The Internet and the Global Reach of EU Law

Christopher Kuner

LSE Law, Society and Economy Working Papers 4/2017
London School of Economics and Political Science
Law Department

The Internet and the Global Reach of EU Law

Christopher Kuner [*]

Abstract: EU law has significant influence on the Internet and parties outside the EU's territorial boundaries that use it and are affected by it. The Internet has enabled the EU to extend to third countries the application of its fundamental values, including the autonomy of EU law, the rule of law, and fundamental rights. There are many examples of the EU exerting its global reach regarding the Internet, particularly in data protection law, but also in areas such as Internet governance, international agreements, and private international law. This occurs through a variety of mechanisms, including emulation and learning; international negotiation; coercion and conditionality; and blocking recognition of third country legal measures. The EU's actions in exercising its global reach implicate important normative issues, such as distinguishing between the furtherance of core EU legal values and the advancement of the EU's political interests; promoting the principles of EU law as universal values; ensuring that EU legal values are upheld in practice; and determining the territorial boundaries of EU law. The influence exercised by the EU carries responsibilities towards third countries, particularly those in the developing world. The Internet may also be influencing EU law, as is shown by the changing role of the Court of Justice.

[*] Professor of Law and Co-Chair of the Brussels Privacy Hub, Vrije Universiteit Brussel (VUB), Brussels; Visiting Professor, Department of Law, London School of Economics and Political Science; Affiliated Lecturer, Faculty of Law, University of Cambridge; Senior Privacy Counsel, Wilson Sonsini Goodrich & Rosati, Brussels. I am grateful for feedback given by the students in my lectures at the Summer Course on European Union Law at the Academy of European Law held in July 2016 at the European University Institute, Florence, which was the genesis of this chapter. This is an advanced draft; a final, revised version will be published by Oxford University Press in the *Collected Courses of the Academy of European Law*. This version takes into account developments through January 2017.

1. INTRODUCTION

Since becoming available for widespread use in the mid 1990s, the Internet has 'contributed to a shrinking of the world and to an interconnectedness of legal orders that has never been as intense in legal history'.[1] During the same period, EU law has become a normative power that exerts its influence over a variety of phenomena,[2] including the Internet.

The relationship between EU law and the Internet is one of mutual influence. On the one hand, EU law has influenced the development of the Internet, and impacted countries and parties outside the EU's borders. On the other hand, the Internet raises important questions about the application, scope, and normative values of EU law. In many ways the Internet is the ideal vehicle for examining the ambitions of EU law in an increasingly complex and globalized world.

The Internet functions based on technical protocols rather than legal rules. It was established as a distributed network not under the control of a sole country or government,[3] and operates based on open standards that allow networks around the world to connect with each other. The Internet also makes it possible for anyone to create content or offer products and services without permission from a central authority. This open, independent structure has been one of the keys to its success.

However, these same factors complicate the relationship between EU law and the Internet. The Internet is not an enterprise, public authority, product, technology, or other entity or institution of the type that is normally the subject of influence by EU law. Furthermore, instruments of 'soft law' (for example, contractual arrangements between private parties) play a crucial role in the way the Internet is used.[4] This demonstrates how the governance and regulation of the Internet can be regarded as an example of pluralism and global legal hybridity.[5] This chapter will examine the influence that EU law has over the Internet and

---

[1] J. Basedow, 'The Law of Open Societies—Private Ordering and Public Regulation of International Relations', 360 *Recueil des cours/Collected Courses of the Hague Academy of International Law* (2012) 9, at 471.

[2] Some of the leading scholarly examinations of this topic include Bradford, 'The Brussels Effect', 107 *Northwestern University Law Review* (2013) 1; Gilardi, 'Transnational diffusion: Norms, ideas, and policies', in W. Carlsnaes, T. Risse, and B. Simmons (eds) (2012), *Handbook of International Relations* (2012) 453, <http://www.fabriziogilardi.org/resources/papers/gilardi_handbook_IR_v2.pdf> (last visited 12 November 2016); Scott, 'Extraterritoriality and Territorial Extension in EU Law' 62 *American Journal of Comparative Law* (2014) 87; Scott, 'The New Extraterritoriality' 51 *Common Market Law Review* (2014) 1343; De Witte and Thies, 'Why Choose Europe? The Place of the European Union in the Architecture of International Legal Cooperation', in B. Van Vooren, S. Blockmans and J. Wouters (eds), *The EU's Role in Global Governance* (2013) 23; Young, 'The European Union as a Global Regulator? Context and Comparison', 22 *Journal of European Public Policy* (2015) 1233.

[3] For a brief description of the Internet, what it is, and how it operates, see Internet Society, 'The Internet: How it Works', <https://www.internetsociety.org/internet/how-it-works> (last visited 23 October 2016).

[4] See L. Bygrave, *Internet Governance by Contract* (2015), at 6 (Kindle edition); C. Marsden, *Internet Co-Regulation* (2011).

