available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

An international legal framework for data protection: Issues and prospects

Christopher Kuner

Hunton & Williams, Brussels, Belgium

Keywords:
Data protection
Privacy
EU Data Protection Directive
Data protection in public international law
Harmonization of laws

ABSTRACT

The processing of personal data across national borders by both governments and the private sector has increased exponentially in recent years, as has the need for legal protections for personal data. This article examines calls for a global legal framework for data protection, and in particular suggestions that have been made in this regard by the International Law Commission and various national data protection authorities. It first examines the scope of a potential legal framework, and proceeds to analyze the status of data protection in international law. The article then considers the various options through which an international framework could be enacted, before drawing some conclusions about the form and scope such a framework could take, the institutions that could coordinate the work on it, and whether the time is ripe for a multinational convention on data protection.

1. Introduction

In recent years, a number of influential entities in both the public and private sectors have called for an international legal framework for privacy and data protection. 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'[1]; this appeal was repeated at later data protection commissioners' conferences, such as the 30th International Conference held in Strasbourg in 2008, and at the UN-sponsored World Summit on the Information Society (WSIS) held in Tunis in 2005.[2] Some companies have made similar appeals; for example, in 2007, Google called for the creation of 'Global Privacy Standards'.[3] And in 2009 a group of data protection authorities from around the world chaired by the Spanish Data Protection Authority began a process to draft a global legal instrument on data protection, with a view to submitting it to the United Nations.[4]

[1] See 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>.

[2] See 30th International Conference of Data Protection and Privacy Commissioners, Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Data Protection (2008), <http://privacyconference2008.org/index.php?page_id=197>.

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

[4] See Agencia Española de Protección de Datos, Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data (unpublished draft, January 2009; updated drafts dated 24 February and 24 April 2009).

2212-473X/$ – see front matter
doi:10.1016/j.clsr.2009.05.001

Two main rationales have been advanced for the drafting of international data protection standards:

- *Avoidance of gaps in data protection.* The lack of harmonized standards for data protection around the world, and the lack of any data protection legislation in most States, create risks for the processing of personal data.[5]
- *Facilitation of global data flows.* A growing number of databases are made accessible globally on the Internet, meaning that the same data processing may be subject to a large number of differing data protection standards, which creates substantial compliance burdens and uncertainty for business.[6]

Many of the calls for action are for a legally binding instrument or framework. For example, the International Law Commission of the United Nations has adopted the 'protection of personal data in transborder flow of information' in its long-term work program,[7] which could potentially result in the preparation of a draft international convention.[8] As quoted above, the Montreux Declaration also refers to a 'binding legal instrument'.

The issue of whether a global framework for data protection is desirable, and if so what form it should take, is becoming more acute owing to the growing importance of data processing in the global economy. The processing of personal data has become a key activity of both private-sector entities and governments, and the development of the Internet has made it possible for companies, governments, and individuals to transfer huge amount of data around the globe at the click of a mouse. Moreover, innovations such as 'cloud computing' allow vast amounts of personal data to be processed across national borders on a routine basis, thus severing the gap between data processing and territoriality, and increasing the need for a global regulatory framework for data protection.[9] These developments make it important to ensure both that the processing of personal data receives effective protection regardless of where it is carried out, and that data can flow freely between jurisdictions with as few impediments as possible,[10] which may be best achieved by a global framework for data protection, rather than a collection of national or regional approaches. However, to assess whether a global framework is feasible, it is important to consider what the obstacles are to an international data protection framework; the issues that would have to be faced for it to be approved and implemented; and lessons learned in other contexts about the harmonization of law that could be applied to data protection as well.

2. Scope of the framework

Calls for an international framework have tended to mix the terms 'data protection' and 'privacy'. For example, the resolution approved at the 30th International Conference in Strasbourg quoted above refers to 'the rights to data protection and privacy', while the principles adopted by the 'Global Network Initiative', a group formed by a number of companies, non-governmental organizations, and academics, deal with 'the internationally recognized human rights of freedom of expression and privacy', thus focusing more on privacy than on data protection.[11] The 'Global Privacy Standard', published in November 2006 by a working group led by the Ontario Information and Privacy Commissioner,[12] refers many times to 'privacy', but the principles themselves deal with topics such as consent, purpose limitation, and access rights, that have traditionally been thought to be key concepts of data protection law.

The concepts 'data protection' and 'privacy' are 'twins but not identical'.[13] Generally speaking, data protection law seeks to give rights to individuals in how data identifying them or pertaining to them are processed, and to subject such processing to a defined set of safeguards. Following enactment of the first data protection laws in Europe in the 1970s,[14] data protection was further defined in a ground-breaking judgment rendered in 1983 by the German Federal Constitutional Court,[15] and was adopted throughout the European Union by EU Data Protection Directive

[5] See *Strasbourg Resolution* (no. 2) stating 'The persisting data protection and privacy disparities in the world, in particular due to the fact that many States have not yet passed adequate laws, harm the exchange of personal information and the implementation of effective global data protection'.

[6] See the blog of Google Global Privacy Counsel Peter Fleischer, <http://peterfleischer.blogspot.com/2007/09/eric-schmidt-on-global-privacy.html>, stating that the lack of agreed global privacy standards 'creates uncertainty for business, which can restrict economic activity. How does a company, especially one with global operations, know what standards of data protection to apply in all the different markets where it operates?'

[7] ILC, Report on the Work of its Fifty-Eighth Session (1 May to 9 June to 11 August 2006) UN Doc A/61/10 para 257.

[8] See Statute of the International Law Commission, <http://untreaty.un.org/ilc/texts/instruments/english/statute/statute_e.pdf>, art 1 of which states that the ILC shall 'have for its object the promotion of the progressive development of international law and its codification', and art 15 of which defines the term 'progressive development of international law' as meaning 'the preparation of draft conventions on subjects which have not yet been regulated by international law…'

[9] See 'Let it rise: a special report on corporate IT', The Economist (25 October 2008) 1, stating that 'information technology is turning into a global ''cloud'' accessible from anywhere'.

