Groningen Journal of International Law, vol 2(2): Privacy in International Law

The European Union and the Search for an International Data Protection Framework

Christopher Kuner*

DOI: 10.21827/5a86a82b67dab

Keywords
PRIVACY; DATA PROTECTION; EUROPEAN UNION; INTERNATIONAL LAW; INTERNET

Abstract
The European Union (EU) has supported the growing calls for the creation of an international legal framework to safeguard data protection rights. At the same time, it has worked to spread its data protection law to other regions, and recent judgments of the Court of Justice of the European Union (CJEU) have reaffirmed the autonomous nature of EU law and the primacy of EU fundamental rights law. The tension between initiatives to create a global data protection framework and the assertion of EU data protection law raises questions about how the EU can best promote data protection on a global level, and about the EU's responsibilities to third countries that have adopted its system of data protection.

I. Introduction

In 2009, the author considered the opportunities and difficulties of creating an international legal framework for data protection and privacy.[1] Since then, the globalization of data processing and the Snowden revelations that came to light in the summer of 2013[2] have led to an increased interest in regulating data protection at the international level. It is thus time to revisit some of the points discussed earlier, focusing in particular on EU law as the most influential body of data protection law worldwide.

The trans-border nature of data processing on the Internet has led to increased interest in the possibility of regulating data protection on an international level. Individuals, whose data are routinely transferred around the world via the Internet, often do not know to whom to turn to protect their rights. Companies are frustrated by the lack of harmonisation and the fact that they are often subject to conflicts between data protection

* Director, Brussels Privacy Hub, Vrije Universiteit Brussel (VUB); Associate Professor of Law, University of Copenhagen; Senior Privacy Counsel, Wilson Sonsini Goodrich & Rosati, Brussels; Honorary Fellow, Centre for European Legal Studies, University of Cambridge. This article is written in the author's personal capacity, and is current as of July 2014. The author is grateful to Hielke Hijmans for his valuable comments on an earlier draft.

1 Kuner, C., "An international legal framework for data protection: issues and prospects", *Computer Law & Security Review*, vol. 25, 2009, 307–317. Strictly speaking, data protection law, which restricts the processing of data relating to an identified or identifiable person, and grants persons rights in the processing of data relating to them, is closely related to, but distinct from, the concept of "privacy". See Kokott, J. and Sobotta, C., "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, vol. 3, ed. 4, 2013, 222–228. However, the two terms will be used synonymously here for the sake of convenience, unless otherwise noted.

2 See regarding the Snowden revelations Greenwald, G., *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, MacMillan, New York, 2014.

law and other legal obligations.[3] And data protection authorities (DPAs), many of whom lack sufficient resources to carry out their tasks, often have to deal with complex questions involving data processing that takes place in other regions.

Existing instruments dealing with the international regulation of data protection all have various shortcomings. International human rights instruments protect the processing of personal data,[4] but they are typically not detailed enough to provide individuals with a direct remedy in individual cases. In 1990 the UN adopted guidelines concerning computerised personal data files, which have had little practical impact.[5] The UN General Assembly passed a resolution on 18 December 2013 that affirms the online application of the right to privacy,[6] and the UN Human Rights Commission is working to promote the right to privacy in the digital age,[7] but these initiatives are by themselves unlikely to lead to a complete solution.

There have been growing calls for a stronger international legal framework for 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'.[8] Since then, further instances of the International Conference have adopted similar resolutions.[9] Some companies have also made such appeals; for example, in 2007, Google called for the creation of "global privacy standards".[10] Civil society groups have also called for global standards.[11]

EU institutions and Member States have been particularly active in promoting global data protection standards. Thus, the Article 29 Working Party (the group of DPAs from the EU Member States) has stated that 'global standards regarding data protection are

---

[3] For example, with regard to conflicts between data protection law and civil litigation rules in the US. See, e.g., Article 29 Working Party, "Working Document 1/2009 on pre-trial discovery for cross border civil litigation" (WP 158, 11 February 2009).

[4] Universal Declaration of Human Rights (UDHR), 1948, Article 12; ICCPR International Covenant of Civil and Political Rights (ICCPR), 1966, Article 17. See GA Resolution 68/167 (68th session) A/RES/68/167, 18 December 2013.

[5] UN Guidelines concerning Computerized Personal Data Files, E/CN.4/1990/72, 14 December 1990. See Bygrave, L., *Data Privacy Law: An International Perspective*, Oxford University Press, Oxford, 2014, 2272 (Kindle edition), stating that the UN Guidelines "have had a lower public profile and practical impact than the majority of the other main international instruments...".

[6] GA Resolution 68/167 (68th session) A/RES/68/167, 18 December 2013.

[7] United Nations, Office of the High Commissioner of Human Rights, *The Right to Privacy in the Digital Age*, at <ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx> (accessed 30 June 2014).

[8] Privacy Conference, 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*, 14–16 September 2005, available online at <privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf> (accessed 20 June 2014).

[9] See, e.g., Privacy Conference, 35th International Conference of Data Protection and Privacy Commissioners, *Resolution on Anchoring Data Protection and the Protection of Privacy in International Law*, 23–26 September 2013, available online at <privacyconference2013.org/web/pageFiles/kcfinder/files/5.%20International%20law%20resolution%20EN%281%29.pdf> (accessed 20 June 2014).

[10] Google Public Policy Blog, Peter Fleischer, *Call for Global Privacy Standards,* available online at <googlepublicpolicy.blogspot.com/2007/09/call-for-global-privacy-standards.html> (accessed 20 June 2014).