[5] See P. Schiff Berman, *Global Legal Pluralism* (2012), at 177-178 (Kindle edition).

parties outside the EU's territorial boundaries that use and are affected by it. The global reach of EU law is manifested in different types of actions taken by the EU and its Member States, such as asserting EU values and interests in international organisations and the conclusion of international treaties; influencing the adoption of legislation in third countries; requiring compliance with EU legal standards outside its borders; and undertaking regulatory investigations in third countries. It will also deal with the interaction between the underlying values of EU law and the Internet, i.e., situations when these values apply to the Internet and produce effects outside the EU. The extension of EU values to the Internet has been made possible by the evolution of EU law in recent years through the adoption of the Treaty of Lisbon[6] and the elevation of the EU Charter of Fundamental Rights[7] to the level of binding primary law.[8] In exerting its global reach, the EU increasingly attempts to promote its legal values as universal values.

The Internet also presents EU law with important challenges. Because of the fragmented and global nature of Internet governance and regulation, much activity conducted on it is not subject to the direct control of EU law. The relationship between the EU institutions and the Member States also plays an important role in determining the limits and efficacy of EU action regarding the Internet.

An examination of the interaction between EU law and the Internet raises a number of important normative questions, such as regarding the interrelationship between EU legal values and the EU's political or policy interests; the implications of asserting EU values as universal values; how to ensure that EU values apply to the Internet in practice as well as in theory; whether there are territorial limits to the application of EU law; and what responsibilities EU law has towards the third countries that it influences, particularly those in the developing world. It also seems that, just as EU law influences the Internet, the Internet may be changing EU law.

2. THE NATURE OF THE INTERNET AND ITS GOVERNANCE

A. WHAT IS THE INTERNET?

Defining the Internet is more difficult than it might seem at first glance. The definition articulated in 1995 by the US Federal Networking Council (FNC) is often cited:

> 'Internet' refers to the global information system that (i) is logically linked

[6] Treaty of Lisbon, OJ 2007 C 306/1.
[7] Charter of Fundamental Rights of the European Union, OJ 2010 C83/389.
[8] Consolidated Version of the Treaty on European Union (TEU), OJ 2012 C326/13, at Art. 6(1).

> together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/ follow-ons; (ii) is able to support communications using the Transmission Control Protocol / Internet Protocol (TCP/IP) suite or its subsequent extensions/ follow-ons, and/ or other IP-compatible protocols; and (iii) provides, uses, or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.[9]

This definition focuses on the Internet's use of the TCP/IP suite[10] in order to differentiate it from other networks. However, the Internet is much more than a single technical protocol. Nowadays, different networks may be connected to transfer data at least in part via the Internet, not all of which employ TCP/IP.[11] The term 'Internet' is often used not just in relation to a particular protocol or technology, but to refer to the interconnection of electronic communications networks around the world, including the technical infrastructure that they use. Because Internet technologies and their use change so quickly, it seems best to adopt a broad definition that includes not only networks that run based on TCP/IP, but the global communications infrastructure that underlies the Internet.[12] Understood in this way, the Internet can be defined to include the broad range of infrastructure, content, applications, hardware, and other phenomenon that determines both the purpose of the Internet, and how it operates in practice.[13] Thus, the Internet will be considered here to constitute the 'network of networks' that includes the totality of global communications networks, infrastructure, and content that are connected to it and transmitted on it.

B. How is the Internet governed?

The Internet functions based on a multi-layered governance model, as illustrated by the following chart:[14]

---

[9] FNC Resolution of 24 October 1995, <https://www.nitrd.gov/fnc/Internet_res.aspx> (last visited 22 October 2016).

[10] The TCP/IP suite is a set of communications protocols widely used to transmit data packets on the Internet. See <http://www.pcmag.com/encyclopedia/term/52614/tcp-ip> (last visited 22 January 2017).

[11] For a discussion of the factors involved in defining what constitutes the Internet, see Bygrave, *supra* note 4, at 14-17 (Kindle edition).

[12] *Ibid.*, at 15 (Kindle edition).

[13] L.B. Solum, 'Models of Internet Governance', in L. Bygrave and J. Bing (eds), *Internet Governance: Infrastructure and Institution*s (2009) 48, at 48–9, stating that 'In the broad sense, the Internet is a complex entity that includes the hardware and software technical infrastructure, the applications, and the content that is communicated or generated using those applications'.

[14] The chart is adapted from Cerf, Ryan, and Senges, 'Internet Governance is our Shared Responsibility', 10 *I/S: A Journal of Law and Policy for the Information Society* (2014) 1, at 10. The bullet points included in each layer are exemplary rather than exhaustive.

Social Layer • Trust and identity • Human rights applied to the Internet • Internet governance principles (e.g. net neutrality)
Content Layer • Data protection • Intellectual property rights • Cybercrime • SPAM
Logical Layer • Internet naming and numbering • Protocols & other standards
Infrastructure Layer • Connectivity & universal access

In this model, the infrastructure layer comprises the networks through which data travels on the Internet; the logical layer contains the code and mechanisms by which the Internet operates; the content layer contains the information that is transmitted through it and the legal rules that govern such information; and the social layer deals with 'practices that define paramount rights and principles associated with 'social conduct' online'[15]. This chapter will mainly be concerned with the third and fourth layers (i.e., the content and social layers), though EU law may impact all four.