[10] The removal of obstacles to the free flow of data within Europe was also one of the main reasons for enactment of the EU Data Protection Directive. See Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, Recital 3.

[11] See <http://www.globalnetworkinitiative.org/index.php>.

[12] Global Privacy Standard (8 November 2006), <http://www.ipc.on.ca/index.asp?navid=46&fid1=575>.

[13] Paul de Hert and Eric Schreuders, 'The Relevance of Convention 108' 33, 42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19–20 November 2001.

[14] See, eg, Hessisches Datenschutzgesetz of 30 September 1970 (Data Protection Act of the German federal state of Hessen); Loi no. 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (French Act No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties); Swedish Data Protection Act of 11 May 1973.

[15] Bundesverfassungsgericht, Judgment of 15 December 1983, 65 BVerfGE 1.

95/46 that has been implemented in all 27 EU Member States (and a number of non-EU European States as well). Data protection is also explicitly mentioned as a fundamental right in several EU Member State constitutions.[16]

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'.[17] In the United States, the US Supreme Court has interpreted the Constitution to protect, under the rubric of 'privacy', values that go beyond the protection of personal data, such as an individual's constitutional right to be free from unreasonable searches and seizures by the government[18]; the right to make decisions about contraception,[19] abortion,[20] and other intensely personal areas such as marriage, procreation, child rearing, and education[21]; and the right to associate free from government intrusion.[22] 'Privacy' can thus be seen as a concept which is both broader than and independent from data protection,[23] though there can be a significant overlap between the two.

There are also differences in the way these terms are understood in different legal systems and regions. Privacy has long been recognized in some States that do not have omnibus data protection laws.[24] However, data protection law is largely a European invention, although it has now begun to spread and has influenced the enactment of similar laws in jurisdictions as diverse as Argentina, Canada, the Dubai International Financial Center (DIFC), Hong Kong, Israel, and Russia.

Important questions also arise about whether certain areas of data processing should be exempted, in whole or in part, from data protection law. For example, the EU Data Protection Directive exempts from its scope the processing of personal data in the course of activities such as public security, defence, State security, and the activities of the State in the area of criminal law.[25]

Any international instrument would therefore need to clarify whether it covers data protection, privacy, or both, and whether any areas should be exempted from its scope. Since 'privacy' is a broader concept than 'data protection', it would seem more practical to limit the scope of any instrument or standards to data protection. Thus, this article focuses solely on a global framework for 'data protection'. However, it should be remembered that the two terms can overlap, and that some parties that have appealed for global standards may want them to cover both data protection and privacy.

3. Data protection in public international law

An increasing number of States have adopted data protection legislation in recent years, and a fundamental, legally binding right to data protection is recognized both in the national law of numerous States (particularly in Europe), and in certain regional legal instruments. The question then arises of whether data protection is similarly recognized in international law as a binding legal concept.

The normative basis of data protection law relies heavily on human rights treaties such as the Universal Declaration of Human Rights of 1948 (UDHR) and the International Covenant on Civil and Political Rights of 1966 (ICCP) that protect the right to privacy or private life.[26] However, these conventions do not explicitly mention data protection, and the only data protection instrument issued so far by the United Nations takes the form of a non-binding guidance document.[27] While some legally binding international conventions do contain a right to data protection (such as 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] and other instruments such as the European Convention on Human Rights[29] have served as the basis for court decisions recognizing a legal right to data protection,[30]

[16] See, eg, Belgian Constitution of 7 February 1831, last revised in July 1993, art 22; Portuguese Constitution of 2 April 1976, art 26; Spanish Constitution of 27 December 1978, art 18; Swedish Constitution of 1 January 1975, art 2.

[17] Parliamentary Assembly of the Council of Europe, Resolution 428, para C2 (1970). See Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 8, which describes privacy in terms of such rights as respect for private and family life, and the freedom from interference by public authorities.

[18] *Katz v United States*, 389 US 347 (1967).

[19] *Griswold v Connecticut*, 381 US 479 (1965).

[20] *Roe v Wade*, 410 US 113 (1973).

[21] Ibid 152–53.

[22] *NAACP v Alabama*, 357 US 449 (1958).

[23] See, eg, Case T-194/04 *Bavarian Lager v Commission* [2007] para 118, 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''".

[24] See, eg, Louis Brandeis, Samuel Warren, 'The right to privacy' (1890) Harvard Law Review 194, indicating the long-standing tradition of privacy in the United States. Despite the lack of omnibus data protection legislation in the United States, the Code of Fair Information Practices adopted by the HEW (Health, Education, Welfare) Advisory Committee on Automated Data Systems of the US federal government played an important role in the development of data protection concepts. See US Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii (1973), <http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm>.

[25] Article 3(2). The EU has since adopted a Council Framework Decision on data protection concerning police and judicial cooperation in criminal matters. Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters [2008] OJ L350/60.

[26] See UDHR art 12, and ICCP art 17.

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

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

[29] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 8.

[30] See, eg, *Rotaru v Romania* (App no. 28341/95), ECHR 2000-V.

such conventions have been concluded on a regional rather than a global basis. Thus, 'there does not exist a truly global convention or treaty dealing specifically with data privacy'.[31]

The International Law Commission (ILC) was established in 1948 under a resolution of the UN General Assembly,[32] and is charged with promoting 'the progressive development of international law and its codification'.[33] The ILC is composed of some of the most eminent specialists in public international law. In 2006 the Codification Division of the UN Office of Legal Affairs prepared a report on behalf of the ILC entitled 'Protection of Personal Data in Transborder Flow of Information'.[34] The report 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[35]; however, it is doubtful whether such principles have won broad recognition among States. The number of States with data protection authorities is a good measure of the number with legal regimes for data protection, since the existence of an independent data protection authority is generally regarded as a prerequisite for an adequate data protection regime (at least under European views of data protection).[36] As of December 2008 there were 192 Member States of the United Nations, while privacy and data protection authorities from 41 States were accredited to the 29th International Conference of Data Protection and Privacy Commissioners held in September 2007 in Montreal.[37] If one adds to this number an additional 10–20 data protection authorities to take into account those States that are known to have authorities but were not accredited at the Montreal conference,[38] then it seems that no more than one quarter to one third of States (50–60) currently have a comprehensive legal framework for data protection.