[11] The Public Voice, *The Madrid Privacy Declaration, Global Privacy Standards for a Global World*, 3 November 2009, available online at <thepublicvoice.org/madrid-declaration/> (accessed 20 June 2014).

becoming indispensable',[12] and that it supports 'the development of a global instrument providing for enforceable, high level privacy and data protection principles.'[13] In 2009 a group under the leadership of the Spanish DPA published "The Madrid Resolution", which is a set of international standards for data protection and privacy.[14] And a number of EU Member States (Austria, France, Germany, Ireland, Luxembourg, Slovenia, and Spain) were among those proposing the UN General Assembly resolution that was passed in December 2013.[15]

At the same time, EU institutions have worked to promote the adoption of EU data protection law as a global standard. For example, the Vice-President of the European Commission Viviane Reding has stated that 'Europe must act decisively to establish a robust data protection framework that can be the gold standard for the world'.[16] And an unnamed EU official has been quoted as saying 'with these proposals, the EU is becoming the de facto world regulator on data protection'.[17]

The principle that the EU legal system constitutes an independent, autonomous source of law has been recognized since the 1960s.[18] The Court of Justice of the European Union (CJEU) has recently proclaimed its autonomous nature and the primacy of EU fundamental rights law in the context of the Treaty of Lisbon, which entered into force on 1 December 2009.[19] As will be discussed below, the Court's recent judgments have also reaffirmed the application of European data protection law to data processing carried out in other regions.

Thus, while EU institutions have called for the development of international data protection standards, they have also emphasized the autonomous nature of EU law and have sought to advance the adoption of EU data protection law around the globe. The EU's involvement in both these phenomena illustrates the tensions inherent in simultaneous developing global values and asserting regional ones, and raises the question of how the EU can best advance the spread of data protection rights around the world. These activities also illustrate how the EU's global influence should be coupled with a global responsibility towards other States that adopt its standards.

---

[12] Article 29 Working Party, "The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data" (WP 168, 1 December 2009), 10.

[13] Article 29 Working Party, "Opinion 04/2014 on surveillance for electronic communications for intelligence and national security purposes" (WP 215, 10 April 2014), 3.

[14] Privacy Conference, International Conference of Data Protection and Privacy Commissioners, *The Madrid Resolution, International Standards on the Protection of Personal Data and Privacy*, 5 November 2009, available online at <privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf> (accessed 22 September 2014).

[15] GA Resolution 68/167 (68th session) A/RES/68/167, 18 December 2013.

[16] Viviane Reding, "A data protection compact for Europe", 28 January 2014, available online at <europa.eu/rapid/press-release_SPEECH-14-62_en.htm> (accessed 22 June 2014).

[17] European Voice, Vogel, T., *Reding seeks overhaul of data protection rules*, 15 December 2011, available online at <europeanvoice.com/article/reding-seeks-overhaul-of-data-protection-rules/> (accessed 4 July 2014).

[18] E.g. European Court of Justice, 5 February 1963, *Van Gend en Loos,* C-16/62, ECR 1963 p. 1; European Court of Justice, 15 July 1964, *Costa v ENEL*, C- 6/64 , ECR 1964 p. 585 . See also van Rossem, J. W., "The Autonomy of EU Law: More is Less?", *in*: Wessel, R. A. and Blockmans, S., *The EU Legal Order under the Influence of International Organisations*, TMC Asser Press, The Hague, 2013, 13.

[19] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 17 December 2007, 2007/C 306/01.

II. Prospects for an international legal framework

II.1. Varieties of international initiatives

The variety of data protection guidelines, conventions, and other instruments that have been enacted at an international level complicate the prospects of reaching agreement on a single international framework. The differences between them can be can be classified in various ways, such as the following:

Legally binding/non binding: Some of these instruments have binding legal effect. Thus, the EU Data Protection Directive 95/46[20] obligates the EU Member States to implement its provisions (i.e. to reflect them in their national law), and individuals may rely on the Directive to assert their rights.[21] The Council of Europe Convention 108[22] legally obligates States that are parties to it to enact its protections into their domestic law, but cannot be relied on by individuals to create legal rights.[23] The OECD Privacy Guidelines,[24] the APEC Privacy Framework,[25] the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection,[26] and the UN General Assembly Resolution of 18 December 2013 affirming application of the right to privacy to online activities[27] are not legally binding.

International/regional: Some initiatives have been enacted at the regional level and others at the international level. International human rights treaties and instruments adopted by UN bodies are obviously applicable on a global scale. The APEC Privacy Framework is applicable to the twenty-one member countries of the Asia-Pacific Economic Cooperation group, and is thus an example of a regional instrument. The Council of Europe Convention 108 is difficult to categorize, since it was initially enacted

---

[20] 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, available online at <europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm> (accessed 22 September 2014).

[21] See, e.g., European Court of Justice, 24 November 2011, *ASNEF and FECEMD v. Administración del Estado*, Joined Cases C-468/10 and C-469/10 [2011] ECR I-0000; European Court of Justice, 20 May 2003, *Rechnungshof*, Joined Cases C-465/00 and C-138/01 [2003] ECR I-4989.

[22] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, available online at <conventions.coe.int/Treaty/en/Treaties/Html/108.htm> (accessed 22 September 2014).

[23] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, Explanatory Report, para. 38.

[24] The Organisation for Economic Co-operation and Development, *OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data*, 11 July 2013, available online at <oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf> (accessed 22 September 2014).

[25] Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, 2005, available online at <apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx> (accessed 20 June 2014).

[26] The Economic Community of West African States, *Supplementary Act on Personal Data Protection*, 16 February 2010, available online at <statewatch.org/news/2013/mar/ecowas-dp-act.pdf> (accessed 20 June 2010).

[27] GA Resolution, *supra* nt. 15. See regarding the background of the Resolution Social Science Research Network, Milanović, M., *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 31 March 2014, available online at <papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485> (accessed 29 June 2014).

on a regional (i.e. European) scale and is closely entwined with EU law,[28] but is now open for enactment by States in other regions.[29]

Institutional/ad hoc: Some initiatives that have been established within the framework of an existing institution, while others were drafted on an ad hoc basis. For example, the Council of Europe Convention 108 is administered and promulgated by the Council of Europe, and is interpreted by the European Court of Human Rights. An example of an ad hoc initiative is the Madrid Resolution, which is a declaration drafted under the leadership of the Spanish DPA with the participation of other DPAs, private sector entities, NGOs, and other organizations from around the world.

