his advice is of secondary importance. His contribution to the global debate is, in any case, rich and stimulating, at times thought-provoking, and well documented and worth reading.

Peter Hustinx
European Data Protection Supervisor

Brussels
December 2012

Preface

This book examines how the transfer of personal data across national borders is regulated under data protection and privacy law, draws conclusions about its legal nature and underlying policies, and proposes improvements based on theories of legal pluralism. Since the 1970s a number of international institutions, and over 70 countries in all regions of the world, have enacted data protection and privacy laws regulating transborder data flows, yet the topic does not seem to have received a comprehensive, internationally-oriented legal analysis since a few pioneering works in the 1980s and 1990s.

It seeks to refute the view one sometimes encounters that transborder data flow regulation is a narrow subject of interest only to data protection specialists. On the contrary, the subject has significant implications for many other areas of the law besides data protection, such as public and private international law, human rights law, and regulation of the Internet. Because of the broad scope of the topic, inspiration has been drawn from these other areas. Despite what may seem to be an emphasis on European law, I have tried to deal with the topic from a global perspective.

I have done my best to go into sufficient detail on specific topics, without covering all the intricacies of national law, and keeping in mind the maxim that 'nothing should ever be published except where the author has something new to say and can say it in such simple and clear language that all readers can understand it.'[1] The book is current as of 1 January 2013. The analysis is informed by my experience as a practising lawyer and a participant in the work of international organizations, and by information gleaned over many years from discussions with data protection regulators, diplomats, and company privacy officers. It has been written without any ideological 'agenda', and contains solely my personal views and not those of any organization with which I may be affiliated.

My first exposure to this topic occurred while working on behalf of the International Chamber of Commerce (ICC) to negotiate a set of standard contractual clauses with the European Commission. I learned much from this experience, and from colleagues such as Susan Binns, Dr Ulf Brühann, Leonardo Cervera-Navas, Pascale Gelly, Marisa Jimenez, and Rocio Mendez. I am also grateful to the ICC for the opportunity to become part of so many interesting international initiatives. Participation in meetings of the T-PD group of the Council of Europe over the last decade has been invaluable, as has the chance to prepare two reports

[1] F.A. Mann, unpublished manuscript, quoted in Lawrence Collins, 'F.A. Mann', in Jack Beatson and Reinhard Zimmerman (eds), *Jurists Uprooted: German-Speaking Émigré Lawyers in Twentieth-century Britain* 381 (OUP 2004), at 438.

1

Background and Introduction

A. Growth of transborder data flows

1. The changing economic, social, and technological landscape

The global economy is undergoing an 'information explosion' that can 'unlock new sources of economic value, provide fresh insights into science and hold governments to account'.[1] There has been 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'.[2] 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

[1] 'Data, data everywhere—A special report on managing information', *The Economist*, 27 February 2010, at 3.

[2] 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>, at 4.

processing and privacy protection have become important factors in enabling the acceptance of electronic commerce. The international transfer of personal data has 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 new and increased risks.

In the 1970s, the term 'transborder data flows' was typically understood to refer to point-to-point data 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'.[3] By contrast, many transborder data flows today involve multiple partners (ie, persons, organizations) communicating through networks 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 landscape for transborder data flows over the last few decades.

- *The increased globalization 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 because of unprecedented advancements in technology, communications, science, transport and industry'.[4] This has included the wholesale reduction of capital controls (eg, exchange controls, and controls on the international sale or purchase of various financial assets),[5] 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 become a vital component of economic growth. As European data protection regulators have noted, 'In some sectors, particularly in the on-line environment, personal data has become the de facto currency in exchange for on-line content'.[6] The industry for data analytics alone has been estimated to be worth over US$100 billion, and to be growing at almost 10 per cent annually.[7]
- *The social and cultural importance of online activity* With the growth of the Internet, the ability to transfer data around the world online has attained a huge importance in social and cultural terms. The Internet and other online media have become indispensable tools for individuals to communicate globally, and have furthered individual participation in the political process,

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

[4] See <http://youthink.worldbank.org/issues/globalization/>.

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

[6] Article 29 Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173, 13 July 2010), at 5.

[7] 'Data, data everywhere' (n 1), at 4.

increased transparency of governmental activities, and promoted fundamental rights (a well-known example is the use of Internet communications and online social media in the popular 'Arab Spring' uprisings in 2011[8]).

- *The ubiquity of transborder data flows* In past decades, transborder data flows often only occurred when there was the explicit intent to transfer data internationally (eg, when a computer file was intentionally sent to a specific location in another country). Nowadays, the architecture of the Internet and technological solutions such as cloud computing mean 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.[9] As computing devices are routinely implanted in many varieties of implements used in daily life that communicate and process personal data via the Internet (the so-called 'Internet of Things'[10]), great volumes of personal data will be transferred internationally even without the direct involvement of a human being.
- *Increase in data transfers by States and data sharing between them* States (including governments and regulatory agencies) are now transferring an ever-growing amount of personal data across national borders for purposes that can include regulatory coordination, law enforcement, and many others.
- *Interaction between the public and private sectors in the processing of personal data* There is a growing interaction between data processing by private sector organizations, governmental entities, and public authorities. For example, public authorities often seek access to commercial databases maintained by private sector entities.
- *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 borders.
- *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

[8] See, eg, Journalist's Resource, 'The Arab Spring and the Internet: Research Roundup' (22 March 2012), <http://journalistsresource.org/studies/society/internet/research-arab-spring-internet-key-studies/>.

[9] See European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"', 16 November 2012, at 6, stating that cloud computing 'leads to a considerable increase of transfers of personal data over networks, involving many different parties and crossing borders between countries …', and that 'the physical location of the data is usually not known by the client …'

[10] See, eg, Commission of the European Communities, 'Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The Internet of Things—An Action Plan for Europe', COM(2009) 278 final, 18 June 2009.

as electronic commerce and online social networks have made it possible for individuals to initiate the transborder transfer of personal data more easily. At the same time, it has become more difficult for individuals to determine the ways in which data are transferred, and the location where they are processed.

- *Growing danger to the privacy of individuals* These developments have all brought great economic and social benefits, but have also increased the risks of misuse of personal data and of violations of the law. For example, there has been explosive growth in the scale and sophistication of criminal attacks against users' personal data conducted via the Internet.[11] Government access to and sharing of personal data may also create risks.[12]

2. Increase in the volume of data flows

The volume of transborder data flows has grown exponentially over the last few decades, which has driven a corresponding increase in transborder data flow regulation. This growth can be seen from a few examples:

> Wal-Mart, a retail giant, handles more than 1m customer transactions every hour, feeding databases estimated at more than 2.5 petabytes—the equivalent of 167 times the books in America's Library of Congress … Facebook, a social-networking website, is home to 40 billion photos. And decoding the human genome involves analysing 3 billion base pairs—which took ten years the first time it was done, in 2003, but can now be achieved in one week. All these examples tell the same story: that the world contains an unimaginably vast amount of digital information which is getting ever vaster ever more rapidly.[13]

The application of data analytics techniques to large amounts of personal data, including processing of the data for purposes that may be different than those for which they were originally collected, is known as the phenomenon of 'big data'. Such projects typically involve the transfer of data from numerous sources without regard to geography, and can have major benefits for society:

> The discovery of Vioxx's adverse drug effects, which led to its withdrawal from the market, was made possible by analysis of clinical and cost data collected by Kaiser Permanente, the California-based managed-care consortium. Had Kaiser Permanente not aggregated clinical and cost data, researchers might not have been able to attribute 27,000 cardiac arrest deaths occurring between 1999 and 2003 to use of the drug. Similarly, researchers in South Africa discovered a positive relationship between therapeutic vitamin B use and delay of progression to AIDS and death in HIV-positive patients … Another oft-cited

[11] See, eg, Symantec Corp., 'Internet Security Threat Report, Volume XV' (April 2010), <http://www4.symantec.com/Vrt/wl?tu_id=SUKX1271711282503126202>.

[12] Eg, when governmental law enforcement entities access personal data held by the private sector. See, eg, 'Systematic Government Access to Private Sector Data' (special issue), 2(4) International Data Privacy Law (2012).

[13] 'Data, data everywhere' (n 1), at 3.

example is Google Flu Trends, which predicts and locates outbreaks of the flu making use of information—aggregate search queries—not originally collected with this innovative application in mind.[14]

Big data applications can have particular benefits for the developing world.[15] For example, Global Pulse, an initiative of the UN Secretary-General, conducts research and enters into partnerships with States and private sector entities to investigate how data analytics can be used to help to protect vulnerable populations, particularly in developing countries.[16] The work of Global Pulse involves data research and the development of tools all over the world, and is thus dependent on the ability to transfer data freely between different countries. A few examples of how data analytics can be used for development purposes are 'the Healthmap project … [which] compiles disparate data from online news, eyewitness reports and expert-curated discussions, as well as validated official reports, to "achieve a unified and comprehensive view of the current global state of infectious diseases"'; and 'use of crowdsourcing following the earthquake that devastated Haiti, where a centralised text messaging system was set up to allow cell-phone users to report on people trapped under damaged buildings.'[17]

Little empirical research has been done on the exact volume of transborder data flows, but growth in Internet traffic gives an indication of the speed with which they are increasing, since much data processing is carried out on the Internet and is thus routed without regard to national borders. For example, the Cisco Visual Networking Index, a widely watched measurement of Internet usage and growth, gave the following predictions in 2011:

> Annual global IP traffic will reach the zettabyte threshold (966 exabytes or nearly 1 zettabyte) by the end of 2015. In 2015, global IP traffic will reach 966 exabytes per year or 80.5 exabytes per month. Global IP traffic has increased eightfold over the past 5 years, and will increase fourfold over the next 5 years. Overall, IP traffic will grow at a compound annual growth rate (CAGR) of 32 percent from 2010 to 2015. In 2015, the gigabyte equivalent of all movies ever made will cross global IP networks every 5 minutes. Global IP networks will deliver 7.3 petabytes every 5 minutes in 2015.[18]

[14] Omer Tene and Jules Polenetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (20 September 2012), at 9, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364>. See also McKinsey Global Institute, 'Big data: the next frontier for innovation, competition, and productivity' (May 2011), <http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation>, stating: 'analyzing large data sets—so-called big data—will become a key basis of competition, underpinning new waves of productivity growth, innovation, and consumer surplus'.

[15] See Global Pulse, 'Big Data for Development: Challenges and Opportunities' (May 2012), <http://www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf>, at 4, stating: 'the diffusion of data science to the realm of international development nevertheless constitutes a genuine opportunity to bring powerful new tools to the fight against poverty, hunger and disease.' See also Gillian Tett, 'Big data is watching you', *Financial Times*, 10 August 2012, <http://www.ft.com/cms/s/2/97cffaf0-e1b5-11e1-92f5-00144feab49a.html>.

[16] See <http://www.unglobalpulse.org/about-new>.

[17] Global Pulse (n 15), at 22–3.

[18] See <http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html>.

