areas for further drafting and research

Much important research remains to be done regarding the regulation of transborder data flows. Among areas where research is needed are the economic effects of transborder data flows; the benefits and costs of regulation; and the attitudes of individuals to them.

Further policy instruments and practical tools could also be drafted, like guidelines to allow entities exporting personal data to define more precisely various risk levels as they relate to particular data export scenarios (similar to the Guidelines of the Treasury Board of Canada referred to above). In addition, many developing countries would likely benefit from the drafting of a model law dealing with transborder data flows, so that they do not always have to start from scratch or use a regional or national model when doing so. However, the drafting of a model law would require international agreement on the default rule for transborder data flows, which has so far been lacking.

It would be difficult to select a single international organisation to co-ordinate such work. Data protection and privacy is still seen as peripheral to the work of many international organisations, and there is not a single one that combines both the wide membership and specialised expertise to deal with all the ramifications of the topic. This is partly because data protection and privacy law does not neatly fall into a particular area of law, but is a mixture of various areas such as consumer protection, human rights law, and other areas.[139] Each of the organisations that deal with the topic brings strengths and weaknesses. In particular, those organisations with the most expertise in policy issues concerning transborder data flows (like the OECD) lack membership of developing countries,[140] while the various UN organisations tend not to have as much expertise in data protection and privacy law. Regional institutions also may be too closely tied to one region to deal with issues of a global nature. This argues for enhanced co-operation of a number of international organisations in order to make use of the strengths which each of them has.

ENDNOTES

[1] 23 October 1980, *www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html#memorandum*.

[2] For example, the APEC Privacy Framework uses the terms 'international transfer', 'information flows across borders', 'cross-border information flow', and 'cross-border data transfer' interchangeably. APEC Privacy Framework (2005), *www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx*.

[3] OECD Guidelines (n 1), para. 1(c).

[4] 'Data, data everywhere, A special report on managing information', The Economist, 27 February 2010, p. 3.

[5] See Paul M. Schwartz, 'Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment' (2009), *http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf*, p. 4.

[6] J.M. Carroll, 'The Problem of Transnational Data Flows', in: Policy Issues in Data Protection and Privacy, Proceedings of the OECD Seminar 24 to 26 June 1974, p. 201.

[7] See *http://youthink.worldbank.org/issues/globalization/*.

[8] See International Monetary Fund, 'Capital Controls: Country Experiences with their Use and Liberalization' (May 17, 2000), *www.imf.org/external/pubs/ft/op/op190/index.htm*>.

[9] 'Data, data everywhere' (n 4), p. 4.

[10] Kojinjoho no hogo ni kansuru horitsu [Japanese Personal Information Protection Act], Law No. 57 of 2003, Article 23.

[11] See Colin J. Bennett and Charles D. Raab, *The Governance of Privacy* (MIT Press 2006), pp. 117-119.

[12] The document will be available at *http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=1213479*.

[13] See F. Hondius, 'International Data Protection Action', in: Policy Issues in Data Protection and Privacy (n 6), 208, p. 216.

[14] *Compare* Article 29 Working Party, 'Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6' (WP 58, 30 May 2002), at 3, concluding that IP addresses are protected by EU data protection law, *with* Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 69 Fed.R.Serv.3d 173 (C.D. Cal. 2007), in which a US federal court found that IP addresses were not covered by the term 'personal information' contained in the defendants' website privacy policy.

[15] In the case of *Bodil Lindqvist*, Case C-101/01 [2003] ECR I-12971, para. 71, the European Court of Justice found that placing material on a server located in the EU which was accessible worldwide via the Internet did not constitute an international data transfer falling under the restrictions of Article 25 of the EU Data Protection Directive.

[16] Hessisches Datenschutzgesetz, 7 October 1970.

17 Österreichisches Datenschutzgesetz von 1978, pp. 32, 34.

18 Personal Data File Act & Personal Data File Decree, 30 April 1987, p. 22.

19 Loi no. 78-17 relative à l'informatique, aux fichiers et aux libertés, Article 24. However, note that the restrictions in Article 24 were to be regulated in a decree by the Conseil d'Etat which was never issued.