II.2. Continuing challenges

The challenges for realizing a stronger legal framework at the international level remain much as described in 2009.[30] Despite the growing international recognition of data protection and interest in the possibility of having the Council of Europe Convention 108 serve as the basis for an international data protection standard,[31] considerable differences still exist in the approaches to data protection around the world,[32] owing to cultural, historical, and legal factors, and there is a lack of consensus as it can best be strengthened on an international scale. Thus, there is no agreement as to whether the global framework for data protection should be legally binding or not; whether existing instruments can be used, or a new one is needed; what the substance of any data protection standards should be, and their scope; and what institution should coordinate the work. Indeed, in many cases it is not even clear what the calls by different stakeholders for "global standards" or an "international framework" for data protection mean in concrete terms.

This means that reaching agreement on the substance of an international framework will not be easy. There are two issues of particular importance. First of all, it would be necessary to agree on the level at which such standards should be enacted: if they are too abstract, they may not be able to protect personal data in practice, while any standards that are too detailed may be difficult to implement locally, given the differences in legal cultures around the world. Thus far, most international initiatives concerning data

---

[28] See Consolidated version of the Treaty on European Union (TEU), 9 May 2008, 2008/C 115/01, Article 6, indicating that the European Convention on Human Rights (on which the Convention 108 is based) is recognized by EU law and *de facto* incorporated into it.

[29] So far one non-member of the Council of Europe, namely Uruguay, has enacted the Convention. See Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Treaty open for signature by the member States and for accession by non-member States*, available online at <conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG> (accessed 30 June 2014). The Convention is also in force in non-EU States such as Azerbaijan, Georgia, Russia, and the Ukraine.

[30] See Kuner, *supra* nt. 1, 315–317.

[31] See, e.g., Council of Europe, Polakiewicz, J., *Convention 108 as a Global Privacy Standard?*, 17 June 2011, available online at <coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/Convention_108as_a_global_privacy_standards_June_2011.pdf> (accessed 30 June 2014); Social Science Research Network, Greenleaf, G., '*Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?*, 8 May 2013, available online at <papers.ssrn.com/sol3/papers.cfm?abstract_id=2262296> (accessed 30 June 2014).

[32] See Bygrave, *supra* nt. 5, location 6168 (Kindle edition).

protection set the agenda and formulate broad principles, but do not specify how they are to be implemented in detail.[33]

Second, there is no consensus as to which international organization could coordinate the work. Indeed, in the author's experience most international organisations are wary of beginning work on a legally binding data protection instrument because of the political difficulties of reaching agreement, and would hesitate to do so failing a clear mandate from their members. While the UN has the necessary global membership, the work of legal harmonisation bodies such as the United Nations Commission on International Trade Law (UNCITRAL) demonstrates that in the highly politicised atmosphere of the UN, harmonisation even of technical topics tends to proceed slowly and with difficulty.[34] The UN also lacks detailed expertise in the field of data protection.

Thus, the possibility of a global, legally binding data protection instrument being enacted in the foreseeable future remains elusive.

III. EU data protection law in a global context

III.1. Legislative and regulatory activity

EU data protection law has been influential in a global context in two ways: first, by serving as a model for the enactment of data protection law in other regions, and second, by its extraterritorial application to data processing in third countries.

The EU Data Protection Directive has had a substantial influence on the enactment of data protection law in other States,[35] and in particular has influenced States without their own tradition of data protection to enact laws based on the EU model.[36] EU external action policy seeks to promote adoption of EU data protection law in third countries as an aspect of furthering the rule of law, including financing technical assistance projects that allow data protection experts from the EU to work with third countries.[37] More developed States have also been influenced to enact new data protection laws, or update their existing ones, based on EU law.[38] It seems that the EU expects its proposed General Data Protection Regulation[39] to have similar influence.[40]

---

[33] De Hert, P. and Papakonstantinou, V., "Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?", *I/S: A Journal of Law and Policy for the Information Society*, vol. 9, ed. 2, 2013, 271–324, 275.

[34] Based on the author's experience as a longstanding member of the UNCITRAL Working Group on Electronic Commerce and participation in its work on topics such as electronic signatures.

[35] De Hert and Papakonstantinou, *supra* nt. 33, 287–288.

[36] See, e.g., Bygrave, *supra* nt. 5, location 6125 (Kindle edition), stating 'the overwhelming bulk of countries that have enacted data privacy laws have followed, to a considerable degree, the EU model…'; Greenleaf, G., "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108", *International Data Privacy Law*, vol. 2, no. 2, 2012, 68–92.

[37] See Pech, L., "Rule of law as a guiding principle of the European Union's external action", Centre for the Law of EU External Relations (CLEER), T.M.C. Asser Instituut, available online at <asser.nl/upload/documents/2102012_33322cleer2012-3web.pdf> (accessed 4 July 2014), 17–20. For an example of such assistance given in 2011 by the EU focused on 'ensuring the data protection accreditation of Mauritius with the European Union', see <eeas.europa.eu/delegations/mauritius/eu_mauritius/development_cooperation/technical_cooperation/index_en.htm> (accessed 4 July 2014).