The primary instruments of EU law do not explicitly mention the Internet. However, the various layers of governance set forth above are subject to regulation by the EU insofar as there is EU law in the respective area; for example, telecommunications networks are subject to telecommunications regulation, and intellectual property and data protection are affected by those areas of regulation. The fragmented governance structure of the Internet limits the ability of EU to exert control over it. The Internet is accessible globally, and most of the infrastructure on which it runs, the organizations that maintain it, and the individuals that use it are located outside the EU. Moreover, as a global communications infrastructure the Internet is of interest to countries all over the world, which may exercise their own legal and regulatory power over it, potentially leading to legal conflicts.

A number of international entities and organisations play an important role in the functioning and governance of the Internet. In 2006, the United Nations Secretary-General established the Internet Governance Forum (IGF), a forum for dialogue on all issues of policy related to Internet governance that includes participation from stakeholders in all sectors, including governments, the private

[15] *Ibid.*, at 9.

sector, civil society, academia, and the technical community.[16] Several organisations also play a crucial role in setting technical standards for the Internet, such as the Internet Engineering Task Force (IETF),[17] the World Wide Web Consortium (W3C),[18] and the Internet Corporation for Assigned Names and Numbers (ICANN),[19] none of which are 'regulators' in the sense of being public authorities mandated with enforcing a set of laws or legal rules.

The growing social, economic, and political importance of the Internet has led to its increased regulation in all regions of the world,[20] which frequently causes difficulties in application and enforcement of the law. The difficulty of applying and enforcing any regulatory system (not just EU law) to the Internet rests on the fact that its operation involves a highly fragmented universe of actors, norms, procedures, processes, and institutions, including many non-state entities (such as private companies, non-governmental organisations, academic institutions, standards organisations, and others). Their activities have resulted in the adoption of contracts, technical standards, guidelines, and best practices that differ from legislation and legal regulation traditionally enacted by governments, but that still have had a profound effect on how the Internet functions:

> [T]he governance structure for the Internet has been formed largely outside a treaty or other legislative framework that is Internet-specific. Contracts provide the legal bricks and mortar for much of the present structure, and they do so often without a direct basis in legislation. Concomitantly, the governance structure is relatively unencumbered by dirigiste ideology and has permitted a fairly high degree of self-regulation. While tentacles of government control are increasingly visible, private sector bodies have usually been allowed—and often encouraged—to lead the design and management of the Internet. Governments have acted more as facilitative partners of these bodies than as heavy-handed regulators, at least in Western democracies. In other words, governance has been exercised to a large degree by contractually based, co-operative networks rather than decree.[21]

It is often difficult to determine the place where an action on the Internet takes place, or where the actor that initiated or completed it is located. Jurisdictional rules in many legal systems are based on the principle of territoriality, i.e., that

---

[16] See <http://www.intgovforum.org/multilingual/> (last visited 23 October 2016).
[17] See <http://www.ietf.org> (last visited 23 October 2016).
[18] See <https://www.w3.org> (last visited 23 October 2016).
[19] See <https://www.icann.org> (last visited 23 October 2016).
[20] See J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (2008); Schiff Berman, *supra* note 5, at 28-29 (Kindle edition), stating that countries around the world have enacted 'laws purporting to regulate almost every conceivable online activity, from gambling to chat rooms to auction sites, and seeking to enforce territorially based rules regarding trademarks, contractual relations, privacy norms, "indecent" content, and crime, among others'.
[21] Bygrave, *supra* note 4, at 2 (Kindle edition).

jurisdiction obtains over acts committed within the territory of the country in question.[22] However, the Internet complicates application of the territoriality principle, since it can be difficult to localize an online action as occurring in a particular country.[23] This leads to uncertainty as to which law applies or which legal system has jurisdiction over Internet-related activities, which is reflected in the challenges that the Internet presents to EU law.

3. THE EU AND THE MEMBER STATES

Both the EU and the Member States are active in law and policy regarding Internet issues, and the relationship between the two helps determine the scope of EU law concerning the Internet.