The ILC has admitted that data protection is an area 'in which State practice is not yet extensive or fully developed',[39] and the Statute of the ILC suggests that codification should take place 'in fields where there has already been extensive State practice, precedent and doctrine'.[40] The ILC goes on to say with regard to work in the area of data protection that it 'may nevertheless be able to identify emerging trends in legal opinion and practice which are likely to shape any international legal regime which would finally emerge.'[41] All of this suggests that a binding international legal instrument covering data protection would be premature, and that actions such as the identification of trends would be more appropriate than would the preparation of a convention.

Since most data protection legislation is based on the same international documents, the fundamental, high-level principles of the law are similar across regions and legal systems.[42] However, the differences in the cultural, historical, and legal approaches to data protection mean that once one descends from the highest level of abstraction, there can be significant differences in detail. This is not surprising, since concepts such as 'data protection' and 'privacy' are derived from national legal culture and tradition, and thus vary considerably around the world, even in systems that accept the same fundamental principles. For example, the APEC Privacy Framework[43] and EU data protection law are both largely based on the OECD Privacy Guidelines, and the United States has accepted the OECD Guidelines as well, but there are significant differences between the APEC and EU approaches to data protection,[44] and the EU does not accept the US as generally providing an 'adequate level of data protection' under EU Data Protection Directive 95/46.[45]

Most data protection authorities view data protection as a human right of universal application.[46] However, while it seems that human rights norms may constitute part of customary or general international law, there is a lack of agreement about the content of such norms beyond the most serious ones, such as the prohibitions against genocide, slavery, torture, and systematic racial discrimination.[47] The

[31] See Lee Bygrave, 'Privacy protection in a global context—a comparative overview', in: Peter Wahlgren, editor, Scandinavian studies in law, 319, 333 (Stockholm Institute for Scandinavian Law 2004).

[32] UNGA Res 174(II) (21 November 1947).

[33] Statute of the International Law Commission, art 1(1).

[34] *ILC Report* (no. 7), Annex D. The Codification Division acts as the secretariat of the ILC.

[35] Ibid para 11.

[36] See, eg, Council of Europe Convention 108, Additional Protocol, art 1.

[37] See International Conference of Privacy and Data Protection Authorities, Accredited Authorities, 25–28 September 2007 (unpublished). Many more authorities than 41 were accredited to the conference, since some States have multiple data protection authorities, and some other authorities represented international or supranational bodies.

[38] For example, the Dubai International Financial Center, Israel, Japan, and Russia.

[39] *ILC Report* (no. 7), Annex D, para 12.

[40] Article 15.

[41] *ILC Report* (no. 7), Annex D, para 12.

[42] See Bygrave, *Privacy protection in a global context* (no. 31) 347, stating that 'data privacy laws in the various countries expound broadly similar core principles and share much common ground in terms of enforcement patterns'.

[43] APEC Privacy Framework (2005), <http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html>.

[44] See Lee Bygrave, 'International agreements to protect personal data', in: James B. Rule, Graham Greenleaf, editors, Global privacy protection: the first generation, 15, 44–45 (Edward Elgar 2008); Graham Greenleaf, 'Five years of the APEC Privacy Framework: failure or promise?' Computer Law & Security Review 2009, 28; Chris Pounder, 'Why the APEC Privacy Framework is unlikely to protect privacy', <http://www.out-law.com/page-8550>, stating that the APEC Framework 'is unlikely to provide an adequate level of protection as required by the European Data Protection Directive'.

[45] This is demonstrated by the fact that only those data transfers from the EU made to US entities that have joined the US 'safe harbor' scheme have been formally determined to provide an adequate level of data protection. Commission Decision (EC) 2000/520 of 26 July 2000 pursuant to Directive (EC) 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215/7.

[46] See *Strasbourg Resolution* (no. 2), stating 'The rights to data protection and privacy are fundamental rights of every individual irrespective of his nationality or residence'.

[47] See Ian Brownlie, Principles of Public International Law (7th ed. Oxford University Press 2008), 563; American Law Institute, Restatement of the law, the third, the Foreign relations law of the United States (3rd ed. American Law Institute Publishers 1990) § 702.

European Court of Justice has found that the right to data protection must be balanced against other fundamental rights.[48] Also, the European Court of First Instance has found that even the right of a litigant in court to have his case heard on the merits does not constitute a rule of *jus cogens* under international law,[49] and the right to a trial is more widely accepted on an international scale than the right to data protection is.[50] Given the differences between approaches to data protection legislation in various States and regions, and the fact that there are few legally binding instruments on the international level, it is also questionable whether there is both 'substantial uniformity of practice' regarding data protection and the widespread practice among States to regard data protection as 'law', both of which are necessary for the creation of a rule of customary international law.[51]

There is increasing momentum for the adoption of data protection laws by States, and European concepts of data protection have spread to other regions as well. At the same time, there are still substantial cultural and legal differences between various States and regions regarding their approach to data protection, and most States still have no data protection law at all. Thus, there do not yet seem to be sufficient grounds for recognizing a global legal right to data protection in the same way that other fundamental, universal human rights are recognized.

4. Options for an international legal framework

4.1. *General considerations*

Producing an international legal framework for data protection based on agreed standards may be thought of as the 'harmonization' or 'unification' of data protection law, terms which will be referred to synonymously here as 'harmonization'.[52] The primary motivation for the harmonization of laws has been described as 'to reduce the impact of national boundaries',[53] which fits well with the motivation of many advocates of an international data protection framework to facilitate the flow of personal data around the world. There are many different types of harmonization instruments, which can include a multilateral treaty or convention; a model or uniform law which States can enact into their national law; a codification of custom and usage promulgated by a non-governmental organization; terms and conditions that can be incorporated into contracts and other documents concluded between private parties; and others.