To give an idea of the amount of data involved in these statistics, one extabyte of data would hold approximately 36,000 years' worth of HD video, while one zettabyte (which is 1,000 extabytes) is the equivalent of approximately 250 billion DVDs.[19] The growth in Internet traffic is expected to be greatest in less developed regions such as Latin America, the Middle East, and Africa.[20]

Since the Internet is structured to transit data based not on geography but on technical parameters, it can be assumed that a large amount of the personal data transmitted on it must cross national borders, so that the actual route they take is unpredictable. Indeed, technological complexity and the effort required to track data sent over the Internet means that it may no longer be feasible to differentiate between transborder data flows and those that do not cross national borders. Thus, the regulatory framework for transborder data flows is in effect the same as that for data transfers on the Internet, and for the Internet itself.

The scope of data processing and its complexity have changed radically since the first regulation of transborder data flows was enacted in the 1970s. The following excerpt from an article published in 1980 described what was apparently a common scenario at the time:

> The health records of a Swiss national are collected by his employer in Switzerland. Using leased private (dedicated) lines procured from a series of European PTT's [Postal, Telegraph and Telephone service agencies], the employer transmits the data to corporate headquarters in Amsterdam where they are processed, stored, and aggregated with health records of other nationals working in other countries … The employer, having received the fully processed health data, now sends it along via EURONET to the employer's insurance carrier, an Italian firm whose primary data processing facilities are located in Spain. The insurance carrier again processes the data, stores them in Madrid on magnetic tape and issues the appropriate group health policy to the employer.[21]

The cost of transferring data over computer networks in the 1970s was so high that mainly large corporations or governments could take advantage of it.[22] The cost of Internet access today is well within the means of the ordinary citizen, and the Internet is full of free applications and services, so that cost is no longer a factor inhibiting the transborder flow of data.

In the 1970s and 1980s, transborder data flows largely took place using closed networks. This involved the use of technologies such as telephony, telefax, teletext, and Datex; international private telecommunications networks such as TYMNET and IBM1; value-added services offered on a national level such as Bildschirmtext

[19] Charles Arthur, 'What's a zettabyte? By 2015 the Internet will know, says Cisco', *The Guardian*, 29 June 2011, <http://www.guardian.co.uk/technology/blog/2011/jun/29/zettabyte-data-internet-cisco>.

[20] Global Pulse (n 15), at 10, stating: 'While Internet traffic is expected to grow 25–30% between 2011 and 2015 in North America, Western Europe and Japan, the figure is expected to reach or surpass 50% in Latin America, the Middle East and Africa …'

[21] William L. Fishman, 'Introduction to Transborder Data Flows', 16 Stanford Journal of International Law 3, 21 (1980).

[22] Jan Freese, *International Data Flow* (Studentlitteratur 1979), at 25.

in Germany and Videotex in the UK; or corporate networks, such as SWIFT, DFN.[23] Use of these networks or services was generally limited to subscribers or closed user groups; they did not typically interact with other networks; and it was not difficult to determine the location where their use took place. By contrast, the following anonymized case studies published in 2009 indicate the current complexity of transborder data flows in the corporate world:

> A marketer in Spain would use the criteria developed by the analytics vendor in India to select a list of customers from the global Customer Relationship Management (CRM) system in the U.S. which would be transferred to their call center in Mexico for execution of a telemarketing campaign to consumers in Spain. Results from the telemarketing effort from Mexico would then be fed back to the U.S. to update the information in the global CRM system.[24]

> The GRP system [a global recruitment process system that a provider of technology solutions uses to recruit employees] permits interested individuals to apply for an employment position, independent of the country in which they are located or the country from which the opportunity originates … The GRP system allows Zeta and its wholly-owned subsidiaries to assist in identification and selection of candidates, both internal and external, for employment opportunities … [T]he GRP system leads to data transfers on demand. These data transfers cannot necessarily all be predicted in advance of a job posting. A job can be posted from South Africa to the GRP system server in Zurich, and then accessed by Zeta employees in over 100 countries. Some of these employees will send their personal data to the system. In addition, outside recruiters for these or other countries might send in data.[25]

There is a striking contrast between these scenarios, those from 1980 involving the use of proprietary communications networks and magnetic tape, and those from 2009 involving direct access to the data and an upload of the data directly using the same network. The complexity of the data flows has also changed drastically, so that it has become difficult to identify exactly which entity is initiating or controlling the data flows at a particular point in time; to localize the data flows as taking place in a specific location; and to classify the roles of the various actors involved in them.

3. Resulting legal issues

The changing landscape for transborder data flows and the dramatic growth in their volume and scope have led to a corresponding increase in the complexity of legal issues, which can be illustrated by the following examples.

- *Characterizing the activities leading to transborder data flows and the roles and obligations of the parties involved in them* Company A operates a web service

[23] For an overview of data transfer technologies being used at this time, see Michael Bothe and Wolfgang Kilian, *Rechtsfragen grenzüberschreitender Datenflüsse* (Verlag Dr Otto Schmidt 1992), Ch 2.
[24] Schwartz (n 2), at 13. [25] Schwartz (n 2), at 63.

from servers located in its own country. Company A has offices in other countries, but they are only sales offices—that is, all decisions regarding the purposes and means of data processing are taken at its headquarters in its own country, and it only has servers in that country. Customers of the company in other countries go to its website and enter information, which is then processed by Company A on its servers.

Questions Is the access of the website by the individual that results in Company A processing the data in its country to be considered a 'transborder data flow'? If so, which party is exporting the data to Company A, the individual who interacts with the website, or Company A itself? If it is Company A, does it have to register or have the transfer approved by any regulatory authority, and if so, which Company A entity in which country should do so? If the exporter is Company A, how can the company ensure a legal basis for the data transfer? If the exporter is the individual, should the individual have to provide a legal basis for the transfer of his or her own data, and if so, what options are available?

- *Clarifying the policies that underlie transborder data flow regulation* A company with its headquarters in Country A is concerned about the cost of complying with the country's data protection laws. It is considering moving its company database to a newly established office in Country B, where most of its customers reside, and which would result in quicker access of its firm website by customers; Country B does not have a data protection law. Both countries have democratic systems of government, but law enforcement authorities in Country B have greater powers to compel companies to give them access to their databases.

  Questions If the company moves its data processing operations to Country B, should this be considered circumvention of the law of Country A? In answering this question, what weight should be given to the risk of law enforcement access to data in Country B?

- *Outsourcing of data processing to service providers and the interrelationship between transborder data flow regulation and applicable law issues* A data processing service provider in Country A is instructed by a company in Country B to process personal data in Country A and subsequently to transfer them back to the company in Country B. The data were sent to the service provider by the company, and originate from Country B. The data protection laws of both Country A and Country B mandate that certain protections are given to data transferred outside the country, among which is that the country's law should continue to apply to the processing.

  Questions Which country's law should apply to the processing of the data? Should the data transfer requirements of both countries apply to the transfer? Which requirements should apply if there is a conflict between them?

- *The role of technological solutions* Company A transfers personal data to Company B in a different country without data protection or privacy laws. The laws of the country where Company A is established allow transborder

data flows only if the data receive an adequate level of protection in the country of data import. The data are transferred to Company B in encrypted form, so that only it can have access to them.

Questions Should the fact that the data were transferred in encrypted form satisfy the transborder data flow requirements to which Company A is subject? If so, should the encryption have to meet particular technical standards?

- *Conflicts between transborder data flow regulation and other legal requirements* 'Company X does business in many countries, including Country A, a country that lacks sufficient legal protections for personal data. It transfers personal data regarding transactions from countries all over the world to its central database located at its headquarters in Country B. Company X has taken the necessary steps so that its data processing activities are valid under the legal requirements of the countries where it does business. These legal requirements include that Company X will only process data for purposes defined at the time of collection; that it will provide a legal basis for onward transfers of the data to third parties; and that it will only transfer the data to third parties if steps are taken to provide adequate protection in the country to which the data are transferred. In addition, the consumer privacy policy of Company X states that it will use personal data only for limited specified purposes and provide adequate protection for onward transfers of personal data. Law enforcement authorities in Country A approach Company X stating that they have suspicions that certain individuals with which Company X has transacted business may be involved in illegal activities. The individuals are citizens of multiple countries, including those of Country A. These authorities then request Company X to turn over to them all records Company X holds involving transactions with such individuals over the last three years, including those stored at its database in Country B. The request is not based on a judicial order, and does not list any further details beyond the names of the individuals and the time frame in which the relevant transactions took place. The authorities state that if this request is not complied with, they will initiate criminal proceedings against the management board of Company X's subsidiary in Country A.'[26]

  Questions Which legal obligations should Company X comply with, those of Country A or Country B? Should the data protection law of Country B recognize the law enforcement requirements of Country A as a legal basis to transfer the data?

These are just a few of the legal issues that arise under transborder data flow regulation, and that will be dealt with in this study.

[26] Quoted from International Chamber of Commerce (ICC), 'Cross-border law enforcement access to company data—current issues under data protection and privacy law', Doc. No. 373/507 (7 February 2012), <http://www.iccwbo.org/Data/Policies/2012/Cross-border-law-enforcement-access-to-company-data-current-issues-under-data-protection-and-privacy-law/>.

B. Growth of transborder data flow regulation

The growth in transborder data flows has been accompanied by a growth in rules of data protection and privacy law that regulate the transfer of personal data outside the geographical boundaries of the country of data collection and processing. Such regulation began on an international scale in the 1980s with the enactment of instruments such as the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (hereinafter: the 'OECD Guidelines');[27] the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) (hereinafter: 'Council of Europe Convention 108');[28] the EU Data Protection Directive 95/46 (hereinafter: the 'EU Data Protection Directive' or 'the Directive');[29] and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework (hereinafter: 'APEC Privacy Framework').[30] Many of these frameworks are under review; for example, on 25 January 2012 the European Commission issued a proposal for revision of the EU legal framework for data protection (including the EU Directive),[31] and similar exercises are underway in international organizations such as the Council of Europe and the OECD.

Over 70 countries have now adopted data protection or privacy laws that explicitly regulate transborder data flows. Beginning in Europe, such laws have spread to all regions of the world, including North and Latin America; the Caribbean; all Member States of the European Union and the European Economic Area, and several other European countries as well; Africa; the Near and Middle East; Eurasia; and the Asia-Pacific region. Some countries are also in the process of adopting data protection and privacy legislation that includes regulation of transborder data flows, or of amending their existing regulation. In addition, many countries are bound by international legal instruments such as the Additional Protocol to Council of Europe Convention 108, and others are eligible to participate in voluntary systems such as the APEC Privacy Framework (which by itself covers 21 countries). Transborder data flow regulation exists not only at the national level, but also at the local or regional level in a number of federal countries, and is dealt with in data sharing agreements between States. Companies and other data controllers increasingly view such regulation as a matter of high-level strategic importance, which has led to a growth of private sector regulation as well. The Appendix at the end of this

[27] (23 October 1980), <http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

[28] 28 January 1981, ETS 108 (1981).

[29] Directive 95/46/EC 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.

[30] APEC Privacy Framework (2005), <http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx>.

[31] See <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>.

study contains English versions of provisions in data protection and privacy law instruments from around the world that regulate transborder data flows.