At the EU level, the making of law and policy concerning the Internet is fragmented among the institutions. To give a few examples, in the European Commission different Directorates-General take the lead in work on Internet issues such as net neutrality,[24] data protection,[25] and intellectual property rights.[26] Other EU institutions, such as the European Economic and Society Committee[27] and the European Parliament,[28] are also deeply involved in Internet issues. There are Internet-related initiatives pursued jointly by various EU institutions; an example is the Communication concerning the 'Cybersecurity Strategy of the European Union',[29] which was published jointly in 2013 by the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy (the 'High Representative'). As discussed throughout this chapter, there are also numerous legislative initiatives in the EU and judgments of the Court of Justice dealing with the Internet. While it is not an EU institution, the European Court of Human Rights has issued numerous judgments concerning the

---

[22] See, e.g., C. Ryngaert, *Jurisdiction in International Law* (2nd ed., 2015), at 49 (Kindle edition).
[23] See, e.g., Michaels, 'Territorial jurisdiction after territoriality' in: P. J. Slot and M. Bulterman (eds.), *Globalisation and Jurisdiction* (2004) 105, at 106.
[24] See <https://ec.europa.eu/digital-single-market/en/open-internet-net-neutrality> (last visited 10 December 2016), work on which is led by DG CONNECT.
[25] See <http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm> (last visited 10 December 2016), work on which is led by DG JUST.
[26] See <https://ec.europa.eu/growth/industry/intellectual-property_en> (last visited 10 December 2016), work on which is led by DG GROW.
[27] See <http://www.eesc.europa.eu/?i=portal.en.information-society> (last visited 10 December 2016).
[28] See, e.g., the work of the European Parliament Committee on Civil Liberties, Justice and Home Affairs, <http://www.europarl.europa.eu/committees/en/libe/home.html> (last visited 10 December 2016).
[29] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', JOIN(2013) 1 final, 7 February 2013, <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667> (last visited 18 November 2016). See Schaake and Vermeulen, 'Towards a values-based European foreign policy to cybersecurity', 1 *Journal of Cyber Policy* (2016) 75.

Internet.[30]

The Member States exercise influence through the Council's role in enacting EU law and policy (for example, the Council is tasked with identifying the EU's 'strategic interests' in the context of external action[31]). In addition, Member States pursue their own legal and regulatory initiatives dealing with the Internet. A few examples include the 'Digitale-Agenda 2014-2017' of the German Federal Government,[32] the 'Agenda Digitale Italiana' of the Italian government,[33] and the 'Digitales Österreich' initiative of the Austrian government.[34] Legislatures, courts, and regulators in all Member States have been active in issues concerning the Internet.

Shared competence between the EU and the Member States is the general rule,[35] and the Internet is not mentioned in Article 3 TFEU that lists the Union's exclusive competences, so it is an area of shared competence. This conclusion is supported by the fact that some areas listed in Article 4(2) TFEU as examples of shared competence are particularly important with regard to the Internet, such as the internal market and consumer protection. This means that international agreements concluded by the EU concerning the Internet tend to be 'mixed' agreements that must be entered into by both the EU and the Member States.[36]

However, certain areas of EU law related to the Internet may fall primarily within the competence of the EU, as can be seen by the example of data protection. The Member States may act with regard to areas of shared competence only to the extent that the EU has not done so,[37] and data protection, which the EU first regulated on a horizontal basis in Directive 95/46/EC,[38] has now been harmonised via Regulation (EU) 2016/679 (the 'GDPR') that will become

---

[30] See European Court of Human Rights, Research Division, 'Internet: case-law of the European Court of Human Rights, Updated: 2015', <http://www.echr.coe.int/documents/research_report_internet_eng.pdf> (last visited 10 December 2016).

[31] TEU, supra note 8, at Art. 26(1). See P. Eeckhout, *EU External Relations Law* (2011), at 485-486 (Kindle edition).

[32] See <https://www.digitale-agenda.de/Webs/DA/DE/Home/home_node.html> (last visited 10 December 2016).

[33] See <http://www.agid.gov.it/agenda-digitale/agenda-digitale-italiana> (last visited 10 December 2016).

[34] See <https://www.digitales.oesterreich.gv.at> (last visited 10 December 2016).

[35] See Consolidated Version of the Treaty on the Functioning of the European Union (TFEU), OJ 2012 C 326/47, at Art. 4(1); A. Rosas and L. Armati, *EU Constitutional Law: An Introduction* (2012), at 23 (Kindle edition).

[36] For example, the United Nations Convention on the Use of Electronic Communications in International Contracts 2005, 2898 UNTS, Registration No. 50525, can be regarded as a mixed agreement. See Killian, 'The Electronic Communications Convention: A European Union Perspective', in A.H. Boss and W. Killian, *The United Nations Convention on the Use of Electronic Communications in International Contracts: An In-Depth Guide and Sourcebook* (2008) 407, at 414.

[37] TFEU, *supra* note 35, at Art. 2(2). See Rosas and Armati, *supra* note 35, at 246 (Kindle edition).