Each approach to harmonization has its strengths and weaknesses. A convention can produce a greater degree of harmonization, since it results in a single text that is legally binding on States that enact it, but such binding nature can make States reluctant to do so. A convention can also be subject to reservations made by States that are party to it, which can result in a diminution of the very harmonization that the convention was supposed to accomplish, and a convention can be difficult to amend in the face of changing practices or technological evolution.[54] A model law allows States more flexibility in implementation, which may incline them to adopt it, but this very flexibility can result in a lack of harmonization in implementation. Guidance documents and contractual terms and conditions can be adopted more swiftly and be taken up by a large number of parties, but their legally binding nature is of a lesser value than that of a multilateral convention.

The approach taken by organizations such as the United Nations Commission on International Trade Law (UNCITRAL) and the International Institute for the Unification of Private Law (UNIDROIT) has generally been to harmonize 'interface laws', ie, the laws that affect transactions between persons in different States.[55] In the context of data protection law, this could mean ensuring that legal rules allow personal data to flow between States with a minimum of restrictions, or granting some sort of legal recognition to compliance steps taken in other States. In fact, the harmonization of 'rules that operate at the interface of transactions between nations' has been called the most successful type of legal harmonization.[56] An alternate approach would be to harmonize national or domestic data protection rules, so as to minimize the significance of differences between national laws, but this approach would be complicated by the fact that in many States data protection law is regarded as a fundamental human right of constitutional stature and is thus not easily amended.

4.2. *Multilateral conventions*

One option for an international framework would be to adopt a multilateral convention on data protection, which could be drafted by the International Law Commission (ILC). The background paper proposing the incorporation of data protection into the ILC's work states that it has the objective of elaborating 'general principles that are attendant in the

[48] Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-271 paras 65 and 68.

[49] Case T-315/01 *Kadi v Council* [2005] ECR II-3649 paras 286–87. This judgment was reversed by the European Court of Justice in Joined Cases C-402/05 P and C-415/05 P *Kadi v Council* [3 September 2008]. However, in its judgment the Court of Justice explicitly stated that it was not addressing the Court of First Instance's conclusions regarding the scope of *jus cogens* (see para 329 of the ECJ judgment). See Paul James Cardwell, Duncan French, Nigel White, 'Case note on the *Kadi* judgment' (2009) International and Comparative Law Quarterly 229.

[50] For example, both the Universal Declaration of Human Rights (art 11) and the International Covenant on Civil and Political Rights (art 9) enshrine the right to a trial (for criminal offenses).

[51] Statute of the International Court of Justice art 38.1.b; see *Brownlie* (no. 47) 7–8.

[52] However, technically speaking, there is a distinction to be made between 'harmonization' and 'unification' of the law, as pointed out on the UNCITRAL web site (<http://www.uncitral.org/uncitral/en/about/origin_faq.html>).

[53] Roy Goode, 'Reflections on the harmonisation of commercial law' (1991) Uniform Law Review 54.

[54] See Souichirou Kozuka, 'The economic implications of uniformity in law' (2007) Uniform Law Review 683, 693, stating that 'ironically, the more popular a Convention is, the more difficult it is to amend the uniform law in a timely manner'.

[55] See John Goldring, 'Globalisation, national sovereignty and the harmonisation of laws' (1998) Uniform Law Review 435, 437.

[56] Ibid 450.

protection of personal data', and that 'such an exercise would assist in facilitating the preparation of a set of internationally acceptable best practices guidelines and would assist governments in the preparation of national legislation. It would also assist the industry in devising models for self-regulation.'[57] It is further stated that the proposal does not address 'the general question of privacy', and is concerned instead with 'the individual's control over the processing of personal information – its acquisition, disclosure and use, a concept usefully referred to as ''fair record management.''[58] Moreover, the proposal is restricted to addressing personal data flows or transborder data flows.[59] The proposal declares that 'the processing of personal data must be interpreted in accordance with human rights principles',[60] and goes on to identify a number of core principles of data protection.

Another option could be to base a global data protection framework on the General Agreement on Trade in Services (GATS) under the auspices of the World Trade Organization (WTO), which is arguably appropriate given that data flows across national borders for commercial purposes have become ubiquitous. However, since the focus of the GATS is on trade liberalization and promoting economic growth,[61] it is doubtful whether the WTO would be capable of dealing with data protection as a human right. In addition, the GATS specifically exempts data protection regulations from scrutiny under world trade law.[62] Other international organizations such as the United Nations Educational, Scientific and Cultural Organization (UNESCO)[63] and the International Telecommunications Union (ITU) may be considered as possible focal points for work on global data protection standards, but they are also specialized agencies that may not be well-suited to produce standards in an area as diverse and multi-faceted as data protection.

There are disadvantages to basing a global framework for data protection on a binding multilateral convention. One is that the drafting of any such convention would likely take many years: for example, it has been stated that the conclusion of a multilateral convention for legal harmonization seems to take a minimum of ten years,[64] and in some cases may take much longer.[65] The work of the International Law Commission proceeds in five-year terms, and the ILC has not yet appointed a rapporteur for work on data protection, nor is any further worked planned in the near future.[66] Thus, it can be assumed that any ILC proposal for a convention would only be finalized far into the future, if at all. Negotiation of a multilateral convention might also lead to a lowest-common-denominator set of data protection standards, given the difficulties of obtaining the agreement of many States.