C. What are transborder data flows?

The application of transborder data flow regulation, and the obligations it brings, is predicated on the existence of a data transfer. There is a lack of clarity as to the meaning of the term, and regulatory instruments often use different ones without making it clear what they mean. The EU Directive refers to 'transfer to a third country of personal data' (Article 25(1)), without defining 'data transfer'; the Commission's 2012 proposal to amend the EU data protection framework[32] also fails to do so. The APEC Privacy Framework variously uses the terms 'international transfer', 'information flows across borders', 'cross-border information flow', and 'cross-border data transfer' interchangeably to refer to the movement of personal data across national borders.[33] The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) does not distinguish between domestic and international flows of data, and a 'data transfer' is considered to mean 'use' of the data by an organization.[34] The OECD Privacy Guidelines refer to 'transborder data flows', defining the term as 'movements of personal data across national borders' (§ 1(c)), while Council of Europe Convention 108 refers to 'transborder flows of personal data', defined as 'the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed' (Article 12(1)). Since the OECD Guidelines and Council of Europe Convention 108 both refer to 'transborder data flows', that is the term that is used here, but it should be understood to refer generically to all cases of data crossing national borders.

The difficulty of defining what constitutes a 'data transfer' is increased by the fact that data can cross borders not just by being actively transferred, but also by being made available to recipients in other countries.[35] The law tends to conceive of transborder data flows as if they were the result of a discrete act, such as someone pushing a button and causing data to be transferred. In fact, nowadays data transfers often take place as part of a process. This point is brought out in the following description of data flows in a system for clinical drug trials operated by a multinational pharmaceutical company:

> The data flow in a clinical trial system is ongoing, and multi-directional. As the Alpha report states, data transfers 'are rarely uni-directional.' The report adds, 'The data flow

[32] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

[33] APEC Privacy Framework (n 30).

[34] See Office of the Privacy Commissioner of Canada, 'Guidelines for Processing Personal Data Across Borders' (2009), <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf>, at 5.

[35] European Data Protection Supervisor (n 9), at 17.

cannot be considered a discrete event, but is rather a continuous process.' A number of interconnected systems will interact together to produce different data sets that are tailored to the specific user.[36]

In many cases, it is also not clear whether merely making personal data accessible (eg, on the Internet) should be considered to result in such a transfer, or whether this requires some active or automatic transmission of the data. This was the issue in the *Bodil Lindqvist* case[37] decided by the European Court of Justice,[38] where the defendant was charged with breach of Swedish data protection law for publishing on her Internet site personal data of a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church. The Court found that there is no data transfer to a third country within the meaning of Article 25 of the EU Data Protection Directive when an individual in a Member State loads personal data onto an Internet page which is stored on a site on which the page can be consulted and which is hosted by a natural or legal person established in that State or in another Member State, thereby making those data accessible to anyone who connects to the Internet, including people in a third country. The Court's decision was based on the fact that the information was not being sent automatically from the server to other Internet users; that there was thus no direct transfer of personal data between the person loading the information on the server and the person accessing the data from the server; that the data transfer restrictions contained in Article 25 were probably not intended to apply in such a situation; and that if a data transfer were found to exist in this case, then the restrictions of Article 25 would apply any time that information was loaded onto and made accessible via the Internet, which would make EU law applicable to the entire Internet.

The *Lindqvist* decision seems to be based partly on pragmatic considerations, such as the fact that there was no evidence that the personal data were ever actually accessed outside the EU.[39] The Court also seemed to put particular weight on the likely consequences of a contrary decision, namely that finding that a data transfer occurred in this case would effectively make the entire Internet subject to EU data protection law,[40] a consideration that has also been faced by national legislators when deciding whether to define access to data on the Internet as a 'data transfer'.[41] In addition, the Court found that the provisions on international data transfers

[36] Schwartz (n 2), at 41.

[37] C-101/01 [2003] ECR I-12971.

[38] The Court of Justice, the highest court of the Court of Justice of the European Union (CJEU), will be referred to throughout as the European Court of Justice (ECJ), which was its name prior to 2009.

[39] See Ulf Brühann, 'Die Veröffentlichung personenbezogener Daten im Internet als Datenschutzproblem', (2004) Datenschutz und Datensicherheit 201, 203.

[40] C-101/01 [2003] ECR I-12971, at para. 69.

[41] See, eg, Dag Wiese Schartum, 'Norway', in Peter Blume (ed), *Nordic Data Protection Law* (DJØF 2001), at 102–4, describing the concern of the Norwegian government in revising its data protection law that it should not automatically cover the entire Internet.

contained in the Directive were a 'special regime', which were never intended, in the Court's view, to have general application to the entire global Internet.[42]

Some of the Court's reasoning can be faulted. For instance, whether or not the data were actually accessed seems irrelevant, and has been largely rejected by the EU data protection authorities in their interpretation of the case;[43] rather, the key question should be whether the data *could* have been accessed. Failing to consider as data transfers situations when data were not being automatically transmitted to other countries seems untenable, given that the intention to make data available to other countries may exist just as much when they are merely made accessible as when they are actively transmitted, and that technological advancements will probably blur the distinction to a point where it can no longer be maintained.[44] But the Court's decision is praiseworthy, even visionary, in its willingness to consider the international implications of its ruling, and in its decision not to apply the EU restrictions on international data transfers past a point of reasonableness.[45]

Following the *Lindqvist* case, there continues to be a lack of clarity regarding the definition of 'data transfer', particularly with regard to situations in which individuals input their personal data onto an Internet site. The question of whether a data transfer takes place is often used as a proxy for determining whether the data protection law of a particular country or region is applicable to the processing,[46] with the boundaries of the question being that, on the one hand, data controllers should not be able to evade their responsibility by claiming that no data transfer has taken place,[47] while on the other hand, not every interaction of an individual with a website should be considered to be a data transfer,[48] within these broad parameters, the definition of data transfer depends largely on the facts of the particular case.

[42] C-101/01 [2003] ECR I-12971, at para. 69, stating: 'If Article 25 of Directive 95/46 were interpreted to mean that there is "transfer [of data] to a third country" every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet.'

[43] See, eg, UK Information Commissioner, 'The Eighth Data Protection Principle and international data transfers' (30 May 2006), at para 1.3.4, stating: 'In practice, data are often loaded onto the internet with the intention that the data be accessed in a third country, and, as this will usually lead to a transfer, the principle in the Lindqvist case will not apply in such circumstances'.

[44] Dan Jerker B. Svantesson, 'Privacy, the Internet and Transborder Data Flows: An Australian Perspective', 4 Masaryk University Journal of Law and Technology 1, 15 (2010), stating: 'While it is true that Lindqvist could not transfer the content of her website to an Internet user that was not connected to the Internet at the time, or who did not wish to take the steps necessary to visit her website, that is no different to the fact that a TV station cannot provide TV programs to somebody who does not turn on their TV, or who does not chose the TV station's particular channel. Consequently, the Court's justification of their approach, by reference to the relevant technology, is weak indeed.'

[45] Svantesson (n 44), at 16.

[46] See Chapter 6.

[47] See Article 29 Working Party, 'Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based websites' (WP 56, 30 May 2002), at 9, stating that the objective of applicable law rules concerning non-EU websites is 'to ensure that individuals enjoy the protection of national data protection laws …'

[48] Article 29 Working Party (n 47), stating: 'the Working Party is of the opinion that not any interaction between an Internet user in the EU and a web site based outside the EU leads necessarily to the application of EU data protection law'.

Since the existence of a data transfer results in obligations on the part of the data controller to provide a legal basis for the transfer, determining that one has taken place is often a type of protective measure to ensure that local data protection law will continue to apply after the data are transferred.[49] In practice, the likelihood that a data transfer will be found to have occurred is higher in circumstances when the data controller has an establishment in the country of the individual whose data are processed, when the controller is in some way targeting the individual, or when the controller has some degree of control over the means used by the individual to process the data. On the other hand, a transfer is less likely to be found when the individual has initiated contact with the controller without being targeted, when the controller does not have any operations in the individual's country, or when the controller does not exercise control over the purpose or means which the individual uses to process the data.

The definition of data transfer will be further considered later on.[50] Terms such as 'transborder data flows' and 'mere transit' will be broadly construed; technology, business models, and trends regarding online activities of users are changing so fast that a narrow definition would omit many interesting phenomena from analysis.

D. The changing role of the individual

Individuals have a much greater ability to initiate transborder data flows than ever before. For example, a person can now book a hotel room in a foreign country via an Internet website, whereas in past decades this would have required more effort and cost (eg, by telephoning the hotel or sending a letter), or could only have been done via an intermediary (eg, a travel agency or hotel booking service). Internet services such as online social networks have also given individuals a greater power to communicate across borders. But along with this increased power goes a growing concern about the role that individuals play in the online environment. For example, it is easy for individuals to communicate across borders without understanding who is processing their data and the terms under which they are processed, and to transfer the data of third parties without them ever knowing about this.

EU data protection law contains an exemption covering the processing of data 'by a natural person in the course of a purely personal or household activity'.[51]

[49] See, eg, European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World—A European Data Protection Framework for the 21st Century', COM(2012) 9/3, 25 January 2012, at 10, stating: 'Individuals' rights *must continue to be ensured when personal data is transferred* from the EU to third countries, and whenever individuals in Member States are targeted and their data is used or analysed by third country service providers' (emphasis added). See also Chapter 6.B.

[50] See Chapter 8.C.

[51] Article 3(2). See also Article 29 Working Party, 'Opinion 5/2009 on online social networking' (WP 163, 12 June 2009), at 5.

Thus, the protection of an individual's private sphere implies that they should not have to comply with data protection requirements when performing intimate personal activities such as keeping a diary or writing a private letter. This exemption applies not only to transborder data flow regulation, but also to other obligations of a data controller. However, it has special relevance to the transborder flow of data, since many of the online services in the context of which it applies involve the processing of personal data in other countries.

Application of this exemption to data processing in an online environment is becoming increasingly problematic. For example, many online services allow individuals to input their own personal data directly (which routinely involves transferring the data across borders), and data protection authorities have found that the exemption may apply to situations when individuals enter information about their 'personal, family or household affairs' into an online social networking site.[52] However, it is often difficult to determine if such processing should be considered the individual's own personal activity, a commercial activity by the website, or both.[53] In addition, an individual can violate the data protection rights of a third party more easily in the context of the Internet, such as by posting a private photo on a social networking site (and thus making it available for download around the world) without the third party expecting it. There is thus a fine line to be drawn between not overburdening intimate personal and private activities, on the one hand, and not exempting individuals who transfer personal data from all responsibility, on the other hand.

E. Differentiating data transfers from 'mere transit'

Transborder data flow regulation typically does not apply in situations where data are merely 'transiting' across territory. For example, Article 4(1)(c) of the EU Data Protection Directive provides that EU data protection law shall apply also when a data controller 'is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, *unless such equipment is used only for purposes of transit through the territory of the Community*' (emphasis added). The regulation of transborder data flows under the UK Data Protection Act also applies only to 'data transfers', but not to 'mere transit', defined as situations where data are routed through one country on their way to another one.[54]

This means that, for example, a telecommunications provider without a fixed place of business in the EU, but that maintains a telecommunications network over which data flow in and out of the EU, is not subject to EU data protection law (and thus also to transborder data flow regulation under the Directive) to the

[52] Article 29 Working Party (n 51), at 3.
[53] See the discussion in European Data Protection Supervisor (n 9), at 9–10.
[54] UK Information Commissioner (n 43), at para 1.3.2.

extent that such equipment is only used for 'transit' of data. Another example of mere transit is data routing on the Internet, which consists of a router finding the best path for a data packet to travel and then forwarding it on.[55] The policy behind this exemption is that in cases of mere transit of data the rights and freedoms of EU citizens are not affected.[56]

The Directive does not explain what constitutes 'transit', but the Article 29 Working Party has defined it as 'for example in the case of telecommunication networks (cables) or postal services which only ensure that communications transit through the Union in order to reach third countries'.[57] The Working Party goes on to note that this exception should be subject to a narrow interpretation.[58] However, the extent of the distinction between 'mere transit' and data transfers covered by data protection law remains uncertain.