[38] 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, OJ 1995 L281/31.

applicable on 25 May 2018.[39] The new Regulation on Privacy and Electronic Communications[40] (the 'ePrivacy Regulation') proposed by the Commission in January 2017 would also result in harmonisation of data protection issues related to the Internet. This harmonisation means that the EU has more or less exclusive competence concerning data protection with regard to issues that fall within the scope of the harmonising legislation. In addition, the Member States may not undertake obligations with third countries that affect common rules laid down by the EU,[41] a principle that the GDPR affirms with regard to data protection,[42] suggesting that, in practice, the conclusion of international agreements concerning data protection also lies exclusively in the competence of the EU.[43] There are also limits on the ability of the Member States to participate in law-making initiatives in international fora even in the absence of exclusive competence of the EU,[44] in light of the duty of sincere cooperation that applies in cases of shared competence.[45]

With regard to the negotiation of international treaties relating to the Internet, in most cases the Commission should negotiate on behalf of the EU after being nominated by the Council,[46] except for treaties relating exclusively or principally to the Common Foreign and Security Policy, which should be negotiated by the High Representative.[47] This latter case would apply in an area such as cybersecurity insofar as it relates to defence, as this would seem to fall under the Common Security and Defence Policy,[48] which is an integral part of the Common Foreign and Security Policy.[49]

Of course, many important discussions between governments, countries, and other stakeholders take place in the work of institutions that do not focus solely on the conclusion of legally-binding agreements. Both the EU and the Member States are active on the international stage with regard to Internet issues, and both

---

[39] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L119/1.
[40] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final, 10 January 2017.
[41] See Case 22/70, *Commission v. Council (AETR/ERTA)*, [1971] ECR 263 (ECLI:EU:C:1971:32). See also Eeckhout, *supra* note 46, at 71-76 (Kindle edition).
[42] See GDPR, *supra* note 39, at Recital 102, stating 'Member States may conclude international agreements which involve the transfer of personal data to third countries or international organisations, as far as such agreements do not affect this Regulation or any other provisions of Union law and include an appropriate level of protection for the fundamental rights of the data subjects.'
[43] See H. Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (2016), at 468-470.
[44] See De Witte and Thies, *supra* note 2, at 32-33.
[45] See TEU, *supra* note 8, at Art. 4(3).
[46] See TFEU, *supra* note 35, at Art. 218(3); Eeckhout, *supra* note 46, at 195-196 (Kindle edition).
[47] *Ibid.*
[48] See P. Koutrakos, *The EU Common Security and Defense Policy* (2013), at 85 (Kindle edition). See also Cybersecurity Strategy of the European Union, *supra* note 29, at 11-12.
[49] TEU, *supra* note 8, at Art. 42(1).

participate in the work of international organisations such as the Council of Europe, the Organisation for Economic Co-Operation and Development (OECD), various UN agencies, standards-setting bodies, entities dealing with Internet governance, and others.

The relationship between the EU and its Member States with regard to the Internet is marked by both cooperation and tension. On the one hand, the EU seems to favour cooperation with regard to Internet issues on the part of the various EU institutions and the Member States. This can be seen in the European Commission's 2014 Communication on Internet governance, where it is stated that 'The Commission invites the Council and Parliament, the Economic and Social Committee, the Committee of the Regions, as well as Member States, to agree on a common vision as highlighted in this Communication and to defend it jointly in the forthcoming international debates'.[50]

At the same time, the division of competences between the EU and the Member States regarding the Internet can lead to disputes between them. For example, during negotiation of the Directive on Electronic Signatures,[51] the German government sought to have it cover only digital signatures using asymmetric cryptography (as were covered in the original version of the German Digital Signatures Act[52]), and not the broader category of electronic signatures,[53] which led to a dispute between Germany and the Commission as to the scope of the Directive. There were also numerous disputes between the Member States and the European Commission during the drafting and enactment of the GDPR about its contents, scope, and other issues.[54]

I have witnessed this tension first-hand in international organisations such as the Council of Europe in its modernisation of Convention 108,[55] and the United Nations Commission for International Trade Law (UNCITRAL) in its work

[50] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Internet Policy and Governance: Europe's role in shaping the future of Internet Governance', COM/2014/072 final, 12 February 2014, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0072&from=EN> (last visited 27 October 2016).
[51] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, OJ 2000 L13/12.
[52] *Signaturgesetz vom l. August 1997* (BGBl. I S. 1870, 1872), amended by *Signaturgesetz vom 16. Mai 2001* (BGBl. I S. 876) and Artikel 4 des *Gesetzes vom 17. Juli 2009* (BGBl. I S. 2091).
[53] See Bundesregierung der Bundesrepublik Deutschland, 'Anmerkungen der Bundesregierung zu dem Entwurf der Europäischen Kommission einer EG-Richtlinie über elektronische bzw. Digitale Signaturen', 8 April 1998, at 1.
[54] See Burton, De Boel, Kuner, Pateraki, Cadiot, and Hoffman, 'The Final European Union General Data Protection Regulation', 15 *Bloomberg BNA Privacy and Security Law Report* (2016) 153.
[55] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature on 28 January 1981, in force 1 October 1985, ETS 108. Regarding the work of the Council of Europe to modernise the Convention, see <http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp> (last visited 17 November 2016).

concerning both the UNCITRAL Model Law on Electronic Signatures[56] and the United Nations Convention on the Use of Electronic Communications in International Contracts[57] (hereinafter the UNCITRAL Convention on Electronic Communications). Disputes have tended to arise in this regard between the European Commission and the Member States when both were participating in the work of one of the relevant international organisations and the Commission asserted its right to negotiate on behalf of the EU regarding a matter that was the subject of present or pending EU legislation. When such disputes about competence break into the open in the work of international organisations, it weakens the influence of EU law by putting cooperation between the EU institutions and the Member States in a bad light and allowing third counties to assert themselves at the expenses of a disunited EU.