20 Data Protection Bill, 1987, superseded by the Data Protection Act 1998.

21 Loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques.

22 Swedish Data Act of 1973, Article 11.

23 See European Commission, Amended Proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(92) 422 final, 15 October 1992, p. 34, stating that without restrictions on international data transfers, 'the Community's efforts to guarantee a high level of protection for individuals could be nullified by transfers to other countries in which the protection provided is inadequate'.

24 See F. Hondius, 'International Data Protection Action', in: Policy Issues in Data Protection and Privacy (n 6), p. 208, stating that 'the vast majority of data processing operations take place within the limits of national frameworks, either in the private or in the public sector'.

25 OECD Guidelines, Explanatory Memorandum, para. 25.

26 UN Guidelines concerning Computerized Personal Data Files of 14 December 1990, UN Doc E/CN.4/1990/72.

27 UN Doc A/RES/45/95, 14 December 1990.

28 See Peter P. Swire and Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings Institution Press 1998), pp. 189-196.

29 GATS Article XIV(c)(ii).

30 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), [2007] OJ L204/18.

31 Council of the European Union, Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, 24 June 2010. See *www.statewatch.org/news/2010/jun/eu-usa-draft-swift-agreement-com-final-3.pdf*.

32 Reports by the High Level Contact Group (HLCG) on information sharing and privacy and personal data protection (23 November 2009), <http://register.consilium.europa.eu/pdf/en/09/st15/st15851.en09.pdf>.

33 28 January, 1981, ETS 108 (1981).

34 Council of Europe, Recommendation No. R(87)15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, Principle 5.4.

[35] Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31.

[36] See Commission nationale de l'informatique et des libertés, 10e rapport d'activité, p. 32 (1989).

[37] EU Data Protection Directive, Article 1(2).

[38] Ibid., Article 25.

[39] Ibid., Article 26(2).

[40] Ibid., Article 26(1)(a).

[41] Ibid., Article 26(1)(c).

[42] Ibid., Article 26(1)(e).

[43] Article 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (WP 114, 25 November 2005), p. 11.

[44] See Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd ed. Oxford University Press 2007), pp. 162-166.

[45] See, *e.g.,* Article 29 Working Party, 'Working document setting up a framework for the structure of binding corporate rules' (WP 154, 24 June 2008).

[46] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2008] OJ L350/60.

[47] The APEC member economies include Australia; Brunei Darussalam; Canada; Chile; the People's Republic of China; Hong Kong, China; Indonesia; Japan; the Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; the Republic of the Philippines; the Russian Federation; Singapore; Chinese Taipei; Thailand; the United States; and Vietnam.

[48] See APEC Privacy Framework (n 2), Principle 9, providing that a personal information controller 'should be accountable for complying with measures that give effect to the Principles…When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles'.

[49] OECD Guidelines, Accountability Principle (Paragraph 14).

[50] Malcolm Crompton, Christine Cowper and Christopher Jefferis, 'The Australian *Dodo* Case: An Insight for Data Protection Regulation' (26 January 2009) BNA Privacy & Security Law Report 180, p. 181.

[51] See APEC Data Privacy Pathfinder Projects Implementation Work Plan (Revised), APEC document 2009/SOM1/ECSG/SEM/027, *http://aimp.apec.org/Documents/2009/ECSG/SEM1/09_ecsg_sem1_027.doc*.

[52] Australian Government, 'Australian Privacy Principles, Exposure Draft' (24 June 2010), p. 15-17, *www.smos.gov.au/media/2010/docs/Privacy-reform-exp-draft-part-1.pdf*; and Australian Government,

'Australian Privacy Principles, Companion Guide' (June 2010), p. 13, *www.smos.gov.au/media/2010/docs/100622-privacy-part-1-Companion-Guide.pdf*.

53 Office of the Privacy Commissioner of Canada, 'Guidelines for Processing Personal Data across Borders' (2009), p. 5, *www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf*.