[38] See, e.g., New Zealand Privacy Commissioner, "Privacy amendment important for trade and consumer protection", 26 August 2010, available online at <privacy.org.nz/news-and-publications/statements-media-releases/updated-media-release-30-8-10-privacy-amendment-important-for-trade-and-consumer-

EU data protection law can apply extraterritorially to personal data processed in other regions,[41] which expands its influence beyond the geographic borders of the EU. For example, standard contractual clauses for data transfer approved by the European Commission obligate data importers outside the EU to agree to audits at the request of data exporters and, 'where applicable, in agreement with the Supervisory Authority' (for example, the DPA of the EU Member State with jurisdiction over the transfer), as well to submit itself to the authority of the DPA and the EU court with jurisdiction over it.[42]

The applicable law regime of the proposed Regulation would be even more expansive than at present. Under the EU Data Protection Directive, EU law applies extraterritorially primarily in situations when a non-EU data controller uses 'equipment' situated in the EU to process personal data,[43] whereas under the Regulation it would apply in cases where non-EU controllers offer goods or services to individuals in the EU or monitor their behaviour.[44] By doing away with the requirement that equipment situated in the EU be used in order for EU law to apply, the new applicable law regime of the Regulation 'seems likely to bring all providers of Internet services such as websites, social networking services and app providers under the scope of the EU Regulation as soon as they interact with data subjects residing in the European Union'.[45]

Since 2009, the EU legal framework for data protection has also been reinforced by the Treaty of Lisbon. The Lisbon framework creates stronger protection for data protection as a fundamental right, by including a new provision in the Treaty on the Functioning of the European Union (TFEU) that explicitly grants individuals a right to data protection,[46] and by granting full legal effect to the Charter of Fundamental Rights of the European Union.[47]

---

protection/> (accessed 4 July 2014), regarding the influence of EU law on the reform of the New Zealand Privacy Act.

39 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, 25 January 2012.

40 See the speech by European Commission Vice-President Viviane Reding, *supra* nt. 16.

41 See, e.g., Kuner, C., "Data protection law and international jurisdiction on the Internet (Part 2)", *International Journal of Law and Information Technology*, vol. 18, no. 3, 2010, 227–247, 228–234; Svantesson, D. J. B., *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, Copenhagen, 2013, 89–111.

42 See Commission Decision (EC) 2001/497 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive (EC) 95/46 [2001] OJ L181/19, Clauses 5(d) and 7(1); Commission Decision (EC) 2001/16 of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46 [2002] OJ L6/52, Clauses 5(f) and 7(1).

43 Directive, Article 4(1)(c).

44 General Data Protection Regulation, *supra* nt. 39, Article 3(2).

45 Svantesson, *supra* nt. 41, 107. See Article 3(2) of the Proposed Regulation.

46 Consolidated version of the Treaty on the Functioning of the European Union (TFEU), [2010] OJ C83/47, Article 16(1). See regarding the strengthened position of data protection as a fundamental right under the Lisbon framework Hijmans, H. and Scirocco, A., "Shortcomings in EU data protection in the third and second pillars. Can the Lisbon Treaty be expected to help?", *Common Market Law Review*, vol. 46, 2009, 1485–1525.

47 Consolidated version of the Treaty on European Union (TEU), *supra* nt. 28, Article 6. See Charter of Fundamental Rights of the European Union, [2010] OJ C83/2, Article 8, which also grants a right to data protection.

III.2. CJEU judgments

The CJEU's first case dealing with the global application of EU data protection law was the *Lindqvist* judgment of 2003,[48] in which 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 hosted within the EU. The Court's decision was based in part on the fact that finding that a data transfer occurred in this case would effectively make the entire Internet subject to EU data protection law.[49] In this early judgment, the CJEU thus took into account the impact of extending the territorial scope of EU data protection law to the global Internet.

A judgment from outside the field of data protection is of crucial importance for understanding the legal status given to fundamental rights in the EU legal system. In its first *Kadi* judgment,[50] which was issued on 3 September 2008 just before the Lisbon framework came into effect, the CJEU annulled the EU implementation of a UN Security Council resolution that had resulted in the claimant's assets being frozen, finding that it violated his fundamental rights.[51] In particular, the Court noted that even if obligations imposed by the UN Charter were classified as part of the hierarchy of EU legal norms, they would still rank lower than general principles of EU law, including fundamental rights.[52] The Court also re-affirmed the autonomy of the EU legal order,[53] and found that EU implementation of a Security Council resolution is a matter for the 'internal and autonomous legal order of the Community'.[54] The *Kadi* judgment thus affirmed both the position of fundamental rights in the EU legal order, and its autonomous and inward-looking nature.[55]

The influence of the Lisbon framework was demonstrated in the Court's decision in *Digital Rights Ireland*[56] from April 2014, in which it invalidated the EU Data Retention Directive.[57] The decision was based on fundamental rights law and the application of data protection law outside the EU was not directly at issue. However, the Court stated as follows towards the end of the judgment (paragraph 68)

---

48 Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.

49 *Id.*, para. 69.

50 Joined Cases C-402 & 415/05P, *Kadi & Al Barakaat Int'l Found. v. Council & Commission*, [2008] ECR 1-6351. The case has resulted in further litigation; see Joined Cases C-584/10 P, C-593/10 P and C-595/10 P Kadi, 18 July 2013. There have also been other cases involving challenges to the implementation of UN sanctions brought under fundamental rights law before both the CJEU and the European Court of Human Rights. See de Búrca, G., "The European Court of Justice and the International Legal Order after Kadi", *Harvard International Law Journal*, vol. 51, 2010, 1-49; Ziegler, K., "Strengthening the Rule of Law, but Fragmenting International Law: the *Kadi* Decision of the ECJ from the Perspective of Human Rights", *Human Rights Law Review*, vol. 9, 2009, 288–305.

51 *Kadi*, para. 351.

52 *Id.*, paras. 305–309.

53 *Id.*, para. 316.

54 *Id.*, para. 317.

55 See regarding the inward-looking nature of the Court's judgment de Búrca, *supra* nt. 50, 41, stating 'the judicial strategy adopted by the ECJ in *Kadi* was an inward-looking one which eschewed engagement in the kind of international dialogue that has generally been presented as one of the EU's strengths as a global actor'.

56 C-293/12 and C-594/12, 8 April 2014.

57 Directive (EC) 2006/24 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 (EC) 2002/58, [2006] OJ L105/54.

> [I]t should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data…[58]

The criticism in this passage of the Data Retention Directive for failing to require that data be stored in the EU, and the statement that storage outside the EU removes the possibility of supervision by an EU DPA, seems to logically imply that oversight of data processing by the DPAs may also be required with regard to EU data that are transferred to other regions. This conclusion raises a number of questions that the Court did not explore further (e.g., how such extraterritorial supervision could be reconciled with the fact that the enforcement jurisdiction of the DPAs ends at the borders of their respective EU Member States[59]).