4. THE INTERNET AND THE VALUES OF EU LAW

A. INTRODUCTION

The EU is an autonomous legal entity based on values, the promotion of which is one of its aims,[58] and it is obliged to uphold and promote its values and interests in its dealings with the wider world.[59] The TEU contains a detailed list of 'principles' by which the EU is to be guided on the international scene, including 'democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the United Nations Charter and international law'.[60]

The extension of these values to the global Internet has occurred in conjunction with the development of EU law during the last twenty years. One of the first times that the EU dealt with Internet legal issues in an international context was in the scope of the ministerial conference on 'Global Information Networks' held in Bonn on 6-8 July 1997,[61] which was jointly organised by the European Commission and the German government and included representatives of the Commission, the Member States, the US government, other third country governments, international organisations, and the private sector. The final

---

[56] See <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html> (last visited 27 October 2016).
[57] See *supra* note 36.
[58] TEU, *supra* note 8, at Arts. 2 and 3(1). See also T. Tridimas, *The General Principles of EU Law* (2nd ed. 2006), at 15, finding that the values of the EU represent the EU legal order.
[59] TEU, *supra* note 8, at Art. 3(5) and Art. 21(3).
[60] *Ibid.*, at Art. 21(1). See also Hijmans, *supra* note 43, at 33.
[61] See <http://www.echo.lu/bonn/conference.html> (last visited 24 January2017).

'Ministerial declaration' published at the conclusion of the conference contained hardly any mention of actions to be taken specifically by the EU.[62] During the next few years, the EU largely focused on Internet-related issues relevant to the internal market, through the enactment of instruments such as the Directive on Electronic Commerce[63] and the Directive on Electronic Signatures.[64] It was only following entry into force of the Treaty of Lisbon in 2009 and the resultant elevation of the Charter of Fundamental Rights to primary law that EU law was given the tools to assert its values and interests at a global level regarding the Internet,[65] as can be seen in the post-Lisbon judgments of the Court of Justice which rely on the TEU, the TFEU, and the Charter to assert the global reach of EU law.

In considering the relationship between EU law and the Internet, it is important to identify the values, principles, and objectives of EU law that are implicated with regard to the Internet.

B. THE AUTONOMY OF EU LAW

EU law views itself as an autonomous legal system,[66] which has been interpreted to refer to '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'.[67] The autonomy of EU law means that EU legal rules are to be given priority over other rules in case of conflict, even with regard to international agreements.[68]

The pluralistic and fragmented nature of the Internet leads to frequent legal conflicts and situations where different norms cover the same actors or conduct, without the existence of clear rules to determine which has priority. Such situations impact the autonomy of EU law, since they may lead to non-EU norms prevailing over the fundamental values of EU law, a possibility that the Court of Justice has rejected in Internet-related cases.[69]

---

[62] See <http://www.echo.lu/bonn/final.html> (last visited 24 January2017).
[63] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ 2000 L 178/1.
[64] See *supra* note 51.
[65] See Hijmans, *supra* note 43.
[66] See, e.g., Opinion 2/13, 18 December 2014, (CLI:EU:C:2014:2454); Joined Cases C-402 & 415/05P, *Kadi*, [2008] ECR 1-6351 (ECLI:EU:C:2008:461).
[67] de Búrca, 'The European Court of Justice and the International Legal Order After Kadi', 51 *Harvard International Law Journal* (2010) 1, at 23.
[68] See *Kadi*, *supra* note 66, at para. 285.
[69] See Case C-362/14, *Schrems*, 6 October 2015 (ECLI:EU:C:2015:650), at paras. 84-87, criticising the EU-US Safe Harbour Arrangement as giving US law primacy over EU fundamental rights in situations where they conflict.

C. THE RULE OF LAW

The rule of law is one of the values upon which the EU is founded.[70] While the meaning of the term is open to interpretation,[71] it includes requirements such as that actions are limited by rules; that such rules are fixed and set in advance; and that judicial review and access to courts are available if they are violated.[72]

As one of the central values of the EU, the rule of law is a benchmark for EU action with respect to third countries, and 'is undoubtedly a value that the EU relentlessly seeks to export "beyond the borders of the Union by means of persuasion, incentives and negotiation," but other more "punishing" means have also been used…'[73] The Court of Justice has emphasized the need to respect the rule of law with regard to data processing on the Internet, as can be seen in its *Schrems* judgment, where it stressed the importance of upholding the rule of law with regard to legislation limiting the effective right to judicial protection contained in Article 47 of the Charter of Fundamental Rights.[74] Thus, upholding the rule of law with regard to the Internet is a key concern of EU law, particularly as this relates to fundamental rights.[75]