Moreover, although a multilateral convention is legally binding in international law, it may still not produce a harmonized legal framework. For example, Council of Europe Convention 108 is not intended to be self-executing and permits derogations in some significant areas.[67] In addition, depending on the rules in national law regarding the adoption of international conventions, if a convention is implemented into domestic law, then the relevant provisions can be amended under the constitutional law of that State, regardless of its obligations under international law.[68] Thus, harmonization of the law requires not just enactment of a convention, but its uniform application in national legal systems.[69]

4.3. *Regional conventions and treaties*

Harmonization of data protection law could also proceed at a regional level. This has the advantage that a regional, supranational organization such as the European Union may directly adopt texts that have the force of law in all Member States, while multilateral treaties are typically promulgated by international organizations such as the United Nations and only become binding law if States decide to adopt them.[70]

A number of regional organizations have either adopted data protection instruments, or have appealed for their

[57] *ILC Report* (no. 7), Annex D, para 12.
[58] Ibid 499–500.
[59] Ibid 501.
[60] Ibid 505.
[61] Final Act Embodying the Results of the Uruguay Round of Multilateral Trade Negotiations: Annex 1b, General Agreement on Trade in Services (GATS) Preamble, referring to the wish 'to establish a multilateral framework of principles and rules for trade in services with a view to the expansion of such trade under conditions of transparency and progressive liberalization and as a means of promoting the economic growth of all trading partners and the development of developing countries…'
[62] See GATS art XIV(c) (ii), stating that 'Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures … (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to … (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts…'
[63] See Graham Greenleaf, 'UNESCO starts Asia-Pacific response to Montreux Declaration' (2006) Privacy Law & Policy Reporter 219.
[64] *Goode* (no. 53) 62.
[65] For example, the Vienna Convention on the Law of Sales of 1980 was the result of over 50 years' work. See *Goldring* (no. 55) 448.
[66] E-mail correspondence (8 December 2008) and meeting (16 April 2009) with the Director of the Codification Division of the UN Office of Legal Affairs.
[67] See Lee Bygrave, Data protection law: approaching its rationale, logic and limits (Kluwer Law International 2002) 34, citing arts 3, 6, and 9 of the Convention.
[68] See Alan Rose, 'The challenges for uniform law in the twenty-first century' (1996) Uniform Law Review 9, 13.
[69] Ibid 14: '[U]ltimate uniformity is not guaranteed by mere accession to an internationally binding instrument but results from and depends as much on the form and substance of any domestic implementing legislation and the interpretation of that legislation in domestic courts. The acid test occurs with the actual adoption in practice and application by a domestic court of a uniform rule in a contested situation'.
[70] See José Angelo Estrella Faria, 'Legal Harmonization through Model Laws: the Experience of the United Nations Commission on International Trade Law' (UNCITRAL) 8, <www.doj.gov.za/alraesa/conferences/papers/s5_faria2.pdf>.

adoption. Beyond the existing European data protection instruments, calls for international data protection standards have been made, for example, by the 11th Summit of La Francophonie held in Budapest in September 2006, and the Ibero-American Data Protection Network at its sixth meeting held in Colombia in May 2008. A prominent example of regional data protection standards is the APEC Privacy Framework, which is a set of nine privacy principles that members of the Asia-Pacific Economic Cooperation (APEC) countries may voluntarily implement in their national economies.[71] The APEC framework is designed to be a flexible system that can be implemented in the vastly differing cultural and legal frameworks of the twenty-one APEC Member States.

Another option would be to have States accede to Council of Europe Convention 108. The Council of Europe has opened accession to the Convention to non-member States,[72] and views the Convention as having potentially 'universal' application, ie, as proving the basis for global data protection standards.[73] Some Member States of the Council of Europe, such as France, have also called for promotion of Convention 108 as an international standard.[74]

However, certain factors would seem to restrict the possibility of using Convention 108 as the basis for a global data protection framework. Accession to the Convention by non-member States of the Council of Europe is only open to those with data protection legislation that is in accordance with the Convention,[75] which greatly restricts the number of States that may join. This restriction reflects the intention of the Convention's drafters, who seemingly had non-European OECD Member States in mind as potential candidates for accession,[76] and many of the OECD Member States already have data protection laws. In addition, accession to the Convention by non-Council of Europe Member States does not create binding rights on behalf of individuals, since individual rights cannot be derived from a convention which is not self-executing,[77] and non-member States acceding to the Convention are not obliged to accede to the European Convention on Human Rights, unlike Council of Europe Member States. Thus, while Convention 108 may be enforced against Council of Europe Member States before the European Court of Human Rights, there could be no enforcement of the Convention against States acceding to it who are not members of the Council of Europe, which would undermine the rationale for having a binding legal framework for data protection in the first place.

A regional approach could also fail to produce international harmonization, given that having differing regional instruments may itself lead to a splintering of the law rather than harmonization. In order to produce harmonization, it would be necessary to find some way for the different regional approaches to data protection to interface with each other in a harmonized manner. One way to accomplish this goal would be through the conclusion of instruments for recognition of foreign data protection standards. This kind of system is foreseen in, for example, EU Data Protection Directive 95/46, which generally restricts the transfer of personal data to countries outside the European Union, but allows the European Commission to issue decisions recognizing such countries as providing an 'adequate level of data protection'.[78] In theory, this could facilitate the recognition of data protection standards between different regions and legal systems, which could then gradually converge toward a global standard. However, in the ten years since the Directive came into force, only a handful of adequacy determinations have been rendered by the European Commission,[79] indicating that the mutual recognition of different data protection standards based upon their purported adequacy is not an efficient or effective mechanism for the creation of global standards. More promising along these lines is the APEC Privacy Framework, which encourages APEC Member States to support the development of 'cross-border privacy rules' adopted by organizations (such as companies) across the APEC region, and to 'work with appropriate stakeholders to develop frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between and among the economies'.[80] The APEC mutual recognition approach is more flexible than one based on 'adequacy', but it would likely take years (or even decades) for it to become widely accepted on an international scale.