54 Galway Project and Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements, A Document for Discussion' (2009), *www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf*, pp. 11-14.

55 APEC Privacy Framework (n 2), p. 31.

56 Ibid., p. 8.

57 For example, Austria, the Netherlands, and Spain, among many others.

58 *E.g.*, Argentina Personal Data Protection Act 2000, Article 21(2)(e); Croatian Act on Personal Data Protection 2003, Article 14(10).

59 *E.g.*, Croatian Act on Personal Data Protection 2003, Article 34.

60 For example, in the German federal states and a number of Canadian provinces. See, *e.g.*, Hessisches Datenschutzgesetz § 17; Alberta Freedom of Information and Protection of Privacy Act § 40(1)(g); British Columbia Freedom of Information and Protection of Privacy Amendment Act § 30.1. See also Fred Cate, 'Provincial Canadian Geographic Restrictions on Personal Data in the Public Sector' (2008), *www.hunton.com/files/tbl_s47Details/FileUpload265/2312/cate_patriotact_white_paper.pdf*.

61 See, *e.g.*, Carnegie Endowment for International Peace, 'The World Order in 2050' (April 2010), *www.carnegieendowment.org/files/World_Order_in_2050.pdf*, p. 1, predicting that by 2050, 'traditional Western powers will remain the wealthiest nations in terms of per capita income, but will be overtaken as the predominant world economies by much poorer countries'.

62 See Government of Mauritius, Debate No. 12 of 01.06.04, Second Reading of the Data Protection Bill (No. XV of 2004), p. 2, stating that adoption of a data protection bill 'will also constitute a strong incentive for prospective overseas agencies to do business in Mauritius in the ICT sector proper, or in businesses where personal data is used routinely'.

63 See Burkina Faso, Assemblée Nationale, Dossier N°06 relatif au projet de loi portant sur la protection des données à caractère personnel, p. 3.

64 See République du Sénégal, Rapport sur le projet de loi N°32/2007 portant sur la protection des données à caractère personnel, p. 3.

65 See European Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, [2000] OJ L215/7.

66 See Onward Transfer Principle of the Safe Harbor Privacy Principles issued by the US Department of Commerce on 21 July, 2000, *www.export.gov/safeharbor/eu/eg_main_018475.asp*>.

67 See Article 29 Working Party, 'Working Document setting up a framework for Binding Corporate Rules' (n 45), p. 7.

68 See Commission Decision (EC) 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46/EC of the European Parliament and of the Council, [2010] OJ L39/5, Clause 11; Commission Decision (EC) 2004/915 of 27 December 2004 amending Decision (EC) 2001/497 as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, [2004] OJ L385/74, Clause 2.

69 Voluntary Model Data Protection Code for the Private Sector (Version 1.3 final), Principle 4.1.1.

70 Treasury Board of Canada, 'Taking Privacy into Account Before Making Contracting Decisions' (2006), www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp-eng.rtf>.

71 The Madrid Resolution, 'International Standards on the Protection of Personal Data and Privacy' (2009).

72 Ibid., para. 15(1).

73 Ibid., para. 15(2).

74 Ibid., para. 15(3).

75 Ibid.

76 See Article 1, referring to the individual's 'right to privacy, with regard to automatic processing of personal data relating to him'.

77 Article 8, together with case law interpreting it, such as *Rotaru v Romania* (App no 28341/95) ECHR 2000-V.

78 Article 8, [2000] 2000/C364/01.

79 See APEC Privacy Framework (n 2), p. 3, stating that 'APEC economies realize that a key part of efforts to improve consumer confidence and ensure the growth of electronic commerce must be cooperation to balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region'.

80 C-101/01 [2003] ECR I-12971, paras. 63 and 69; see above n 15.

81 See n 67.

82 See n 68.

83 See RAND Europe, 'Review of the European Data Protection Directive' (2009), *www.rand.org/pubs/technical_reports/2009/RAND_TR710.pdf*, pp. 34-35.