The extraterritorial application of EU data protection law was re-affirmed more strongly in *Google Spain v. AEPD and Mario Costeja Gonzalez*[60] from May 2014. One of the issues in this case was whether EU data protection law could apply when a company (in this case Google) has an establishment in an EU Member State that promotes a search engine that orients its activity towards the inhabitants of that State, even though the actual data processing is carried out by the establishment's parent company located outside the EU. In finding that EU data protection law did apply in such a case, the Court noted that the Directive should be interpreted to have 'a particularly broad territorial scope'.[61] The Court also held that the right to delete data under the EU Data Protection Directive applies to the results of Internet search engines (popularly referred to as the 'right to be forgotten').[62]

The influence of *Kadi* can be seen in the self-referential style of the *Google Spain* judgment, in which the Court does not even mention the European Convention on Human Rights, the jurisprudence of the European Court of Human Rights, or any international human rights instruments. By contrast, in his opinion Advocate-General Jääskinen had recognised the implications of the case for the global Internet,[63] an approach that the Court did not refer to and thus impliedly rejected. This is also demonstrated by the fact that the Court favoured data protection rights over the rights of

---

58 Digital Rights Ireland, para. 68.

59 See EU Data Protection Directive, Article 28.

60 Case C-131/12 (13 May 2014).

61 *Id.*, para. 54.

62 *Id.*, paras. 89–99.

63 See Opinion of Advocate General Jääskinen, Case C-131/12, 25 June 2013, paragraph 31, mentioning the need in the case to strike 'a correct, reasonable and proportionate balance between the protection of personal data, the coherent interpretation of the objectives of the information society and legitimate interests of economic operators and Internet users at large'. See also regarding the implications of the case for the Internet, Ausloos, J., "European Court Rules against Google, in Favour of Right to be Forgotten", 13 May 2014, available online at <blogs.lse.ac.uk/mediapolicyproject/2014/05/13/european-court-rules-against-google-in-favour-of-right-to-be-forgotten/> (accessed 1 July 2014); Jerker B. Svantesson, D., "Google court ruling creates a more forgetful Internet", 14 May 2014, available online at <theconversation.com/google-court-ruling-creates-a-more-forgetful-internet-26696> (accessed 1 July 2014).

Internet users,[64] and did not refer to the right to transfer data 'regardless of frontiers' that is protected both by international human rights law[65] and the EU Charter of Fundamental Rights.[66] *Google Spain* thus seems to mark a new era in which the CJEU applies to data processing on the Internet the pronouncements made in the *Kadi* judgment on the autonomy and primacy of EU data protection rights.

An upcoming decision by the CJEU may develop the themes dealt with in *Digital Rights Ireland* and *Google Spain* even further. On 18 June 2014 the Irish High Court stated that it would refer a question to the CJEU in the case *Schrems v. Data Protection Commissioner*,[67] which involves a challenge by an Austrian student to the transfer of personal data to the US by Facebook under the EU-US Safe Harbor scheme. While the exact wording of the question(s) to be referred to the CJEU had not yet been published when this article was finalised, it seems that they will involve whether the European Commission's adequacy decision of 2000 creating the Safe Harbor should be re-evaluated in light of widespread access to data by US law enforcement, and whether the DPAs should be allowed to determine whether the Safe Harbor provides adequate protection.[68] The High Court in the *Schrems* case criticised the Safe Harbor and data access by law enforcement in the US as failing to provide oversight 'carried out on European soil',[69] which seems inspired by paragraph 68 of the *Digital Rights Ireland* judgment.

III.3. Data protection standards and applicable law

The extraterritorial application of data protection law currently fulfil much the same function as would an international legal framework, i.e., it extends legal protection to the processing of the personal data regardless of their location. This can be seen in the case of EU data protection law, which often applies to data processing outside the EU, and which also includes restrictions on transborder data flows that require data processing in third countries to be conducted under EU data protection standards.[70]

An effective global legal framework for data protection thus requires clarity about rules of applicable law. In the author's experience, bodies drafting transnational data protection rules are reluctant to deal with the topic of applicable law because of its complexity and the fear of unintended consequences,[71] and thus far, the EU Data Protection Directive is the only international data protection instrument to contain rules on applicable law.[72] There is thus no accepted international framework for applicable law rules as they relate to data protection.

---

64 See Google Spain, paragraph 81, stating that the data subject's rights protected by Articles 7 and 8 of the Charter of Fundamental Rights 'override, as a general rule, that interest of internet users …'.

65 UDHR, UN GA Res 217 A(III), Article 19; ICCPR, 999 UNTS 171, 1966, Article 19(2).

66 See Article 11 of the Charter, which states: 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.

67 2013 No. 765JR, 18 June 2014.

68 *Id.*, paras. 71 and 84.

69 *Id.*, para. 62.

70 See Kuner, C., *Transborder Data Flows and Data Privacy Law*, Oxford, Oxford University Press, 2013, 125–129.

71 With regard to the failure of the Council of Europe Convention 108 to include clear rules on applicable law, see Bygrave, *supra* nt. 5, locations 2057–2058 (Kindle edition).

72 I*d.*, location 2428 (Kindle edition).

III.4. The increasing insularity of EU law

The recent judgments of the CJEU cited above (in particular *Kadi* and *Google Spain*) reflect an increasing concern for the autonomy of EU law and a self-referential style that carry the risk of a growing insularity.

This is also reflected in the lack of options in EU data protection law for granting legal recognition to non-EU data protection standards. The Directive recognises non-EU standards only in line with a formal adequacy determination by the European Commission, as described above. The Regulation proposed in 2012 fails to include a provision explicitly requiring the Commission to take into account the enactment by third countries of regional and international instruments (for example, Council of Europe Convention 108) when assessing the adequacy of protection.