D. FUNDAMENTAL RIGHTS

Fundamental rights are a value upon which the EU is founded,[76] and they play a key role in the relationship between EU law and the Internet. First of all, the EU must promote fundamental rights in its dealings with the wider world, including the Internet. Second, fundamental rights place limits on the action that the EU may take and oblige it to protect the rights of EU individuals. Fundamental rights must be respected whenever EU law applies,[77] as the Court of Justice has stressed in various judgments dealing with Internet-related issues of data protection,[78] online copyright infringement,[79] and the retention of telecommunications data.[80]

---

[70] TEU, *supra* note 8, at Art. 2.
[71] See Kochenov, 'The EU Rule of Law: Cutting Paths through Confusion', 2 *Erasmus Law Review* (2009) 5, at 9.
[72] Rosas and Armati, *supra* note 35, at 46 (Kindle edition).
[73] Pech, 'Rule of Law as a Guiding Principle in the EU's External Action', Centre for the Law of EU External Relations, CLEER Working Papers 2012/13, <http://www.asser.nl/media/1632/cleer2012-3web.pdf> (last visited 28 October 2016), at 13.
[74] See *Schrems*, *supra* note 69, at para. 95.
[75] See Hijmans, *supra* note 43, at 27-31.
[76] See TEU, *supra* note 8, at Art. 2. See also Art. 6(1) TEU, stating that fundamental rights have the same legal value as the Treaties.
[77] See Case 617/10, *Åkerberg Fransson*, 26 February 2013 (ECLI:EU:C:2013:105), at para. 21.
[78] See, e.g., *Schrems*, *supra* note 69; Case C-131/12, *Google Spain*, 13 May 2014 (ECLI:EU:C:2014:317).
[79] Case C-160/15, *GS Media BV*, 8 September 2016 (ECLI:EU:C:2016:644), at para. 31.
[80] *Digital Rights Ireland and Seitlinger*, Joined Cases C-293/12 and C-594/12, 8 April 2014 (ECLI:EU:C:2014:238); *Tele2 Sverige AB*, Joined Cases C-203/15 and C-698/15, 21 December 2016 (ECLI:EU:C:2016:970).

5. INTERACTION BETWEEN EU LAW AND THE INTERNET

A. INTRODUCTION

Some topics of EU law are by their nature 'external', while others are inherently 'internal' but have global reach.[81] The Internet merges the distinction between these two categories, since 'in a globalized economy, everything has an effect on everything'.[82] The discussion herein will thus cover several areas of EU law that directly focus on the Internet (such as Internet governance), as well as other ones that routinely raise Internet-related issues (such as data protection). This is by necessity a selection of a few areas where EU law interacts with the Internet, and is not intended to be exhaustive. As this examination will show, the EU exerts its influence on Internet-related developments in many areas, including in some cases the direct application of EU law to activities in third countries.

B. INTERNET GOVERNANCE

The term 'Internet governance' refers not just to the technical management of the Internet, but also to law and policy in a host of areas dealing with communication and information policy.[83] This is reflected in the definition used by the European Commission in its 2014 Communication on Internet governance, which defines the term broadly and emphasizes its pluralistic nature.[84] One of the EU's main objectives in Internet governance is to have the law apply to the Internet just as it does to the offline world,[85] a view that has also been advocated by the UN Human Rights Council.[86]

An example of EU action to promote its own values regarding internet governance concerns the domain name system (DNS), which functions as a kind of address book that translates domain names to Internet protocol addresses so that computers connected to the Internet can communicate with each other.[87] Domain name registrars maintain a register of the owners of domain names that can be queried online by searching the WHOIS servers, which contain a

---

[81] See Rosas and Armati, *supra* note 35, at 237 (Kindle edition); Cremona and Micklitz, 'Introduction', in M. Cremona and H.-W. Micklitz (eds), *Private Law in the External Relations of the EU* (2016) location 1427, at location 1451 (Kindle edition).
[82] Michaels, *supra* note 23, at 123.
[83] See *supra* section 2B.
[84] See Communication from the Commission, *supra* note 50, at 2, stating: 'Internet governance is broadly understood to refer to the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet'.
[85] *Ibid.*, at 2.
[86] UN Human Rights Council, 'The promotion, protection, and enjoyment of human rights on the Internet' (29 June 2012), UN Doc A/HRC/20L.13, at 2, stating that 'the same rights that people have offline must also be protected online…'.
[87] See <http://www.internetsociety.org/dns> (last visited 27 December 2016).

substantial amount of data about registered domains, their registrants, and the servers used. Placing this data to be searched on the Internet via the WHOIS protocol clashes with EU data protection law,[88] which has led to criticism of the WHOIS system by the body of EU and Member State data protection authorities (called the Article 29 Working Party).[89] These criticisms have resulted in ICANN granting waivers in some cases to domain name registrars in the EU with regard to the conditions for data access and retention contained in the Registrar Accreditation Agreement (RAA) that controls how registrars store and make available WHOIS data, in order to allow them to take EU data protection requirements into account.[90]