F. Scope of the study

Only *legal* issues relevant to the regulation of transborder data flows will be covered, and only those that arise under data protection and privacy law (unless otherwise noted). Such regulation exists in other areas of the law as well (eg, under export control restrictions, media law, tax law) that will not be examined, since they either involve the processing of non-personal data or are only peripherally related to data protection and privacy.[59]

Many data protection laws regulate the transfer of personal data to third parties apart from specific regulation of *transborder* data flows. For example, Japanese law restricts data transfers to third parties in general,[60] without containing a specific provision on international data transfers. While such general restrictions on data transfers may restrict international transfers as well, including them would exceed

[55] For a description of data routing on the Internet, see 'Routing 101: the Basics', <http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094822.shtml#ns339/ns392/ns399/ns400/networking_solutions_white_paper0900aecd802d5489.shtml>.

[56] See Spiros Simitis and Ulrich Dammann, *EU-Datenschutzrichtlinie* (Nomos-Verlag 1997), at 130.

[57] Article 29 Working Party, 'Opinion 8/2010 on applicable law' (WP 179, 16 December 2010), at 23.

[58] Article 29 Working Party (n 57), stating: 'As this is an exception to the equipment criterion, it should be subject to a narrow interpretation. It should be noted that the effective application of this exception is becoming infrequent: in practice, more and more telecommunication services merge pure transit and added value services, including for instance spam filtering or other manipulation of data at the occasion of their transmission. The simple "point to point" cable transmission is disappearing gradually. This should also be kept in mind when reflecting on the revision of the data protection framework.'

[59] For a discussion of transborder data flow regulation in areas such as media law, taxation, and telecommunications law, see Anne W. Branscomb, 'Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition', 36 Vanderbilt Law Review 985 (1983); John M. Eger, 'Emerging Restrictions on Transnational Data Flows: Privacy Protection or Non-Tariff Trade Barriers?', 10 Law and Policy in International Business 1055 (1978).

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

the scope of this study. Thus, it is limited to examining rules that specifically regulate the flow of data across national borders, with a few exceptions.

The concept of 'regulation' will be broadly construed to include all types of conditions, limitations, and restrictions on the transfer of data across national borders. For example, some data protection laws require data exporters to register transborder data flows with a regulatory authority before they are carried out,[61] which may involve considerable effort, and can impede or slow down data transfers. It also encompasses measures that private actors take, whether or not they have binding legal force, which limit or constrain the transfer of personal data across national borders. Many actions of private parties affect, influence, or restrict the transfer of personal data across national borders, even if they may lack the overriding legal quality of governmental regulation. Private sector instruments such as contractual clauses, internal company policies, and codes of practice are becoming more widely used to structure and protect international data transfers, and may have binding legal value, such as through contract law or regulatory approval. Schemes whereby instruments used by the private sector are either drafted in advance by public authorities (eg, the EU-approved standard contractual clauses[62]) or approved by them (eg, 'binding corporate rules' or BCRs in the EU) are becoming increasingly common, resulting in a patchwork of private and public regulation.[63] Indeed, the inherently international nature of transborder data flows means that they are not easily susceptible to a single regulatory solution, and a mixture of public and private sector regulation may be the most effective way to deal with them. This broad definition of 'regulation' is in line with modern regulatory scholarship.[64]

This study is concerned mainly with international flows of *personal* data, defined as data relating to an identified or identifiable natural person (ie, an individual).[65]

[61] See, eg, Argentina Personal Data Protection Act 2000, Article 21(2)(e); Austrian Data Protection Act 2000, § 17 in conjunction with § 19 no. 5; Croatian Act on Personal Data Protection (12 June 2003), no. 1364-2003 (as amended by Act on Amendments to the Personal Data Protection Act, No. 2616-2006), Article 14(1); Dutch Data Protection Act, § 28 lit. e; French Data Protection Act, § 23 in conjunction with § 30; Polish Data Protection Act, § 41(7).

[62] See Commission Decision 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 95/46/EC of the European Parliament and of the Council, [2010] OJ L39/5; Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC 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.

[63] See Christopher Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (CUP 2011), at 44, stating: 'The role of corporations, consumers and states in inter-meshed webs of regulatory activity is now accepted by legal theorists …'; Bert-Jaap Koops, 'Criteria for normative technology: the acceptability of "code as law" in light of democratic and constitutional values', in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* 161 (Hart 2008), at 161, stating: 'Traditionally, the acceptability of "private" regulation can be and has been interpreted separately from acceptability of "public" regulation, but a sharp distinction between public and private regulation can no longer be made as we are moving towards a world of polycentric governance'.

[64] See Colin J. Bennett and Charles D. Raab, *The Governance of Privacy* (MIT Press 2006), at 117–19.

[65] See EU Data Protection Directive (n 29), Article 2(a).

Thus, for the most part it does not examine flows of non-personal data, or data that can only identify a legal person (eg, a company). Distinguishing what are and are not personal data can be a difficult exercise, and the term can have different meanings in different legal systems.[66] Moreover, advances in modern computer technologies now allow an ever-increasing variety of data that may previously have been considered non-personal or anonymous to be tied to an individual, given enough time and computing power.[67] However, the limitation to personal data is necessary since most regulation focuses on it, and to make it clear that data that are clearly non-personal will not be covered (eg, data about logistics shipments, weather patterns, statistical information).

Regulatory obligations under data protection and privacy law differ based on whether the party processing personal data is deemed to be a 'data controller' (ie, a party determining the purposes and means of data processing) or a 'data processor' (ie, a party processing data on the instruction of a data controller),[68] and there is considerable disagreement about what these terms mean in practice. Data processing by both types of parties will be covered here.

Certain types of data flows carried out by the public sector (eg, those conducted for law enforcement purposes) may give rise to special issues. Warnings were already being made in the 1970s about drawing a sharp boundary between data privacy rules in the public and private sectors,[69] which are even more relevant today, since 'the distinction between activities of the private sector and of the law enforcement sector is blurring'.[70] Law enforcement entities often seek access to personal data processed by the private sector; for example, the EU Data

[66] *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 FRD 443, 69 FedRServ3d 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.

[67] See, eg, Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', 57 UCLA Law Review 1701, (2010), stating: 'Computer scientists have recently undermined our faith in the privacy-protecting power of anonymization, the name for techniques that protect the privacy of individuals in large databases by deleting information like names and social security numbers. These scientists have demonstrated that they can often "reidentify" or "deanonymize" individuals hidden in anonymized data with astonishing ease.'

[68] Essentially, the data controller is subject to most compliance responsibilities, while a data processor is responsible for complying with the instructions given to it by the controller. See, eg, Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' (WP 169, 16 February 2010).

[69] See Frits W. Hondius, 'International Data Protection Action', in *Policy Issues in Data Protection and Privacy, Proceedings of the OECD Seminar 24th to 26th June 1974*, 208, at 216, stating: 'We should also warn against drawing too sharp a boundary between rules on data privacy in the private or the public sector. Not only do certain activities take place in one country in the private and in another country in the public sphere but there is also intensive interchange between the two sectors (for example public bodies entrusting certain operations to private firms)'.

[70] Opinion of the European Data Protection Supervisor on Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, 'A comprehensive approach on personal data protection in the European Union' (14 January 2011), at 9.

Retention Directive[71] mandates that Internet and telecommunications service providers retain certain types of data generated by their users, and make such data available to law enforcement authorities upon request. The volume and scope of such requests have increased, in some cases even requiring private sector entities to monitor communications of third persons on an ongoing basis.[72] Given the growing interaction between data processing in the private and public sectors, which routinely involves the transfer of personal data across national borders, it makes little sense to consider the two sectors separately with regard to the regulation of transborder data flows.

Much of the discussion will involve European Union law, since the EU has the most long-standing, influential, and complex transborder data flow regulation. However, this study is global in scope, and the analysis it provides is intended to apply to all regions of the world. It purposely does not delve into the minutiae of national regulatory requirements, and focuses on the main jurisprudential themes.

G. Towards a normative framework

1. Conceptual questions

Several factors make it difficult to develop a normative framework against which to measure the quality and success of data protection law (of which regulation of transborder data flows is a component).

First, there is disagreement between legal systems about how concepts such as 'data protection' and 'privacy' are to be understood. 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. 'Privacy' can be seen as a concept that is both broader than and independent from data protection, though there is significant overlap between the two. Generally speaking, data protection (sometimes also referred to as 'informational privacy') deals with the legality of processing data regarding an identified or identifiable individual, while privacy deals with protection of an individual's 'personal space';[73] however, the two are closely related and can seldom be

[71] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, [2006] OJ L105/54.

[72] See ICC (n 26).

[73] See, eg, Case T-194/04 *Bavarian Lager v Commission* [2007] ECR-II 04523, para. 118 (partially reversed by the ECJ, Case C-28/08 P *Bavarian Lager* [2010] ECR I-06055), where the European Court of First Instance stated: 'it should also be emphasized that the fact that the concept of "private life" is a broad one, in accordance with the case-law of the European Court of Human Rights, and that the right to the protection of personal data may constitute one of the aspects of the right to respect for private life … does not mean that all personal data necessarily fall within the concept of "private life"'.

neatly distinguished.[74] In European law, 'privacy' includes issues relating to the protection of an individual's 'personal space' that go beyond data protection, such as 'private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially.'[75] Privacy is also a concept that must be determined based on the social customs of the particular society in question.[76] Transborder data flow regulation relates to the processing of personal data and is thus, strictly speaking, a question of data protection rather than privacy law, though the issues involved are closely linked in many ways, and thus reference to privacy will sometimes be made.

Secondly, the legal nature of data protection law is an important factor in determining the normative framework for transborder data flow regulation. Thus, whether a particular area of the law is considered to be private law, public law, administrative law, human rights law, commercial law, or some other type of law will influence what criteria are used for determining how it should be evaluated. However, such classification is particularly difficult with regard to data protection law, since it is a mixture of various types of law:

> Data protection legislation will typically contain provisions of a public law nature, relating to an authority and its duties and decisions. But the law will also often include civil law provisions, typically on liability for data protection violations. The provisions of data protection legislation may therefore have to be qualified as belonging to different areas of law, to which different relevant connection criteria are assigned.[77]

The hybrid nature of data protection law can be seen by the example of the EU Data Protection Directive, which sets forth two goals, namely furtherance of the free flow of personal data within the EU internal market, and achievement of a high level of data protection throughout the EU.[78] Thus, the Directive has both economic motivations (promoting the free flow of data) and human rights motivations (protecting fundamental rights to data protection). The normative framework

[74] See, eg, James Griffin, *On Human Rights* (OUP 2008), at 229, who describes the relationship between data protection and privacy as follows: 'The right to informational privacy protects us against people's access to certain knowledge about us. The right to the privacy of space and life protects us against intrusions into that space and into that part of our life—say, into our married or family life. These two rights overlap in their protections, but, on the face of it, are different'. See also Roger Brownsword and Morag Goodwin, *Law and Technologies of the Twenty-First Century* (CUP 2012), at 308.