4.4. *Model laws*

Another approach would be to enact a model law on data protection which States could enact into their own national legal structures. The International Law Commission has considered elaborating 'general principles that are attendant in the protection of personal data', and has stated that it 'would assist governments in the preparation of national legislation',[81] which approach seems similar to the preparation of a model law. The model law approach has been used

[71] See *APEC Privacy Framework* (no. 43).

[72] Council of Europe, Committee of Ministers, 1031st meeting (2 July 2008), Decision, Item 10.2.

[73] See 29th International Conference of Data Protection and Privacy Commissioners, Montreux Declaration—First Periodic Evaluation (unpublished report) (25–28 September 2007) 6, quoting the Secretary General of the Council of Europe as referring to the 'potentially universal mission of Convention 108'.

[74] Eric Besson, *France numérique 2012, Plan de développement de l'économie numérique* (October 2008) 49, <http://francenumerique2012.fr>, stating that it is a goal of the French government to promote a global data protection convention and to promote adhesion to existing international legal instruments such as Convention 108.

[75] *Council of Europe Decision* (no. 72).

[76] See Convention 108, Explanatory Report, para 90, stating that 'The Convention was elaborated in close cooperation with OECD and the non-European member countries of that organisation and it is in particular those countries which one had in mind when this article [ie, art 23 governing accession by non-member countries] was drafted'.

[77] Ibid para 38.

[78] *Directive 95/46* (no. 10), art 25.

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

[80] *APEC Privacy Framework* (no. 43), para 47.

[81] *ILC Report* (no. 7), Annex D, para 12.

successfully in a number of areas by UNCITRAL, such as in the UNCITRAL Model Law on Electronic Commerce of 1996. On the other hand, negotiation of the UNCITRAL Model Law on Electronic Signatures of 2001 was more difficult, because of different understandings of the subject matter by States and the evolving nature of the technologies for electronic signatures.[82] Thus, it is not clear whether the adoption of a model law by States would truly lead to harmonization of data protection law, though it would have the advantage of being more acceptable to States that might be uncomfortable with a binding convention.

4.5. *Non-binding technical standards*

Several groups have already created technical standards for data protection and privacy which are not legally binding, but which can be adopted by States and organizations on a voluntary basis. Professor Lawrence Lessig famously proclaimed that 'code is law', ie, that 'the software and hardware that make cyberspace what it is *regulate* cyberspace as it is',[83] and it could be argued that technical standards for data processing could lead to globally-harmonized data protection practices more swiftly and effectively than an international convention could. Bodies such as the International Telecommunications Union (ITU) and the World Wide Web Consortium (W3C) have promulgated technical standards that have proven highly influential for the processing of personal data,[84] and several organizations are also working on data protection standards. For example, the International Organization for Standardization (ISO) has been working on voluntary standards for privacy protection, and regional bodies have also issued such standards.[85]

In a practical sense, such technical standards may be more influential in determining how personal data are processed than most laws are. But technical standards do not represent a panacea, since they may be implemented differently in different regions and sectors; must be carefully drafted so as not to advance the interests of a particular industry, sector or company[86]; and can be overtaken by new technological developments. Thus, while technical standards will likely play an increasingly important role in the global harmonization of data processing rules, they are unlikely to be a complete solution to problems presented by the absence of a global legal framework for data protection.

4.6. *International guidelines, recommendations, and codes of practice*

A number of international guidelines and recommendations in the area of data protection have proved influential, even though they are not legally binding. Such instruments 'tend to be aimed not just at encouraging enactment of national rules but also harmonisation of these rules'.[87] The earliest such guidelines were the UN Guidelines concerning Computerized Personal Data Files of 14 December 1990,[88] which contain high-level data protection principles but are not legally binding and have been of limited practical relevance. The OECD Privacy Guidelines[89] are also not legally binding but have been highly influential in inspiring the enactment of data protection legislation in many regions around the world.[90] Governments have also agreed between themselves on data protection principles for information shared for law enforcement purposes.[91] Such international guidelines have also been published on a sectoral basis; an example is the code of practice entitled 'Protection of workers' personal data' published by the International Labour Office of the UN.[92]

4.7. *Non-binding policy standards*

Various groups have issued policy documents containing voluntary data protection principles that are designed to be used on a global basis. For example, on 8 November 2006, a working group led by the Ontario Information and Privacy Commissioner published a 'Global Privacy Standard'.[93] Also, in late 2008, a number of companies, non-governmental organizations, and academics established the 'Global Network Initiative', which is defined as 'a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector'.[94]

4.8. *Legislative guides and private-sector instruments*

UNCITRAL has adopted legislative guides and recommendations in order to advance the objective of harmonization in

[82] See José Angelo Estrella Faria, 'Drafting and negotiating history of the electronic communications convention', in: Amelia H. Boss, Wolfgang Kilian, editors, The United Nations convention on the use of electronic communications in international contracts (Wolters Kluwer 2008) 17, 30.

[83] Lawrence Lessig, Code and other laws of cyberspace (Basic Books 1999) 6.

[84] For example, the ITU's international allocation of radio-frequency spectrum has established a de facto standard which is followed in 191 ITU Member States; and the W3C has published over 110 technical standards for the World Wide Web, see <http://www.w3.org/Consortium>.

[85] See, eg, ISO, TMB Task Force on Privacy, June 2008, SCC (Canada) request to the TMB to review Privacy, giving an overview of ISO privacy standardisation work. Among the regional bodies the document refers to that have done work on privacy standardisation are ANSI, CEN/ISSS, and PRIME.

[86] See 'Clash of the clouds', The Economist (4 April 2009) 56–7, describing how certain companies are attempting to establish technical standards for 'cloud computing' because widespread adoption of such standards 'would expand the market for their products'.

[87] See Bygrave, *Privacy Protection in a Global Context* (no. 31) 336.

[88] UN Doc E/CN.4/1990/72.

[89] Organisation for Economic Cooperation and Development (OECD), Recommendation of the Council concerning guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980).