84 Office of the Privacy Commissioner of Canada, 'Guidelines for Processing Personal Data across Borders' (n 53), p. 6. See also Galway Project and Centre for Information Policy Leadership, 'Data Protection Accountability: The Essential Elements, A Document for Discussion' (n 54), p. 11, stating 'An accountable organisation demonstrates commitment to accountability, implements data privacy policies linked to recognised outside criteria, and establishes performance mechanisms to ensure responsible decision-making about the management of data consistent with organisation policies'.

85 European Commission, 'First Report on the implementation of the Data Protection Directive (95/46/EC)' COM(2003) 265 final (15 May 2003), *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT*, p. 19.

86 European Union Agency for Fundamental Rights, 'Data Protection in the European Union: the Role of National Data Protection Authorities' (2010), <http://fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf>, p. 42.

87 See SWIFT press release of 4 October 2007, *www.swift.com/about_swift/legal/compliance/statements_on_compliance/swift_board_approves_messaging_re_architecture/index.page*?.

88 See, *e.g.*, Fred H. Cate, 'The Failure of Fair Information Practice Principles', in: Jane K. Winn (ed.), *Consumer Protection in the Age of the Information Economy* (Ashgate 2006), also online at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972*.

89 See Privacy (Cross-border Information) Amendment Bill 221-2 (2008), Part 11A, *www.legislation.govt.nz/bill/government/2008/0221/latest/DLM1362819.html*.

90 See Article 29 Working Party, 'The Future of Privacy' (WP 168, 1 December 2009), p. 3.

91 See Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 'Ein modernes Datenschutzrecht für das 21. Jahrhundert' (18 March 2010), pp. 14-16, in which the conference of German DPAs calls for incorporation of the accountability principle in German data protection law, as a way to ensure legal responsibility in data processing situations involving multiple data controllers.

92 Office of the Privacy Commissioner of Canada, 'Guidelines for Processing Personal Data across Borders' (n 53), p. 3, stating that cross-border transfers 'do raise some legitimate concerns about where the personal information is going as well as what happens to it while in transit and after it arrives at some foreign destination'.

93 See State Services Commission of New Zealand, 'Government Use of Offshore Information and Communication Technologies (ICT) Service Providers: Advice on Risk Management' (2009), www.e.govt.nz/library/offshore-ICT-service-providers-april-2007.pdf, pp. 6-7, 14-15, and pp. 26-27.

94 See, *e.g.*, Information & Privacy Commissioner for British Columbia, 'Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing' (October 2004), *www.oipc.bc.ca/images/stories/sector_public/archives/usa_patriot_act/pdfs/report/privacy-final.pdf*, recommending the enactment of restrictions on the outsourcing of data under the control of Canadian public bodies based on concerns about access to such data by the US government under the Patriot Act; such restrictions have been enacted in Alberta, British Columbia, Nova Scotia, and Québec.

95 See Luke O'Brien, 'Yahoo betrayed my husband', Wired, 15 March 2007, www.wired.com/politics/onlinerights/news/2007/03/72972, regarding a case in which the Chinese government arrested a political dissident based on information that was provided to it by Yahoo.

96 See Jonathan Zittrain, 'Lost in the Cloud', New York Times, 19 July 2009, *www.nytimes.com/2009/07/20/opinion/20zittrain.html?_r=1*.

97 See, *e.g.*, Article 29 Working Party, 'Opinion 7/2001 on the Draft Commission Decision (version 31 August 2001) on Standard Contractual Clauses for the Transfer of Personal Data to Data Processors Established in Third Countries under Article 26(4) of Directive 95/46' (WP 47, 13 September 2001), p. 3, stating that 'the physical location of the data in third countries makes the enforcement of the contract or the decisions taken by Supervisory Authorities considerably more difficult'.

98 See OECD, 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy' (2007), *www.oecd.org/dataoecd/43/28/38770483.pdf*.

99 EU Data Protection Directive, Article 28(6).

100 For example, a DPA of an EU member state informed the author that it receives 20 to 30 cooperation requests annually from other EU DPAs.

101 *E.g.*, under Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2001] OJ L12/1.