[75] Parliamentary Assembly of the Council of Europe, Resolution 428, para. C2 (1970).

[76] See Alan Westin, *Privacy and Freedom* (Atheneum 1970), at 12.

[77] Jon Bing, 'Data Protection, Jurisdiction and the Choice of Law', [1999] Privacy Law & Policy Reporter 92, 93, also available at <http://www.austlii.edu.au/au/journals/PLPR/1999/65.html>.

[78] See Article 1 of the Directive, stating that its object is both to 'protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data', and to ensure that 'Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'

is determined in large part by the aim of regulation and the policies it pursues, so that it is more difficult to determine which framework should apply when regulation is motivated by diverse goals. Regulation to further economic interests is generally based on a rationale that it is necessary to overcome 'market failures',[79] but regulation may also be enacted for reasons other than economic efficiency, such as to further a desirable social policy,[80] and economic efficiency cannot serve as the sole criterion for regulation that is designed to advance fundamental rights.[81]

Thirdly, transborder data flow regulation takes a variety of divergent forms, which makes it more difficult to arrive at a scheme for its normative evaluation.[82] Such regulation is based not only on legislation, but may also include private law instruments such as contractual clauses between parties transferring personal data across borders, as well as non-binding instruments like codes of practice. With regard to one example illustrating the differences between legal systems, in the US there is a greater resistance to legal regulation of privacy and a greater reliance on private sector and technological solutions, whereas in the EU government regulation and regulatory agencies play a greater role.[83]

Fourthly, transborder data flow regulation requires consideration of many areas of law, including human rights law, contract law, public and private international law, EU law, and others. It will be necessary to go into each of these areas in sufficient detail, without dealing with them exhaustively.

2. Normative theories

Transborder data flow regulation involves norms arising from fundamental rights law, economic regulation, law enforcement requirements, and private sector practices; legal sources, such as national law, regional agreements, and international treaties; and actors such as individuals, companies, data protection regulators, national governments, and law enforcement authorities. The diversity of actors, norms, and policy goals makes it impossible to construct an overarching framework that could

[79] See Robert Baldwin, Martin Cave, and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd edn, OUP 2012), at 15, stating: 'many of the rationales for regulating can be described as instances of "market failure". Regulation in such cases is argued to be justified because the untolled marketplace will, for some reason, fail to produce behavior or results in accordance with the public interest'.

[80] Baldwin, Cave, and Lodge (n 79), at 23.

[81] Baldwin, Cave, and Lodge (n 79), at 26, stating: 'questions of justice … cannot be answered by economists' appeals to efficiency and distributional questions … have to be made on the basis of grounds other than efficiency.' See also Ronald Dworkin, 'Is Wealth a Value?', (1980) 9 Journal of Legal Studies 191.

[82] See Baldwin, Cave, and Lodge (n 79), at 37, stating: 'if it is the case that a regulatory regime involves numbers of regulators of different kinds—state and non-state, national and trans-national, public interest and private/commercial—there are likely to be complex interactions or legitimation claims, numbers of competing conceptions of regulatory quality, and a variety of processes for furthering legitimation claims.'

[83] See Charles D. Raab and Paul De Hert, 'Tools for Technology Regulation: Seeking Analytical Approaches Beyond Lessig and Hood', in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* 263 (Hart 2008), at 268 fn 8.

reconcile the various legal conflicts and issues. Indeed, suggesting a grand scheme to 'solve' the problems presented by transborder data flow regulation diverts attention from other possibilities which, even if they do not represent a complete solution, can help to deal with some of the major issues. This study will therefore describe systematically the relevant issues and problems through the perspective of legal pluralism, which is defined as a situation based on 'the existence of a multiplicity of distinct and diverse normative systems, and the likelihood of clashes of authority-claims and competition for primacy amongst these … It emphasizes the value of diversity and difference amongst various national and international normative systems and levels of governance, and the undesirability and implausibility of constitutional approaches which seek coherence between these systems.'[84] Individual steps will also be suggested that could reduce the scope of the problems to a more manageable level, drawing on different areas of law.

Any regulation is enacted to further certain goals or policies,[85] and it must be asked what policies transborder data flow regulation is supposed to further; how these policies are articulated; whether such regulation actually does advance them; and whether they are justifiable. Examination of the policies and purposes for which regulation was enacted is used as a method of evaluation in other areas as well, such as EU law[86] and public international law.[87] It is also necessary to examine basic conditions of regulatory 'craftsmanship'—that is, what substantive and procedural characteristics regulation should exhibit.[88]

Theories concerning the regulation of information technology are helpful for evaluating the regulation of transborder data flows, since the two areas share a number of characteristics. In particular, both of them involve issues of economic efficiency and of fundamental rights; are subject to regulation under both traditional legislation and private sector instruments; and are inherently international in nature. Moreover, perhaps the majority of transborder data flows occurs online, making theories of technology regulation particularly relevant. Koops has summarized the views of a number of authors who have sought to develop theories of how technologies can be regulated, and has divided them into primary (eg, human rights and other moral values, the rule of law, and democracy) and secondary criteria (eg,

[84] Gráinne de Búrca, 'The European Court of Justice and the International Legal Order after *Kadi*', 51 Harvard International Law Journal 1, 12, 32 (2010).

[85] See Chris Reed, 'How to Make Bad Law: Lessons from Cyberspace', 73 Modern Law Review 903, 904 (2010), stating: 'a fundamental aim of any law … is to influence behaviour to some useful end.'

[86] See Hannes Rössler, 'Interpretation of EU Law', in Jürgen Basedow, Klaus J. Hopt, Reinhard Zimmermann, and Andreas Stier (eds), *Max Planck Encyclopedia of European Private Law* (OUP 2012), at 979.

[87] See Vienna Convention on the Law of Treaties (adopted on 23 May 1969, entered into force on 27 January 1980) 1155 UNTS 331, Article 31; Nicola Vennemann, 'Application of International Human Rights Conventions to Transboundary State Acts', in Rebecca M. Bratspies and Russell A. Miller (eds), *Transboundary Harm in International Law: Lessons from the Trailsmelter Arbitration* 295 (CUP 2006), at 301–2 (note that Vennemann cites Article 27 of the Vienna Convention but seems to mean Article 31).

[88] See, eg, Baldwin, Cave, and Lodge (n 79), at 27; Lon L. Fuller, *The Morality of Law* (2nd edn, Yale University Press 1969), at 39.

transparency of rule-making, accountability, efficiency).[89] None of these criteria provide a complete answer by themselves to the questions raised by transborder data flow regulation, but they will be drawn on in combination throughout.

3. Conclusions

As will be explained in more detail in Chapter 8, transborder data flow regulation is an example of a pluralistic legal framework, and the norms, parties, and institutions that it involves are so diverse and fragmented that they cannot be analysed under a single regulatory theory. In keeping with theories of legal pluralism, various criteria (fundamental rights, efficiency, transparency, accountability, etc.) suitable to each of its constituent elements will be used to evaluate them as appropriate.

[89] Koops (n 63), at 169.

country. In 1976, Brazil introduced a system whereby the use of international computer networks, foreign data banks, and other computerized systems resulting in transborder data flows required prior permission of a government board.[26] Such approvals were apparently granted sparingly:

> Between May 1978 and January 1980, 19 applications were filed and decisions were taken on 16. Approval was denied for applications related to the use of time-sharing services and data banks abroad and certain types of the international operations of foreign affiliates; approval was given for airline reservation systems and demonstration systems. In general, the Government of Brazil 'does not allow the use of computers placed abroad, which through teleinformatics accomplish tasks whose solutions can be obtained in the country'.[27]

In 1979, Brazil established a Special Informatics Agency (SEI) to regulate the flow of data out of the country. According to one author, 'SEI examines potential transborder data flows and international information services on an individual basis. SEI then determines what the impact of the services will be in terms of economic, privacy, and national sovereignty concerns. Based upon this analysis, the application is either accepted, rejected, or conditionally accepted.'[28] Brazil was apparently the only developing country to institute a thorough system of transborder data flow controls on such a scale;[29] perhaps not coincidentally, a military government ruled the country at the time.

The Brazilian restrictions were resisted by the US, which saw the ability to transfer data freely across borders as a lynchpin of its own national sovereignty.[30] As one US politician put it in 1977: 'One way to "attack" a nation such as the United States which depends heavily on information and communication is to restrain the flow of information—cutting off contact between the headquarters and the overseas branches of a multinational firm; taxing telecommunications crossing borders; building information walls around a nation.'[31] Thus, some nations saw regulation of transborder data flows as a way to protect their sovereignty, whereas others saw it as a threat to their sovereignty.

Governments continue to regulate, or even block completely, the transborder flow of data for reasons relating to national sovereignty. For example, the government of China blocks access to many kinds of Internet content,[32] and in 2011 the Egyptian government attempted to quell internal rebellion by completely shutting down access to the Internet.[33] These actions are assertions of power to protect governmental interests, and have nothing to do with the protection of privacy.

[26] Mengel (n 4), at 201. [27] Mengel (n 4), at 201.

[28] Jane Bortnick, 'International Information Flow: The Developing World Perspective', 14 Cornell International Law Journal 333, 342 (1981).

[29] See Schoonmaker (n 22), at 14, stating: 'the Brazilian military government, however, was the only one to implement a major policy in this area'.

[30] Schoonmaker (n 22), at 50–6. [31] Schoonmaker (n 22), at 51.

[32] See Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2008), at 92–100.

[33] See Ryan Singel, 'Report: Egypt Shut Down Net with Big Switch, Not Phone Calls', Wired (10 February 2011), <http://www.wired.com/threatlevel/2011/02/egypt-off-switch/>.

Recent technological developments such as cloud computing have also spurred governments to assert concerns about information sovereignty. For example, some EU Member States (eg, France and Germany[34]) have begun promoting the construction of cloud computing infrastructures located in their own countries, based on concerns that government data stored with providers in the US may be subject to access by US law enforcement authorities.[35] The ever-increasing globalization of data processing may cause a counter-reaction and motivate States to assert their sovereign interests in data processing and transborder data flow regulation more aggressively,[36] both because of privacy concerns and for economic reasons. Thus, regulation of transborder data flows to protect interests of national sovereignty remains alive and well.

D. Free flow of data and freedom of information

Transborder data flow regulation is dealt with not only in data protection and privacy law, but in a number of specialized international treaties in areas such as telecommunications, satellite transmission, and broadcasting,[37] which will generally not be dealt with in detail here since they do not focus solely on privacy and data protection.