The increasing insularity of EU data protection law can also be seen in the involvement of the EU in international policymaking bodies like the Council of Europe and the OECD. Over the last few years, it seems that the EU's priority in participating in the work of such organisations is to emphasise the need to finalise enactment of the proposed Regulation, rather than to further the adoption of a global legal framework for data protection.[73]

The recent judgments of the CJEU also demonstrate the tension between the promotion of EU data protection law and the furtherance of other important fundamental rights on a global basis. The Internet enables communication and the dissemination of information across borders, which brings great cultural, economic, and social benefits to individuals in the EU. If access to Internet services becomes fragmented along regional or national lines, then these benefits will be diminished. The judgment in *Google Spain* may cause Internet search results to be presented to individuals in the EU in a different way than they are in other regions.[74] In fact, the judgment has already led to controversy concerning the effect of deleting links to news stories on a regional basis.[75] The Snowden revelations are also strengthening the interest in initiatives such as a "Schengen for data" that would provide incentives to store the data of European companies on servers located within the EU.[76]

---

[73] Based on the author's experience as an observer for the International Chamber of Commerce (ICC) in the data protection work of the Council of Europe, and as a consultant for the OECD.

[74] See Ahmed, M., "Google in fight to stop global removal of sensitive links", *Financial Times*, 23 July 2014, available online at <ft.com/intl/cms/s/0/f3dfc9e4-127b-11e4-93a5-00144feabdc0.html?siteedition=intl#axzz38KKenC25> (accessed 23 July 2014), indicating that the DPAs have been pressing Google to interpret the *Google v. Spain* decision as requiring that links expunged from Google's European search engines should also be removed from its website google.com.

[75] Ball, J., "EU's right to be forgotten: Guardian articles have been hidden by Google", 2 July 2014, available online at <theguardian.com/commentisfree/2014/jul/02/eu-right-to-be-forgotten-guardian-google> (accessed 8 July 2014). See also Article 29 Working Party, "European DPAs meet with search engines on the 'right to be forgotten'", 25 July 2014, available online at <ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140725_wp29_press_release_right_to_be_forgotten.pdf> (accessed 27 July 2014).

[76] See "Atos CEO calls for 'Schengen for data'", available online at <thierry-breton.com/lire-lactualite-media-41/items/atos-ceo-calls-for-schengen-for-data.html> (accessed 6 July 2014); "Ein Internet nur für Deutschland", *Frankfurter Allgemeine Zeitung*, 10 November 2013, available online at <faz.net/aktuell/wirtschaft/netzwirtschaft/plaene-der-telekom-ein-internet-nur-fuer-deutschland-12657090.html> (accessed 6 July 2014).

IV. Conclusions

IV.1. The pluralist nature of global data protection policymaking

The EU's activities on the international stage have been marked by tension between efforts to strengthen the international legal framework for data protection on the one hand, and the increased emphasis given to the fundamental right of data protection under EU law and the autonomous nature of EU law on the other hand. These latter points were also strengthened by the *Kadi* judgment, where the CJEU's reasoning emphasised 'the separateness and autonomy of the EC from other legal systems and from the international legal order more generally, and the priority to be given to the EC's own fundamental rules'.[77]

This tension reflects the pluralist nature of the international legal order.[78] In a pluralist view, the presence of various conflicting norms is a normal situation when there is a lack of a hierarchical legal structure that can provide an overall, authoritative governance framework.[79] The EU's apparent decision that the best way to develop data protection at a global level is to promote and apply its own data protection law extraterritorially could have either positive or negative consequences for the further global recognition of data protection rights, depending on the direction which global developments take

> [I]f each instrument takes positive steps to converge with the others, creating in essence a single international regulatory framework, international governance of data privacy would benefit from an unexpected gift. However, if on the contrary, each model decided to further its own purposes and follow its own path, one more obstacle to the creation of a single regulatory framework would be erected by the release of yet another generation of diverging approaches.[80]

The same impediments to the adoption of an international legal framework that existed in 2009 still exist today, namely the lack of an international organisation to oversee the work; cultural and legal differences between various systems of data protection law; and uncertainty about how such standards could be implemented at the national level.[81] However, even if 'the short-term chances of extensive harmonization are slim',[82] this should not impede work towards greater harmonisation and interface between systems, and dialogue concerning the conflicting attitudes towards data protection may serve as the basis upon which a global framework can gradually be constructed. All this is consistent with a pluralist view of data protection at a global level.

At present, the Council of Europe Convention 108 presents perhaps the best treaty-based possibility for the adoption of an international data protection framework.

---

77 de Búrca, *supra* nt. 50, 23.

78 Regarding pluralism as a normal feature of the international legal order, see UN International Law Commission, "Fragmentation of International Law: Difficulties arising from the Diversification and Expansion of International Law, Report of the Study Group of the International Law Commission finalized by Martti Koskenniemi", UN DOC A/CN.4/L.682, 13 April 2006, available online at <legal.un.org/ilc/documentation/english/a_cn4_l682.pdf> (accessed 3 July 2014), 248.

79 See Krisch, N., "The pluralism of global administrative law", *European Journal of International Law*, vol. 17, ed. 1, 2006, 247–278, 278.

80 De Hert and Papakonstantinou, *supra* nt. 33, 323.

81 Bygrave, *supra* nt. 5, location 6167 (Kindle edition).

82 *Id.*, location 6167–6168 (Kindle edition).

Convention 108 has the advantage that it offers a high level of protection, and is based on existing EU data protection law, which automatically makes it interesting for those States that have adopted the EU approach. At the same time, it requires detailed national implementation, thus being flexible enough to accommodate a variety of national differences. In some respects Convention 108 thus resembles a model law of the type promulgated by international organizations such as UNCITRAL, i.e., it sets forth high-level rules while leaving the details up to local implementation. The advantages (flexibility) and disadvantages (the potential for lack of harmonisation) are also similar to those of a model law. Unfortunately, it seems that the EU (which wields great influence within the Council of Europe) is unwilling to tolerate finalisation of the modernisation process for the Convention 108 until its proposed General Data Protection Regulation is adopted.