102 See, *e.g.*, OECD, 'Report on the Cross-Border Enforcement of Privacy Laws' (2006), *www.oecd.org/dataoecd/17/43/37558845.pdf*, pp. 23-24.

103 See *www.privacyenforcement.net/*.

104 See 'APEC launches new Cross-border Data Privacy Initiative', *www.apec.org/Press/News-Releases/2010/0716_ecsg_cpea.aspx*.

105 See OECD, 'Report on Compliance with, and Enforcement of, Privacy Protection Online' (12 February 2003), *www.oecd.org/officialdocuments/displaydocument/?doclanguage=en&cote=dsti/iccp/reg(2002)5/final*, p. 14.

106 See, *e.g.*, OECD, 'Report on the Cross-Border Enforcement of Privacy Laws' (2006), *www.oecd.org/dataoecd/17/43/37558845.pdf*, at 8-9; Office of the Privacy Commissioner of Canada, 'Revisiting the Privacy Landscape a Year Later' (March 2006), *www.priv.gc.ca/information/survey/2006/ekos_2006_e.cfm*, in which 94% of respondents express either moderate or high concern about Canadian companies transferring personal information on customers to other countries.

107 See, *e.g.*, OECD, 'Report on the Cross-Border Enforcement of Privacy Laws' (n 102), p. 9, stating that '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'.

108 See Eurobarometer Study (for the European Commission), 'Data Protection in the European Union--Citizens' Perceptions--Analytical Report', February 2008, *http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf*, at 33, indicating that only 17% of EU citizens are aware of European legal restrictions on transborder data flows.

109 Eurobarometer Study (for the European Commission), 'Data Protection in the European Union--Data Controllers' Perceptions--Analytical Report', February 2008, *http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf*, p. 7.

110 See OECD Guidelines (n 1), noting that 'transborder flows of personal data contribute to economic and social development'.

111 World Economic Forum, 'Global Information Technology Report 2009-2010', *www.weforum.org/pdf/GITR10/GITR%202009-2010_Full%20Report%20final.pdf*, p. vii.

112 Margaret Coker, Tim Falconer and Phred Dvorak, 'UAE Puts the Squeeze on Blackberry', Wall Street Journal, 31 July 2010, *http://online.wsj.com/article/SB10001424052748704702304575402493300698912.html?mod=WSJEUROPE_hpp_LEFTTopStories*.

113 See New Zealand Privacy Commissioner, 'Privacy amendment important for trade and consumer protection' (26 August 2010), *www.privacy.org.nz/media-release-privacy-amendment-important-for-trade-*

and-consumer-protection/, quoting the New Zealand Privacy Commissioner as follows regarding amendments to the New Zealand Privacy Act that restrict international data transfers: 'An EU adequacy finding is also likely to satisfy data export requirements of other countries. I believe New Zealand businesses are already losing some trading opportunities through a gap in our privacy laws. This change will allow New Zealand to compete on a secure basis for international data business'.

114 Cate (n 60), p. 2.

115 See OECD Guidelines, Explanatory Memorandum, para. 8, stating that a consensus on data privacy principles 'would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws'.

116 See International Law Commission, 'Report on the Work of its Fifty-Eighth Session' (1 May to 9 June and 3 July to 11 August 2006) UN Doc A/61/10, at 499, stating that data protection is an area 'in which State practice is not yet extensive or fully developed'. See also Christopher Kuner, 'An international legal framework for data protection: Issues and prospects', 25 Computer Law & Security Review 307 (2009).

117 See n 71.

118 See, *e.g.*, Commission Decision (EC) 2004/915 of 27 December 2004 amending Decision (EC) 2001/497 as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, [2004] OJ L385/74, Clauses II(i) and III; Safe Harbor Onward Transfer Principle, *www.export.gov/safeharbor/eu/eg_main_018475.asp*.

119 See Article 29 Working Party, 'Opinion 5/2009 on online social networking' (WP 163, 12 June 2009), pp. 5-7.

120 See C de Terwagne and S Louveaux, 'Data Protection and Online Networks', 13 Computer Law and Security Report 234, 238 (1997).