However, such instruments demonstrate that transborder data flows have long been the subject of international lawmaking. For example, before the first International Telegraph Convention was concluded in 1865, States had concerns about the transmission of telegraphic messages across their borders, so that it was necessary to cable a message to the last territorial station of the sending State, carry it across the border in written form, and then transmit it further telegraphically in the adjoining State.[38] During negotiation of the Convention, agreement to allow the transfer of telegrams across national borders was only reached by incorporating into it the possibility for States to restrict their transfer for reasons such as State security, compliance with law, and public order—that is, by allowing States to regulate the transborder flow of telegraphic data.[39]

[34] See 'Innenminister Friedrich will sichere "Bundescloud" aufbauen' (18 December 2011), <http://www.teltarif.de/bundes-cloud-friedrich-regierung-telekom-sichere-speicherung/news/45000.html>.

[35] See Kristina Irion, 'Government cloud computing and the policies of data sovereignty' (September 2011), <https://www.econstor.eu/dspace/bitstream/10419/52197/1/672481146.pdf>.

[36] See Zachary N.J. Peterson, Mark Gondree, and Robert Beverly, 'A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud', <http://rbeverly.net/research/papers/soverign-hotcloud11.pdf>.

[37] A number of these are discussed in Edward W. Ploman, *International Law Governing Communications and Information* (Frances Pinter Ltd 1982), at 143 and 228–32.

[38] Gotlieb, Dalfen, and Katz (n 20), at 228.

[39] Gotlieb, Dalfen, and Katz (n 20). See also Anne W. Branscomb, 'Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition', 36 Vanderbilt Law Review 985, 995–6 (1983).

Of particular relevance are the principles of the 'free flow of information' and 'freedom of information'.[40] Both terms refer to the open and free exchange of information, and derive from basic human rights instruments under public international law. Thus, the Universal Declaration of Human Rights of 1948 (UDHR) and the International Covenant on Civil and Political Rights of 1966 (ICCPR) both protect the right to privacy or private life[41] and mention the freedom to transfer data 'regardless of frontiers'.[42] This indicates that the ability to transfer data freely across national borders is essential to freedom of expression and freedom of opinion, as the negotiating history of the ICCPR shows.[43] At the same time, the free flow of information is not unlimited, and is subject to a balancing against other rights, including the right to privacy.[44]

Further instruments under international law support the free exchange of data globally. For example, Article 1(2) of the Constitution of the United Nations Educational, Scientific and Cultural Organization (UNESCO) of 1945 states that the Organization will 'promote the free flow of ideas by word and image', and the Agreement on the Importation of Educational, Scientific and Cultural Materials of 1950 (Florence Agreement) aims to facilitate 'the free flow of books, publications and educational, scientific and cultural materials'[45] by obligating signatory States not to impose customs duties or charges on their importation.[46] In the 1940s and 1950s, proposals were made in the United Nations for an international convention (or series of conventions) dealing with freedom of information, access to information, and its transmission between countries, but they did not gain the requisite support.[47]

[40] Note that in this context, 'freedom of information' has a different meaning than the right of citizens to gain access to data held by the public sector. Ploman (n 37), at 125, states that the distinction between the concepts of 'freedom of information' and 'free flow of information' is 'to some extent arbitrary', and rests on the fact that the UN has been dealing with the 'politico-juridicial aspects' of the issue under the heading of freedom of information, while UNESCO has been dealing with 'practical measures to promote the flow of information'.

[41] See UDHR, Article 12; ICCPR, Article 17. Neither instrument explicitly mentions data protection.

[42] See UDHR, Article 19, stating: 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and *regardless of frontiers*' (emphasis added); ICCPR, Article 19(2), stating: 'Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, *regardless of frontiers*, either orally, in writing or in print, in the form of art, or through any media of his choice' (emphasis added).

[43] See Lauri Hannikainen and Kristian Myntti, 'Article 19', in Asbjørn Eide et al. (eds), *The Universal Declaration of Human Rights: A Commentary* (Scandinavian University Press 1992), at 278, analysing the negotiating history of Article 19 of the UDHR and concluding that its aim 'was to promote an unobstructed flow of information in all directions and regardless of frontiers'.

[44] See Manfred Nowak, *UN Covenant on Civil and Political Rights (CCPR Commentary)* (N.P. Engel 1993), at 354, who states in commentary on Article 19 of the ICCPR that: 'The freedom to seek information may be limited in the interest of the rights of others. Principally conceivable here is the protection of privacy and intimacy pursuant to Art. 17'.

[45] Preamble to the Florence Agreement.

[46] These documents are all reproduced in Ploman (n 37), at 142–67, who cites several other international agreements promoting the free flow of information, some of them going back to the 19th century (eg, the Convention for the International Exchange of Official Documents and of Scientific and Literary Publications, Brussels, 1886).

[47] See Plowman (n 37), at 127–8.

E. Transborder data flows in international law

The regulation of transborder data flows for data protection or privacy reasons has not traditionally received much attention in public international law.[48] The normative basis of data protection law ultimately rests on human rights treaties such as the UDHR and the ICCPR that protect the right to privacy or private life[49] but do not mention data protection. Council of Europe Convention 108,[50] which is discussed later, is the only binding international treaty dealing with data protection, but so far is more of regional than global application. There have been calls for an international convention dealing with data protection and privacy; for example, in 2005 the 27th International Conference of Data Protection and Privacy Commissioners issued the 'Montreux Declaration', in which it appealed to the United Nations 'to prepare a binding legal instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights'.[51] Some companies have made similar appeals; for example, in 2007, Google called for the creation of 'global privacy standards'.[52] However, so far 'there does not exist a truly global convention or treaty dealing specifically with data privacy'.[53]

The International Law Commission (ILC) of the United Nations has stated that 'the international binding and non binding instruments, as well as the national legislation adopted by States, and judicial decisions reveal a number of core principles of data protection.[54] However, the ILC goes on to say that data protection is an area 'in which State practice is not yet extensive or fully developed'.[55] Since most data protection legislation relies on the same international documents, the fundamental, high-level principles of the law are similar across regions and legal systems,[56] but once one descends from the highest level of abstraction, there can be significant differences in detail. There is also considerable divergence in the details of regulation, their aims, and their legal nature.[57]

[48] See on the status of data protection under public international law Christopher Kuner, 'An International Legal Framework for Data Protection: Issues and Prospects', 25 Computer Law and Security Review 307, 309–11 (2009).

[49] See UDHR, Article 12 and ICCPR, Article 17.

[50] 28 January 1981, ETS 108 (1981).

[51] 27th International Conference of Data Protection and Privacy Commissioners, 'The protection of personal data and privacy in a globalised world: a universal right respecting diversities' (2005), <www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf>.

[52] See <http://googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html>.

[53] See Lee Bygrave, 'Privacy Protection in a Global Context—A Comparative Overview', in Peter Wahlgren (ed), *Scandinavian Studies in Law* 319 (Stockholm Institute for Scandinavian Law 2004), at 333.

[54] 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, Annex D, para. 11.

[55] ILC (n 54), Annex D, para. 12.

[56] Bygrave (n 53), at 347, stating: 'data privacy laws in the various countries expound broadly similar core principles and share much common ground in terms of enforcement patterns.'

[57] See Chapter 3.

Various organs of the United Nations have dealt with the subject of data protection since the late 1960s.[58] Most work on transborder data flow regulation has been done by the 'Commission on Transnational Corporations' of the UN Economic and Social Council, which in 1981 issued a report that gives much useful information on the way the subject was viewed at the time.[59] The report stresses both the risks and benefits of transborder data flows, and mentions that, while relatively few networks for data communication existed then, their growth was proceeding at a rapid pace,[60] with many of the transborder data flows that were taking place being carried out by corporations in the course of their business.[61]

In 1990, the United Nations issued its Guidelines concerning Computerized Personal Files, which take the form of a non-binding guidance document.[62] 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'.[63] 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 [sic] 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'.

Since adoption of the UN Guidelines, the United Nations has not been very active with regard to transborder data flow regulation, and issues under public international law have been dealt with mostly in regional organizations such as the EU or the Council of Europe rather than by UN institutions. It is thus not surprising that national data protection legislation tends to be more influenced by the OECD Guidelines, the EU Directive, or Council of Europe Convention 108 than by anything issued by the United Nations. Moreover, there seems to be little political will of UN member States to enact a multilateral convention dealing with data protection or transborder data flows.

[58] For an overview, see Mengel (n 4), at 183–244.

[59] Report of the Commission on Transnational Corporations of the Economic and Social Council of 6 July 1981, reprinted in Mengel (n 4), at 185–207.

[60] Mengel (n 4), at 188–90.

[61] Mengel (n 4), at 198, stating as an example that 'in the case of Canada, for instance, approximately 90 per cent of total net transborder data flows involve data flows from foreign affiliates in Canada to parent corporations abroad.'

[62] UN Guidelines concerning Computerized Personal Data Files of 14 December 1990, UN Doc. E/CN.4/1990/72, <http://www.unhcr.org/refworld/docid/3ddcafaac.html>.

[63] UN Doc. A/RES/45/95 (14 December 1990).

F. OECD Privacy Guidelines of 1980

The OECD is an international organization based in Paris that deals with economic and social policy and currently has 34 member countries[64] from various regions, including many EU Member States and countries from North America (eg, Canada and the US), the Asia-Pacific region (eg, Australia and Korea), and Latin America (eg, Chile and Mexico). This global membership gives the group's work on privacy considerable geographic reach. But the fact that the members of the OECD are largely developed, industrialized States raises questions about the legitimacy of its work for the less developed world.[65]

Discussion of transborder data flows began in the OECD in 1970, and culminated in publication of the OECD Privacy Guidelines 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.[66]

The Guidelines contain the following main provisions dealing with transborder data flows:

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.
17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

[64] Member countries are Australia; Austria; Belgium; Canada; Chile; Czech Republic; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Iceland; Ireland; Israel; Italy; Japan; Korea; Luxembourg; Mexico; Netherlands; New Zealand; Norway; Poland; Portugal; the Slovak Republic; Slovenia; Spain; Sweden; Switzerland; Turkey; the United Kingdom; and the US.

[65] See Michael Kirby, 'The history, achievement and future of the 1980 OECD guidelines on privacy', 1 International Data Privacy Law 6, 13–4 (2011).

[66] OECD Guidelines, Explanatory Memorandum, para. 25.

The OECD Guidelines represent the most global consensus yet achieved in the area of data protection and transborder data flow regulation, but were purposely written at a high level, and are focused on the facilitation of global data flows for economic purposes rather than on human rights.[67] The Guidelines may be implemented by law in the OECD member countries, but are not legally binding. At the time they were finalized, there was optimism that the Guidelines could lead to greater harmonization of data protection law;[68] in fact, since their enactment, the regulation of transborder data flows has become more diverse, reflecting differences in national and regional legal frameworks for privacy protection.

In 2010 the OECD initiated a process to review the Guidelines, to determine if they require amendment; this process had not been completed at the time this study was finalized.

G. Council of Europe Convention 108 and Additional Protocol

1. Background

The Council of Europe is an international organization with currently 47 State members working in the areas of human rights, the rule of law, and democracy.[69] Preparatory work on data protection law in the Council of Europe began as early as 1968, when the Committee of Ministers began a study on the protection of individuals' private sphere in light of developments in modern technology.[70] In 1981, the Council of Europe enacted its Convention 108,[71] which is 'the hereto sole international treaty dealing specifically with data protection',[72] and which entered into force on 1 October 1985. The Convention is also open for signature by countries that are not member States of the Council of Europe; no non-member has so far acceded to it, although on 31 March 2011 Uruguay officially requested permission to accede,[73] and several other non-members (particularly African and

[67] See Frits W. Hondius, 'A Decade of International Data Protection', 30 Netherlands International Law Review 103, 106 (1983), stating: 'the thrust of the Council of Europe's Convention is the protection of human rights; that of the OECD Guidelines the facilitation of transborder data flows'.