[90] See Bygrave, *Data Protection Law* (no. 67) 32.

[91] See, eg, Statement on Information Sharing and Privacy and Personal Data Protection between the European Union and the United States of America, 13 December 2008, <http://www.dhs.gov/xlibrary/assets/usa_statement_data_privacy_protection_eu_12122008.pdf>.

[92] See <www.ilo.org/public/english/protection/condtrav/pdf/wc-code-97.pdf>.

[93] See <http://www.ipc.on.ca/index.asp?navid=46&fid1=575>.

[94] See <http://www.globalnetworkinitiative.org/index.php>.

situations where national legal systems use widely disparate legislative techniques for solving an issue, or States are not yet ready to agree on a single approach or common rule.[95] Such texts can provide a set of possible legislative solutions to an issue depending on the particular national context, and may provide a standard against which governments can review and update existing law.

Private-sector groups have also published such guides and recommendations; an example is the 'Privacy Toolkit' published by the Task Force on Privacy and the Protection of Personal Data of the International Chamber of Commerce (ICC), which outlines principles for privacy protection for governments and companies based on the OECD Guidelines and suggests ways to implement them in practice.[96] Other private-sector instruments also play an important role in protecting personal data processed on a global scale; examples include contractual clauses containing protections for data transferred in the course of commercial transactions,[97] and online privacy policies of companies.

5. Conclusions

Different opinions have been expressed as to the likelihood of developing an international legal framework for data protection. One commentator has stated:

> *The chances of achieving, in the short term, greater harmonisation of privacy regimes across the globe are slim. This is due not simply to the strength of ingrained ideological and cultural differences around the world, but also to the lack of a sufficiently strong, dynamic and representative international body to bridge those differences … [F]uture international policy making on privacy issues will be increasingly complicated and, arguably, increasingly destined to fail in terms of offering clear and relatively stringent norms.*[98]

On the other hand, Google has stated that 'surely, if privacy principles can be agreed upon within the 21 APEC member economies, a similar set of principles could be applied on a global scale'.[99]

At a minimum, the following questions would have to be addressed in order to construct a global legal framework for data protection:

The form of the legal framework: a decision would have to be made as to whether global standards should be legally binding or non-binding in nature. Each option would have advantages and disadvantages. A binding legal framework would address the problems that have led to the calls for a global framework, namely the lack of data protection standards in many States, and the difficulties that data controllers face in applying differing legal standards to the same data processing. At the same time, a legally binding framework (most likely embodied in a multilateral convention) would take much longer to draft and approve than would a non-binding framework, and would also be subject to many more political hurdles. Moreover, experience in the unification of private law has shown that States tend to give a low priority to the implementation of such conventions, so that it is questionable whether enactment of a convention would lead to true harmonization.

Whether an existing instrument should be used, or a new one should be drafted: a number of international instruments already exist that could serve, at least in theory, as the basis for an international legal framework for data protection. These include conventions such as Council of Europe Convention 108, or international guidelines such as the OECD Privacy Guidelines. However, political factors would likely make it difficult to re-open existing international instruments, and using a regional convention as the basis for an international instrument could prove controversial.[100] Moreover, not all such instruments are legally binding in nature. The alternative would be to produce a new instrument, such as a convention drafted by the International Law Commission, but this would likely take a long time. The drafting of a non-binding instrument such as a model law on data protection could be another option, but steps would have to be taken to encourage States to implement it in a uniform manner.

The standards that would serve as the basis for an instrument: principles would have to be drafted to provide the substance of the data protection rules incorporated in any international framework. While there is broad international agreement on the principles of data protection law at the highest level as embodied in instruments such as the OECD Privacy Guidelines, once one begins going into more detail, the differences between the different regional and national approaches become pronounced. It is precisely in areas where national law and policy differ that efforts to harmonize the law are most difficult,[101] and the details of data protection law differ substantially between different regions and legal systems.

The institution that would coordinate the work: an international institution would have to coordinate the work on a global instrument for data protection. Data protection law is a mixture of various legal areas, such as human rights law, public law, private law, and others, and not all these different areas have traditionally been covered in the work of the

[95] An example is the UNCITRAL Recommendation on the Legal Value of Computer Records (1985). See Estrella Faria, *Legal Harmonization through Model Laws* (no. 70) 15.

[96] See <http://www.iccwbo.org/policy/ebitt/id5289/index.html>.

[97] See, eg, Commission Decision (EC) 2004/915 of 27 December 2004 amending Decision (EC) 2001/497 as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries [2004] OJ L385/74, in which the European Commission approved a set of standard contractual clauses for international data transfers that were originally proposed to the Commission by seven business associations, including the International Chamber of Commerce.

[98] Bygrave, *International Agreements* (no. 44) 48–9.

[99] Peter Fleischer on the Google Public Policy Blog on 14 September 2007, 'Call for Global Privacy Standards', <http://googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html>.

[100] See, eg, Peter Ford, 'Asia-Pacific privacy: some myths exposed' (October 2008) Privacy Laws & Business International Newsletter 11, where the author, a former Australian government official, questions whether European data protection rules should be viewed as a model for the Asia-Pacific region.

[101] See *Goldring* (no. 55) 451, stating 'where the policies of nations are not perceived by the governments as being identical, efforts to harmonize or unify the municipal legal rules have been less successful'.

international institutions dealing with the harmonization of law such as UNCITRAL and UNIDROIT.[102] While the International Law Commission has produced instruments in many areas of public international law, it does not seem well-suited to dealing with a fast-moving and politically-charged area like data protection. Institutions such as the Council of Europe may be too closely tied to one region to produce an instrument of truly global application, while the OECD has limited membership that currently consists of thirty developed States. Other international organizations such as the ITU, UNESCO, or the WTO seem too specialized to take up the task of drafting an international data protection instrument. Thus, either a new group would have to be created, or the mandate of an existing international organization would have to be expanded to encompass data protection and to ensure that it was provided with the necessary expertise.