121 APEC Privacy Framework (n 2), Principle IX. Accountability, at 31, *www.apec.org*, stating 'Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred'.

122 New Zealand Privacy Act 1993, section 10; Law Commission of New Zealand, 'Review of the Privacy Act 1993' (March 2010), *www.lawcom.govt.nz/sites/default/files/publications/2010/03/Publication_129_460_Part_17_Chapter-14-Trans-border%20Data%20Flows.pdf,* at 389-390.

123 See Australian Government, 'Australian Privacy Principles, Companion Guide' (n 52), p. 13.

124 See, *e.g.*, European Commission, 'Comparative Study on Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments', Final Report, 20 January 2010, <http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf>, p. 24, referring to the 'ambiguity and different implementation of the "applicable law" rules' of EU data protection law.

125 See regarding problems with the EU system for reaching adequacy determinations Article 29 Working Party, 'The Future of Privacy' (n 90), pp. 10-11, stating that the process for reaching adequacy decisions should be 'redesigned'.

126 At the time this study was finalized, such adequacy decisions covered Argentina; Canadian organizations subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA); the Bailiwick of Guernsey; Israel; the Bailiwick of Jersey; the Isle of Man; Switzerland; the US safe harbor system; and transfers of airline passenger data to the US Department of Homeland Security (DHS).

127 An example occurred in July 2010, when the government of Ireland delayed an EU adequacy decision for Israel based on alleged Israeli government involvement in the forging of Irish passports.

128 Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2008), p. 183.

129 See, *e.g.*, 'India says BlackBerry agrees to give it real-time access to corporate messages' (6 September 2010) BNA Privacy & Security Law Report 1241, quoting the Indian Home Secretary as stating 'All people who operate communications services in India should have a server in India…'

130 Treasury Board of Canada, 'Guidance Document' (n 70), p. 2: 'Each institution is responsible and accountable for any personal information under its care'.

131 Ibid. at 7 and Annex A.

132 See Australian Government, 'Australian Privacy Principles, Companion Guide' (n 52), pp. 12-13.

133 See OECD, 'Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy' (2007) (n 98), at 7, 9, 11; Law Commission of New Zealand, 'Review of the Privacy Act 1993' (n 122) , pp. 398-399.

134 See Gerhard Kegel, *Internationales Privatrecht* (6th ed. Verlag C.H. Beck 1987), p. 303, explaining that the fact that actions were taken with the intent to circumvent otherwise applicable law may be taken into account when determining which law to apply to a dispute.

135 See Hague Conference on Private International Law, 'Cross-Border Data Flows and Protection of Privacy' (13 March 2010), <*http://www.hcch.net/upload/wop/genaff2010pd13e.pdf*>.

136 See Paula J. Bruening and K. Krasnow Waterman, 'Data tagging for new models of information governance', 8 IEEE Security & Privacy 64 (Sept.-Oct. 2010), *http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5601491*.

137 See, *e.g.*, United Nations Commission on International Trade Law (UNCITRAL), Report of the Working Group IV (Electronic Commerce) on the work of its fortieth session, Vienna, 14-18 October 2002, UN Document A/CN.9/527, p. 20, in which countries decided against including consumer matters in the scope of the 2005 United Nations Convention on the Use of Electronic Communications in International Contracts.

138 Declaration on Transborder Data Flows (Adopted by the Governments of the OECD Member Countries on 11th April 1985), *www.oecd.org/document/32/0,3343,en_2649_34255_1888153_1_1_1_1,00.htm*.

139 See Jon Bing, 'Data Protection, Jurisdiction and the Choice of Law' (1999) Privacy Law & Policy Reporter 92, *www.austlii.edu.au/au/journals/PLPR/1999/65.html*.

140 Michael Kirby, 'The History, Achievement and Future of the 1980 OECD Guidelines on Privacy', 1 International Data Privacy Law 6, at 14, asking what the OECD should do 'to ensure the consideration of representative opinions from developing countries in the expression of the values that will impact on global technology'.