[68] See, eg, Michael D. Kirby, 'Transborder Data Flows and the "Basic Rules of Data Privacy"', 16 Stanford Journal of International Law 27, 65–6 (1980).

[69] Member countries are Albania; Andorra; Armenia; Austria; Azerbaijan; Belgium; Bosnia and Herzegovina; Bulgaria; Croatia; Cyprus; Czech Republic; Denmark; Estonia; Finland; France; Georgia; Germany; Greece; Hungary; Iceland; Ireland; Italy; Latvia; Liechtenstein; Lithuania; Luxembourg; the former Yugoslav Republic of Macedonia; Malta; Moldova; Monaco; Montenegro; Netherlands; Norway; Poland; Portugal; Romania; Russia; San Marino; Serbia; Slovakia; Slovenia; Spain; Sweden; Switzerland; Turkey; Ukraine; and the United Kingdom.

[70] Mengel (n 4), at 25.

[71] Convention for the Protection of Individuals with regard to Automatic Data Processing of Personal Data, 28 January 1981, ETS 108 (1981).

[72] Lee Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer Law International 2002), at 32.

[73] See 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)—Request by Uruguay to be invited to accede, 6 July 2011', in which the deputies invited Uruguay to accede; Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108], 'Opinion on Uruguay's request to be invited to accede to Convention 108 and its additional Protocol', T-PD (2011) 08 rev en (26 May 2011), <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD%20BUR_2011_08%20en.pdf>; 'Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (T-PD)—Abridged report of the 24th plenary meeting', 2 July 2008, in which the deputies of the Committee of Ministers agreed to take account of the T-PD's recommendation that countries that are not members of the Council of Europe be allowed to accede to Convention 108.

Latin American countries) are known to be considering doing so. Convention 108 is a high-level instrument that does not create rights for individuals[74] and is not directly applicable against private parties, but obligates States to implement in their law the protections that it provides.[75] It leaves considerable leeway for States to implement its provisions in different ways in light of their legal and constitutional systems.[76]

The Convention was an important milestone in the development of data protection as a fundamental right. Unlike the European Convention on Human Rights, membership of Convention 108 does not give rise to jurisdiction of the European Court of Human Rights, so that there is no direct judicial enforcement of the Convention. However, in some cases the European Court of Human Rights has referred to Convention 108,[77] and Article 8 of the European Convention on Human Rights probably includes the obligation to give effect to the provisions of Convention 108.[78] The EU has also committed to ensure that its law is consistent with the relevant conventions of the Council of Europe (though EU law may provide more extensive protection);[79] for example, the EU Charter of Fundamental Rights is to be interpreted in the same way as the European Convention on Human Rights.[80]

Article 12 of Convention 108 provides as follows:

> 1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
> 2. 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.

[74] Council of Europe Convention 108, Explanatory Report, para. 38.

[75] Council of Europe Convention 108, Article 3.

[76] Council of Europe Convention 108, Explanatory Report, at para. 39, stating that implementing measures 'can take different forms, depending on the legal and constitutional system of the State concerned: apart from laws they may be regulations, administrative guidelines, etc. Such binding measures may be usefully reinforced by measures of voluntary regulation in the field of data processing, such as codes of good practice or codes of professional conduct.'

[77] See, eg, *Amann v Switzerland* (2000) ECHR 87, para. 65; *Rotaru v Romania* (2000) ECHR 191, para. 43.

[78] See Paul De Hert and Serge Gutwirth, 'Data Protection in the Case law of Strasbourg and Luxembourg: Constitutionalisation in Action', in Serge Gutwirth et al. (eds), *Reinventing Data Protection?* 3 (Springer 2009), at 27.

[79] See Memorandum of Understanding between the Council of Europe and the European Union, May 2007, at para. 27.

[80] EU Charter of Fundamental Rights, Article 52(3).

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
   a. 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;
   b. when the transfer is made from its territory to the territory of a non-contracting State through the intermediary of 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.

In 2001 the Council of Europe adopted an Additional Protocol to the Convention, which may only be signed by the signatories to the Convention itself.[81] The relevant Article 2 of the Additional Protocol provides as follows:

1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.
2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:
   a. if domestic law provides for it because of:
      – specific interests of the data subject, or
      – legitimate prevailing interests, especially important public interests, or
   b. 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.

As of January 2013, the Convention had been ratified or acceded to by 44 Council of Europe member States, and the Additional Protocol by 33 of them, most of which are located in Europe or border on it. In addition to being in force in all (in the case of the Convention) or most (in the case of the Additional Protocol) EU Member States, both the Convention and the Additional Protocol are in force in several non-EEA (European Economic Area) and non-EU countries as well,[82] thus providing a source of legally binding regulation of transborder data flows beyond what is applicable in those regional groups.

[81] See Additional Protocol, Explanatory Report, para. 34.

[82] Non-EEA and non-EU Member States that have enacted the Convention include Albania; Andorra; Armenia; Azerbaijan; Bosnia and Herzegovina; Croatia; Georgia; the former Yugoslav Republic of Macedonia; Moldova; Monaco; Montenegro; Serbia; Switzerland; and the Ukraine, and those that have enacted the Additional Protocol include Albania; Andorra; Armenia; Bosnia and Herzegovina; Croatia; the former Yugoslav Republic of Macedonia; Moldova; Monaco; Montenegro; Serbia; Switzerland; and the Ukraine.

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, as follows:[83]

> **5.4. International communication**
>
> Communication of data to foreign authorities should be restricted to police bodies. It should only be permissible:
> a. if there exists a clear legal provision under national or international law,
> b. in the absence of such a provision, 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, and provided that domestic regulations for the protection of the person are not prejudiced.'

2. Modernization

In 2010 the Council of Europe began an ongoing process to modernize the Convention and update it in light of the many social, economic, and technological changes that have occurred since it was originally enacted. The proposals for modernization have been discussed for several years in the Council of Europe's Bureau of the Consultative Committee of the Convention for the Protection of individuals with regard to the Automatic Processing of Personal Data (known as the 'T-PD Bureau', and referred to throughout as the 'T-PD'), an expert group made up of representatives of Council of Europe member States, data protection authorities, and observers. The T-PD has built up a substantial body of expertise on the legal issues presented by the Convention, and on international data protection law in general.

The T-PD considered a number of drafting proposals for revision of Article 12 of the Convention and Article 2 of the Additional Protocol in the period from September 2011 to June 2012 (this period has been selected as representative since it is between when consideration of proposals to modernize these instruments began and the date of the group's first 2012 plenary meeting). Four of the texts were prepared by the Secretariat of the T-PD (most are available on the Internet[84]), and two were presented for discussion by the International Chamber of Commerce (ICC, which has official observer status in the group). These texts are the following:

- ICC proposal of 2 September 2011;
- Secretariat version of 15 November 2011;[85]
- Secretariat version of 18 January 2012;[86]
- ICC proposal of 31 January 2012;

[83] 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 (17 September 1987), Principle 5.4.

[84] See <http://www.coe.int/t/dghl/standardsetting/dataprotection/Modernisation_En.asp>.

[85] T-PD-BUR(2011) 27_en (15 November 2011), <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_27_en.pdf>.

[86] T-PD-BUR(2012)01EN (18 January 2012), <http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01_EN.pdf>.

4

National, Private Sector, and Technological Approaches

A. Introduction

Beginning in Europe, data protection laws have spread to all regions of the world, and a survey published in early 2012 named 89 countries worldwide as having them.[1] While not all data protection or privacy laws contain restrictions on transborder data flows,[2] the Appendix lists a minimum of 73 countries with laws that do so (ie, the 27 EU and three EEA member States, and 43 other countries),

[1] Graham Greenleaf, 'Global data privacy laws: 89 countries, and accelerating', Queen Mary University of London, School of Law Legal Studies Research Paper No. 98/2012 (2012), <http://ssrn.com/abstract=2000034>.

[2] An example of a data protection law that does not regulate transborder data flows is the Azerbaijani Law on Personal Data No. 998-IIIQ (2010).

representing approximately 38 per cent of the current 193 UN member States. This number does not include those countries that have not enacted such regulation at the level of national law but that are parties to international legal instruments such as the Additional Protocol to Council of Europe Convention 108, and those eligible to participate in voluntary systems such as the APEC Privacy Framework (which by itself covers 21 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.[3] If one includes all such instruments, then the number of countries regulating transborder data flows by means of data protection and privacy law is closer to 100. In addition to legislation, there is an increasing variety of private sector regulation such as contract clauses, codes of conduct, internal corporate rules, and others.

National legislation demonstrates a wide variety of approaches. The most influential model is the EU Directive: besides being directly applicable in the 27 EU and three EEA member States, it has significantly influenced transborder data flow regulation in other European countries (eg, Albania, Bosnia and Herzegovina, Serbia, and Switzerland), and in other regions like South America (eg, Argentina, Colombia, and Peru), Africa (eg, Angola, Benin, and Morocco), and Asia (eg, Macau and New Zealand). The influence of the EU Directive has been due at least in part to the perceived economic benefit that can accrue to countries that enact it and are then able to import personal data under an EU 'adequacy decision',[4] and the fact that it presents a single, clearly structured document that is seemingly easy to adopt (when participating in the work of international organizations dealing with legal harmonization, the author has observed that States often find it easier to use an existing regional text as a model rather than draft a new legal instrument from scratch). However, modelling transborder data flow regulation on the EU Directive raises complex issues, since the Directive is based on constitutional principles and fundamental rights under EU law. Other newer regional models (eg, the APEC Privacy Framework, and a potential model law being developed by the Organization of American States (OAS)) will no doubt gain influence as time goes on. Some countries show the influence of multiple approaches; for example, Russia

[3] Eg, in the German federal states and a number of Canadian provinces. See, eg, 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 H. Cate, 'Provincial Canadian Geographic Restrictions on Personal Data in the Public Sector' (2008), <http://www.hunton.com/files/tbl_s47Details/FileUpload265/2312/cate_patriot-act_white_paper.pdf>.

[4] See New Zealand Privacy Commissioner, 'Privacy amendment important for trade and consumer protection' (26 August 2010), <http://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.'

is part of APEC, but it bases the possibility of transferring personal data on the adequacy test derived from the EU Directive.[5]

Conspicuous by their absence from the list of countries with transborder data flow regulation are some of the major world economies such as China and the US, which together represent approximately one-third of global gross domestic product.[6] However, economic growth over the long term is likely to be higher in developing countries than in the more developed economies,[7] and many developing countries have adopted regulatory frameworks for transborder data flows, so that the economic power of countries that have enacted legislation will probably increase over time. Among the motivations for developing countries to enact such frameworks are the promotion of electronic commerce,[8] the protection of private life,[9] and the protection of privacy in connection with large-scale government data collection projects (such as digitalization of the electoral rolls).[10]

B. Listing of national approaches

The following overview of national transborder data flow regulation is organized by region, with comments on some provisions of particular interest; the Appendix contains English versions of all texts.