The scope of the instrument: difficult decisions would also have to be made regarding the scope of the instrument, such as whether it would cover only data protection or also privacy, and whether it should contain exceptions, such as for data processing by law enforcement.

A few conclusions can be drawn based on all these factors:

The need for a global legal approach to data protection will only increase as data processing becomes increasingly global: there is no doubt that the globalization of data processing is increasing at an explosive pace, while for the most part data protection law tends to be national or regional. The tension between the global nature of data processing on the one hand, and the national or regional nature of data protection law on the other hand, will increase the need for a global legal framework for data protection.

It will be difficult to agree on the substance of global data protection standards: while a number of data protection principles are widely accepted, the different cultural and legal conceptions of data protection around the world, together with the lack of any data protection law in most States, will make it difficult to reach broad international agreement on a defined set of standards. The level of strictness of such standards could pose a dilemma: if global standards were set too high, then it is likely that many States would be reluctant to enact them, while if they were set too low, then States and entities with a long tradition of data protection law might oppose them as watering down their existing standards (this could be a particular problem for the European Union). A related question is whether any global standards should override local law: while many States would likely accept global standards only if they applied without prejudice to national requirements, allowing local law to apply on top of any global standards could defeat the goal of providing a reasonable degree of international harmonization. Indeed, the example of the EU Data Protection Directive, which sets forth general principles of data protection law but allows the EU Member States considerable leeway in implementing them into national legislation, demonstrates that allowing national law to take precedence over international standards can result in a lack of harmonization.[103] To provide real added value, global data protection standards should thus produce true harmonization, and not just act as an extra layer of regulation to apply in addition to existing law.

The time does not yet seem ripe for a binding international legal instrument on data protection: the difficulty of selecting the standards that should serve as the basis for a binding legal instrument, of agreeing on its scope, and of selecting an appropriate international organization to coordinate the work, indicates that the drafting of such an instrument is unlikely to be possible within a reasonable time period, and to a useful degree of specificity. Data protection was developed as a discrete legal area only in the 1970s, and the lack of extensive State practice argues against its suitability as the subject of a multilateral convention at the present time. It could be easier to agree on a convention covering particular aspects of data protection, such as providing an interface between the different national and regional approaches, in order (for example) to facilitate international data transfers, or to allow for mutual recognition of different regional data protection approaches. Of course, even agreeing on such a limited convention could be difficult without general agreement on detailed data protection standards that would be needed to underlie such an interface between different systems.

Other mechanisms besides a convention could lead to a harmonization of data protection law: while an international convention on data protection may be premature, other actions could lead to a gradual harmonization of the law. For example, an international body could draft a model data protection law, which could then be the basis for more States to enact data protection legislation, thus leading to greater international consensus on the substance of data protection standards. In addition, regional groups dealing with data protection such as APEC, the European Union, and others could continue their existing dialogue, and business groups could produce harmonized tools for data protection compliance to be used on a global basis. Widespread adoption of technical standards for data protection could also gradually lead to increased legal convergence.

None of these steps would rule out discussions on a global legal instrument for data protection, and such discussions have indeed been started by a group chaired by the Spanish Data Protection Authority that began working on global standards in early 2009, and which includes participation by data protection authorities, academics, private-sector representatives, and non-governmental organizations from around

[102] However, on occasions UNIDROIT for one has also dealt with public law issues. See the UNIDROIT web site, <http://www.unidroit.org/dynasite.cfm?dsmid=84219>, stating that 'Unidroit's basic statutory objective is to prepare modern and where appropriate harmonised uniform rules of private law understood in a broad sense. However, experience has demonstrated the necessity of permitting occasional incursions into public law, especially in areas of law where hard and fast lines of demarcation are difficult to draw or where transactional law and regulatory law are intertwined'.

[103] See European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final 12; Christopher Kuner, European data protection law: corporate compliance and regulation (2nd ed. Oxford University Press 2007) 57–61.

the world.[104] The Spanish effort is a useful way to explore the commonalities and differences between the various approaches to data protection, and can make a positive contribution to the eventual development of global standards. However, at this stage the primary value of such efforts is to facilitate discussion between representatives of the various approaches to data protection, without expecting that an international convention could be adopted any time soon.

This multi-faceted approach is in keeping with modern thinking regarding the harmonization of laws, which stresses the need to consider other, more flexible approaches besides the drafting of international conventions.[105] Data protection is deserving of further legal protection on a global scale, the need for which will continue to increase as both governments and private-sector entities seek to process an increasing amount of personal data. The time for a global approach to data protection has definitely come, but efforts at global legal harmonization must be flexible enough to encompass approaches beyond traditional instruments like international conventions. In the interregnum between a purely national or regional view of data protection and a legally binding international data protection framework, it will be necessary to make use of other mechanisms to achieve greater international harmonization of data protection law.

Acknowledgements

This article is written in the author's personal capacity. The author is indebted to the following persons for their valuable comments on previous drafts: Cédric Burton; Prof. Lee Bygrave; Prof. Fred Cate; John Kropf; and Kenneth Propp.

Christopher Kuner *(ckuner@hunton.com) Partner, Hunton & Williams, Brussels; Chairman, Task Force on Privacy and the Protection of Personal Data of the International Chamber of Commerce (ICC). The author also participates on behalf of the ICC in the UNCITRAL Working Group on Electronic Commerce.*

[104] See Agencia Española de Protección de Datos, Draft Joint Proposal for International Standards for the Protection of Privacy and Personal Data (unpublished draft, January 2009; updated drafts dated 24 February and 24 April 2009).

[105] See the UNIDROIT web site, <http://www.unidroit.org/dynasite.cfm?dsmid=84219>, which states regarding international conventions for legal harmonization: '[T]he low priority which tends to be accorded by Governments to the implementation of such Conventions and the time it therefore tends to take for them to enter into force have led to the increasing popularity of alternative forms of unification in areas where a binding instrument is not felt to be essential'.