It would be useful for the development of global data protection standards if the international community would devote greater efforts to mapping areas of convergence between standards in different legal systems. Greater mutual understanding about the different cultural and legal approaches to data protection around the world would help create the conditions for eventual adoption of an international framework. Academic institutions should also devote greater attention to the area of comparative data privacy law than is now the case.

A good example of such an initiative is the "referential" that has recently been released regarding the use of binding corporate rules (BCRs) in the EU and corporate binding privacy rules (CBPRs) in the APEC countries.[83] The referential is a document matching the legal requirements for BCRs and CBPRs, which are mechanisms recognised under EU data protection law and the APEC Privacy Framework respectively to allow corporate groups to transfer personal data across borders based on their having implemented certain data protection measures within all members of the group. It is intended to serve as a checklist for companies interested in matching the requirements in both systems, and thus can help lead to gradual accommodation between them, without seeking to produce legal harmonisation.

Another initiative aimed at building bridges between different data protection systems is the "Privacy Bridges" project, which is a group of experts from the EU and the US who are drafting 'a framework of practical options that advance strong, globally-accepted privacy values in a manner that produces interoperability and respects the substantive and procedural differences between the two jurisdictions'.[84]

---

[83] Article 29 Working Party, 'Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents', 27 February 2014, available online at <ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf> (accessed 30 September 2014).

[84] MIT Information Policy Project, MIT Information Policy Project and University of Amsterdam Institute for Information Law launch EU-US Privacy Bridges Study Project, 5 May 2014, available online at <ipp.mit.edu/news/mit-information-policy-project-and-university-amsterdam-institute-information-law-launch-eu-us> (accessed 30 September 2014). The author is a member of the project group.

IV.2. Areas for EU action

The following are three areas in which the EU's approach to the international dimension of data protection could be improved:

Considering the impact of EU policymaking on third countries: Many of the third countries that have enacted legislation based on EU data protection law are developing countries with limited resources, and enacting a legal framework for data protection and all it entails (for example, setting up an independent DPA) can be a considerable burden.[85] The fact that the EU promotes the adoption of its data protection law to third countries means that it has a special responsibility towards them. Indeed, the EU's proposed reform would in effect require many third countries that have already enacted EU-based models to make wide-ranging changes to their data protection legislation, and substantial investments in their data protection infrastructure, in order to have a chance of being found adequate by the EU.[86]

The EU is obligated to advance human rights and the rule of law in its relations with third countries,[87] which includes the promotion of data protection standards. It is also obligated to 'promote multilateral solutions to common problems',[88] which should involve more than simply motivating other States to adopt EU data protection law and then leaving them to their own devices. The EU should thus implement measures to consider the effect on third countries of its data protection rules, and to provide a mechanism for them to obtain information about the effects of such changes. Dozens of smaller and less powerful third countries are affected by EU data protection policymaking, but may have no resources to make their voices heard in Brussels. The author has often received questions from third country representatives about EU law-making initiatives in data protection, so interest on their part certainly exists.

It is becoming increasingly recognised that States or international organisations (like the EU) may have an obligation to account for their actions to foreign stakeholders; examples already exist in areas such as world trade law and environmental law.[89] This does not mean that the EU should sacrifice the interests of its own citizens;[90] indeed, doing so would be legally impossible given the autonomous nature of EU and the primacy of fundamental rights in the EU legal order. However, the EU could at least consult with third countries, gather input from them, and provide them with basic information about EU data protection policymaking, without adversely affecting the interests of EU individuals.

---

85 See, e.g., Madhub, D., "The pioneering journey of the Data Protection Commission of Mauritius", *International Data Privacy Law*, vol. 3, ed. 4, 2013, 239–243.

86 See European Parliament legislative resolution of 12 March 2014 on the 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)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading), available online at <europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN> (accessed 30 September 2014), which would cause adequacy decisions issued by the European Commission to expire after five years, unless they have been amended, replaced or repealed by the Commission.

87 See Consolidated version of the Treaty on the Functioning of the European Union (TFEU), *supra* nt. 46, Article 21.

88 *Ibid*.

89 See Benvenisti, E., "Sovereigns as trustees of humanity: on the accountability of states to foreign stakeholders", *American Journal of International Law*, vol. 107, ed. 2, 2013, 295–333, 319–320.

90 *Id.*, 300.

The European Commission proposal for a General Data Protection Regulation foresees a duty of cooperation and information of the Commission and the DPAs with regard to international developments,[91] but this should be made more concrete. For example, a provision could be included in the Regulation requiring the Commission to establish an Internet portal with information on data protection developments with particular relevance to third countries, to hold regular consultations with them, and to establish an advisory board of third country representatives who would give feedback on the impact of EU data protection law in their countries and regions.

Setting jurisdictional boundaries: The *Digital Rights Ireland* judgment demonstrates that the CJEU will apply the fundamental right to data protection broadly in a territorial sense.[92] Furthermore, in the *Google Spain* case the Court affirmed the applicability of EU data protection law to data processing on servers located in a third country, while conspicuously failing to endorse its holding in *Lindqvist* that EU data protection law should not be interpreted to apply to the entire Internet. The *Google Spain* judgment thus undermines the Court's holding in *Lindqvist*.

The EU seems to have decided to further the global protection of personal data by applying its own standards extraterritorially, rather than moving forward with a new set of standards on an international level. However, the territorial extent of data protection rights under EU law needs to be clarified.[93] Limits to the broad territorial scope of EU data protection law must exist, if it is not to become a system of universal application that applies to the entire world. The CJEU should clarify the geographic limits of EU data protection law, and in doing so should take into consideration the points that Advocate-General Jääskinen had mentioned in his opinion in the *Google Spain* case, in particular the objectives of the information society and the legitimate interests of Internet users.

Providing a better interface with other systems: In the absence of a global data protection framework, different regional standards must be able to co-exist. This would be in the EU's interest, as it would provide an incentive for other regions to move their systems closer to that of the EU. At present, EU law only provides for a possible "adequacy" decision being formally adopted by the European Commission. However, such a decision is based on the third country essentially adopting the EU data protection system, and is thus less an interface than a confirmation that the third country has adopted a system substantially similar to EU law. The procedure for an adequacy decision is cumbersome, and few third countries have received one,[94] so that it seems insufficient as a method of international interface.