1. North America

Countries: Canada (federal and provincial level)

Canadian federal law does not explicitly regulate transborder data flows, but Canadian regulators have interpreted the Personal Information Protection and Electronic Documents Act (PIPEDA)[11] to require that data controllers within

[5] See Federal Law of the Russian Federation of 27 July 2006 No. 152-FZ on Personal Data (as amended by Law of 25 July 2011 No. 261-FZ), Article 12.

[6] See the Conference Board, 'Global Economic Outlook 2012', <http://www.conference-board.org/data/globaloutlook.cfm>, stating that in 2011 the US represented 18.6 per cent and China 15.8 per cent of global gross domestic product.

[7] See, eg, Carnegie Endowment for International Peace, 'The World Order in 2050' (April 2010), <http://www.carnegieendowment.org/files/World_Order_in_2050.pdf>, at 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'.

[8] See Government of Mauritius, Debate No. 12 of 01.06.04, Second Reading of the Data Protection Bill (No. XV of 2004), at 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'.

[9] See Burkina Faso, Assemblée Nationale, Dossier No. 06 relatif au projet de loi portant sur la protection des données à caractère personnel, at 3.

[10] See République du Sénégal, Rapport sur le projet de loi No. 32/2007 portant sur la protection des données à caractère personnel, at 3.

[11] See PIPEDA, Schedule 1, section 4.1 Principle 1: Accountability: 'An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles …'

Canada remain accountable for personal data they transfer to other countries.[12] The Canadian provinces of Alberta,[13] British Colombia,[14] Nova Scotia,[15] and Québec[16] have also enacted such legislation.

The European Commission has found that an adequate level of data protection exists for transfers of personal data to Canadian organizations subject to PIPEDA,[17] and for transfers of airline passenger name record (PNR) data to the Canada Border Services Agency,[18] as well as for transfers under the EU–US Safe Harbor agreement.[19] Bilateral agreements have been reached between the EU and the US finding that adequate protection exists for transfers of PNR data to the US Department of Homeland Security (DHS),[20] and providing protections for financial data accessed in the US for anti-terrorism purposes.[21]

[12] See Office of the Privacy Commissioner of Canada, 'Guidelines for Processing Personal Data across Borders' (2009), <http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_E.pdf>, at 5: 'PIPEDA does not prohibit organizations in Canada from transferring personal information to an organization in another jurisdiction for processing. However under PIPEDA, organizations are held accountable for the protection of personal information transfers under each individual outsourcing arrangement.'

[13] The Alberta Personal Information Protection and Electronic Documents Act, § 40(1)(g), permits the disclosure of personal information controlled by a public body in response to a subpoena, warrant, or order issued by a court only when the court has 'jurisdiction in Alberta'.

[14] The British Colombia Freedom of Information and Protection of Privacy Amendment Act, § 30.1, requires each public body to ensure that 'personal information in its custody or under its control is stored only in Canada and accessed only in Canada'; some exceptions are provided.

[15] The Nova Scotia Personal Information International Disclosure Protection Act (2006), § 5(1), requires that a public body ensure that 'personal information in its custody or under its control … is stored only in Canada and accessed only in Canada'; some exceptions are provided.

[16] The Québec Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information (2006), § 70.1, requires that before 'releasing personal information outside Québec or entrusting a person or a body outside Québec with the task of holding, using or releasing such information on its behalf', public bodies must ensure that the information receives protection 'equivalent' to that afforded under provincial law. In addition, the Act Respecting the Protection of Personal Information in the Private Sector, § 17, provides that an organization doing business in Québec that entrusts a person outside Québec with 'holding, using or communicating such information on its behalf' must take 'all reasonable steps to ensure' that the information will be used only for the purposes for which consent was obtained and will not be 'communicated to third parties' without such consent.

[17] Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, [2002] OJ L2/13.

[18] Commission Decision 2006/253/EC of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, [2005] OJ L91/49.

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

[20] Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, [2012] OJ L215/5.

[21] 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, [2010] OJ L8/11.

2. Latin America

Countries: Argentina,[22] Colombia,[23] Mexico,[24] Peru,[25] and Uruguay[26]

Provisions in Latin American countries show a strong influence of the EU Directive. Of particular interest is the Mexican Decree, which combines elements of the EU approach (eg, the use of consent) with other legal bases that would allow data transfer more liberally than is possible under existing EU law (eg, Article 37III, which would allow data transfers freely within corporate groups). The law of Peru creates broad exceptions for the transfer of data internationally between intelligence agencies to combat certain criminal phenomena, including 'the fight against terrorism, illegal drug trafficking, money laundering, corruption, human trafficking and other forms of organized crime'.[27]

The European Commission has found that an adequate level of data protection exists for data transfers to Argentina[28] and Uruguay.[29]

3. Caribbean countries

Countries: Bahamas,[30] Costa Rica,[31] St Lucia,[32] and Trinidad and Tobago[33]

Four Caribbean countries so far have enacted data protection legislation regulating transborder data flows. Barbados has been working on a data protection law that includes transborder data flow regulations, but it has not yet been passed. The Cayman Islands, which are a British Overseas Territory, have published a consultation document about potentially enacting data protection legislation.[34] The number of Caribbean countries with such laws may well grow, spurred on by activity of the OAS in this area.

[22] Personal Data Protection Act (4 October 2000), Act No. 25,326, Section 12.

[23] Law 1266 of 2008, Article 5; Law 1581 of 17 October 2012.

[24] Decree issuing the Federal Law on Protection of Personal Data Held by Private Parties (2010), Articles 36 and 37.

[25] Law No. 29733/2011 on the Protection of Personal Data, Articles 11 and 15.

[26] Data Protection Act, No. 18.331 (2008), Article 23.

[27] Law No. 29733/2011 on the Protection of Personal Data, Article 15.3.

[28] Commission Decision C (2003) 1731 of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, [2003] OJ L168.

[29] Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, [2012] OJ L227/11.

[30] Data Protection (Privacy of Personal information) Act (11 April 2003), Section 17.

[31] Law no. 8968/2011 on the Protection of Personal Data, Articles 14 and 31.

[32] Data Protection Act 2011, Article 28.

[33] Act No. 13/2011 on the Protection of Personal Privacy and Information, Section 72.

[34] See Consultation on the draft Data Protection Bill 2012 (September 2012), <http://www.dataprotection.ky/images/downloads/general%20public%20consultation%20paper.pdf>.

level of data protection' as provided under the Rules, the transfer is necessary for the performance of a contract between the corporate body or a person and the information provider, or the individual has consented to the transfer. The application of these rules in practice is as yet unclear.

10. Asia-Pacific countries

Countries: Australia,[80] *Macau (Macau Special Administrative Region (MSAR) of the People's Republic of China),*[81] *New Zealand,*[82] *and South Korea*[83]

Countries in the Asia-Pacific region have a wide variety of approaches to privacy, which may also differ from those of western countries like the US and the EU Member States.[84] It is thus not surprising that there are many divergent approaches to the regulation of transborder data flows, ranging from the absence of such regulation in most countries, to those influenced by the EU Directive (eg, New Zealand). The Australian Privacy Act allows transborder data flows under a number of conditions, such as when the data exporter 'reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles', the individual has consented to the transfer, or certain other conditions apply.[85] However, the Australian government was considering amendments to the Privacy Act in 2012 that would implement the accountability principle.[86] The South Korean Personal Information Protection Act, which was enacted in 2011, imposes a duty on data exporters to provide individuals with information about the transfer and to obtain their consent:

> (3) When a personal information manager provides a third person at any overseas location with personal information, he/she shall notify a subject of information of the matters referred to in each subparagraph of paragraph (2) and obtain the consent thereto, and shall not enter into a contract concerning the trans-border transfer of personal information stipulating any details contravening this Act.[87]

The European Commission has found that an adequate level of data protection exists for data transfers to New Zealand.[88] An agreement has been concluded between the EU and the Australian government finding that an adequate level of data protection is provided for transfers of PNR data to Australia.[89]

[80] Privacy Act 1988, as amended on 14 September 2006, Schedule 3, Principle 9.
[81] Personal Data Protection Act (Act 8/2005), Articles 19 and 20.
[82] Privacy Act 1993, Part 11A.
[83] Personal Information Protection Act, Law 10465 (2011), Article 17(3).
[84] See Hiroshi Miyashita, 'The evolving concept of data privacy in Japanese law', 1 International Data Privacy Law 229, 230 (2011).
[85] Schedule 3, Principle 9.
[86] See 'Privacy law reform: challenges and opportunities', remarks by Timothy Pilgrim, Australian Privacy Commissioner (23 February 2012), <http://www.oaic.gov.au/news/speeches/timothy_pilgrim/timothy_pilgrim_emerging_challenges_feb12.html>.
[87] Personal Information Protection Act, Law 10465 (2011), Article 17(3).
[88] European Commission, 'EU approves New Zealand's data protection standards in step to boost trade' (EU RAPID press release) (19 December 2012), <http://europa.eu/rapid/press-release_IP-12-1403_en.htm>.

11. Other countries

Some countries are considering the adoption of data protection and privacy legislation that includes regulation of transborder data flows (eg, Barbados,[90] Malaysia,[91] and South Africa[92]), or the amendment of their existing regulation (eg, Australia[93]). In Hong Kong (which is a Special Administrative Region of the People's Republic of China), privacy legislation is in force, but the specific provision dealing with transborder data flows is not.[94] The Singapore parliament has approved data protection legislation containing regulation of transborder data flows, but would allow any organization to be exempted from such requirements by the Singapore Data Protection Commission.[95]

Certain governmental entities in China may be preparing to enact transborder data flow restrictions. In 2011, the Chinese Ministry of Industry and Information Technology (MIIT) issued a proposed national standard entitled 'Information Security Technology—Guidelines for Personal Information Protection'. According to reports, the draft standard 'would prohibit the transfer of personal data abroad without explicit legal authorization or regulatory approval. It is not clear whether the standard would be mandatory for at least some industries, and whether any regulatory authority would issue guidelines or establish an approval procedure.'[96] In addition, 'Jiansu Province (where many foreign manufacturing joint ventures operate) has gone ahead on its own with a "Regulation of Information Technology" that came into force in January 2012. This ordinance generally requires consent or official approval for data transfers outside the province. The municipal government of Shenzen, near Hong Kong, has announced that it is preparing a similar ordinance.'[97]

[89] Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service, [2008] OJ L213/49.
[90] Data Protection Act (draft bill), § 4(2)(h).
[91] Personal Data Protection Bill (2010) (enacted but not yet in force), § 129.
[92] Protection of Personal Information Bill (2012) (still in the legislative process), Chapter 9, clause 72.
[93] See Parliament of the Commonwealth of Australia, House of Representatives, 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum', at 70–1 (discussing Section 16C of the proposed legislation).
[94] Personal Data (Privacy) Ordinance, § 33.
[95] Personal Data Protection Bill (Bill No 24/2012), Article 26.
[96] See W. Scott Blackmer, 'Transborder data flows at risk', Lexology 20 February 2012, <http://www.infolawgroup.com/2012/02/articles/cloud-computing-1/transborder-data-flows-at-risk/>.
[97] Scott Blackmer (n 96).