There are various possibilities for such an interface. The most wide-ranging one would be for EU law to provide full legal recognition to data protection standards in other regions; this seems to be what the White House means by "international interoperability" between the EU and the US in the paper proposing a consumer data privacy framework

---

[91] See General Data Protection Regulation, *supra* nt. 39, Article 45.

[92] The author knows of influential EU policymakers who share this interpretation of that case.

[93] See *EJIL Talk*, Kuner, C., "Extraterritoriality and the fundamental right to data protection", 16 December 2013, available online at <ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/> (accessed 30 September 2014); Milanović, *supra* nt. 27.

[94] As of July 2014, thirteen such decisions had been adopted in the sixteen years since the Directive came into force. See European Commission, *Commission Decision on the Adequacy of the Protection of Personal Data in Third Countries*, available online at <ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm> (accessed 30 September 2014).

that it published in 2012.[95] However, the political difficulties for the EU to adopt such a system with regard to data protection seem considerable.[96] In addition, the *Kadi* judgment puts into question the possibility of fully recognising a data protection system that does not incorporate EU concepts of fundamental rights (such as that of the US).

However, some room still remains for accommodation between EU data protection law and standards in other regions. From an EU perspective, such accommodation should be possible as long as such standards provide an 'adequate level of protection'.[97] The key challenge here will be to define the core or essential elements of data protection on an international scale. Data protection law contains a number of legal obligations, some of which are central to its nature as a fundamental right while others are not.[98] The EU Charter of Fundamental Rights refers to the "essence" of fundamental rights and freedoms,[99] and explicitly mentions the requirement that data be processed based on consent or some other legal basis, the rights of access and rectification, and control of data protection rules by an independent authority.[100] These can thus be seen as the essential elements of the fundamental right to data protection under EU law. The way that these elements are elaborated in detail to promote convergence in privacy standards between different regional and national systems of regulation would depend on international negotiations that are beyond the scope of this article.

Even if a system does not qualify as fully "adequate" under the EU standard, a narrower level of recognition could still be provided to it. For example, the enactment by a State of Council of Europe Convention 108 may by itself not be sufficient to ensure that it offers "adequate protection", but granting some lesser degree of recognition to States that have enacted it (i.e. considering them as having moved at least part of the path towards adequacy) would help build bridges between the EU system and States that enact the Convention (particularly States outside the EU). At present enactment of the Convention is regarded informally as one indication of potential adequacy,[101] but this is not formally set forth in the Directive.[102] The proposal of the European Commission for a General Data Protection Regulation also contains no mention of the Convention 108 or its interaction with EU data protection law, but the Council of the European Union in its deliberations on the Regulation has proposed adding a provision requiring the Commission to take into account a third country's accession to the Convention when

---

[95] White House, *Consumer Data Privacy in a Networked World*, February 2012, available online at <whitehouse.gov/sites/default/files/privacy-final.pdf> (accessed 30 September 2014).

[96] See Schwartz, P., *Differing privacy regimes: a mini-poll on mutual EU-U.S. distrust*, 22 July 2014, available online at <privacyassociation.org/news/a/differing-privacy-regimes-a-mini-poll-on-mutual-eu-u-s-distrust/> (accessed 30 September 2014).

[97] See Kokott, J. and Sobotta, C., "The Kadi case—constitutional core values and international law—finding the balance", *European Journal of International Law*, vol. 23, ed. 4, 2012, 1015–1024, 1018, stating that the reason for the CJEU's approach in the Kadi case was that the UN Security Council resolution at issue did not provide sufficient protection for fundamental rights.

[98] See European Data Protection Supervisor, Hustinx, P., *Concluding Remarks made at 3rd Annual Symposium of the European Union Agency for Fundamental Rights*, Vienna, 10 May 2012, available online at <secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-05-10_Speech_Vienna_EN.pdf> (accessed 30 September 2014).

[99] Article 52(1).

[100] *Id.*, Articles 8(2)–(3).

[101] Article 29 Working Party, "First orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy" (WP 4, 26 June 1997), 8–9.

[102] See EU Data Protection Directive, Recital 11, stating that the provisions of the Directive 'give substance to and amplify' those contained in Council of Europe Convention 108.

assessing adequacy.[103] Greater use could also be made of adequacy decisions that apply only in specific industries or sectors.

IV.3. Final thoughts

The challenge for the EU with regard to development of a global data protection framework is to promote strong standards at the international level, while avoiding the *Kadi* Court's approach of 'withdrawing into one's own constitutional cocoon, isolating the international context and deciding the case exclusively by reference to internal constitutional precepts'.[104] Taking steps to deal with the three issue mentioned herein would go some way to providing an interface with other legal systems that could help to develop international standards gradually, without weakening the fundamental right to data protection under EU law.

The EU should also recognise that, if it wants its data protection law to be the "de facto standard for the world", then it has certain responsibilities towards other States that adopt it, particularly those in the developing world. Recognition of such responsibilities would ultimately be in the EU's interest, since it would provide additional incentives for other countries to adopt EU data protection law.

The EU should thus be accountable both to maintain its high level of data protection and comply with its obligations under EU fundamental rights law, and to provide sufficient interfaces to other data protection systems. Only this mixture of respect for fundamental rights and flexibility towards the variety of data protection systems that exist around the world can provide the conditions under which an international legal framework for data protection can eventually develop.

*

[103] Council of the European Union, Note from the Presidency to the Working Party on Information Exchange and Data Protection, no. 11028/14, 30 June 2014, Article 81a.

[104] EJIL Talk, Weiler, J., "Editorial: EJIL Vol. 19:5", available online at <ejiltalk.org/letters-to-the-editor-respond-to-ejil-editorials-vol-195/> (accessed 30 September 2014), describing the approach of the CJEU in the *Kadi* judgment.