The EU institutions may cooperate with other entities to assert the values of EU law in Internet governance. For example, the Communication published jointly by the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy Communication in 2013 concerning the 'Cybersecurity Strategy of the European Union'[91] urges that the EU develop 'a coherent international cyberspace policy' that promotes 'EU core values' in cooperation with 'relevant international partners and organisations, the private sector and civil society', and that this be mainstreamed into EU external relations and the Common Foreign and Security Policy.[92]

C. DATA PROTECTION

Data protection law, which subjects the processing of personal data to a set of defined rules in order to protect the fundamental rights of individuals, has become a prime tool for regulating the Internet. Much of the EU's influence in data protection occurs through the extraterritorial application of EU law. There are different varieties or degrees of extraterritoriality, which range from the direct application of EU law to parties or conduct in third countries, to 'extraterritorial extension', meaning governance by the EU of activities not centred on EU territory.[93] With regard to EU data protection law, it is less important to categorize the exact form of extraterritoriality that the law uses, than to recognize that it exerts its influence in different ways on persons and activities in third countries.

The direct extraterritorial application of EU data protection law through the use of rules of applicable law and jurisdiction is discussed below.[94] A further example of extraterritoriality is provided by rules of EU data protection law that

---

[88] See Bygrave, *supra* note 4, at 120 (Kindle edition).
[89] Article 29 Working Party, 'Opinion 2/2003 on the application of the data protection principles to the WHOIS directories' (WP 76, 13 June 2003), at 4.
[90] Bygrave, *supra* note 4, at 121 (Kindle edition).
[91] Cybersecurity Strategy of the European Union, *supra* note 29.
[92] *Ibid.*, at 14-16.
[93] See Scott, 'Extraterritoriality and Territorial Extension of EU Law', *supra* note 2, at 89; Scott, 'The New Extraterritoriality', *supra* note 2; Young, *supra* note 2, at 1241.
[94] See *infra* section 5E.

restrict the transfer of personal data to third countries. Article 25 of Directive 95/46/EC allows data transfers to third countries only when an adequate level of data protection is provided in the country based on EU legal standards. The European Commission is empowered to issue a formal decision based on Article 25 that a third country provides an adequate level of data protection,[95] which is based on a determination that the foreign legal system in question offers a level of protection 'essentially equivalent' to that under EU law.[96] When an adequacy decision has not been issued, Article 26(2) of Directive 95/46/EC permits transfers of personal data if 'adequate safeguards' are provided, which means in practice that standard contractual clauses issued by the European Commission have been signed between the data exporter in the EU and the data importer outside the EU obliging both to provide protections to the transfer and processing of the data,[97] or that the party transferring the data has implemented binding corporate rules (BCRs, which are legally-binding internal data processing rules applied by a group of undertakings or enterprises engaged in a joint economic activity).[98] In addition, derogations from the requirement of adequacy (e.g., when the data subject has consented to the transfer) may apply when there is no essential equivalence and appropriate safeguards cannot be used.[99]

EU data protection law makes the processing of personal data transferred to third countries conditional on the external application of EU data protection standards.[100] In the case of adequacy decisions this occurs through a formal evaluation of third country standards by the Commission, whereas in the case of adequate safeguards the parties that receive data exported from the EU are obliged, either by contract or through the adoption of BCRs, to apply protections based on EU law when they process data in third countries.[101] This approach will

---

[95] There are currently twelve European Commission adequacy decisions in force, covering Andorra; Argentina; the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA); Switzerland; the Faroe Islands; Guernsey; Israel; the Isle of Man; Jersey; New Zealand; the EU-US Privacy Shield; and Uruguay. See <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> (last visited 27 December 2016). In January 2017 the Commission announced that it will 'actively engage with key trading partners in East and South-East Asia, starting from Japan and Korea in 2017, and, depending on progress towards the modernisation of its data protection laws, with India, but also with countries in Latin America, in particular Mercosur, and the European neighbourhood which have expressed an interest in obtaining an "adequacy finding"'. Communication from the Commission to the European Parliament and the Council, 'Exchanging and Protection Personal Data in a Globalised World', COM(2017) 7 final, 10 January 2017, at 8.

[96] The Court of Justice articulated this standard in *Schrems*, *supra* note 69, at para. 73.

[97] See, e.g., Commission Decision (EC) 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive (EC) 95/46/EC of the European Parliament and of the Council, OJ 2010 L39/5, Clauses 5(a), 5(d)(i), and 5(e).

[98] GDPR, *supra* note 39, at Arts. 4(20) and 47.

[99] See Directive 95/46/EC, *supra* note 38, Art. 26(1).

[100] See Mills, 'Private International Law and EU External Relations: Think Local Act Global, or Think Global Act Local?', 65 *International and Comparative Law Quarterly* (2016) 541, at 573-574.

[101] See, e.g., 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ 2004 L385/74, Clause II(h), requiring the data importer to process personal data exported from the EU with one of the following, at its option: 1) the data

continue to apply (in modified form) under the GDPR,[102] which will introduce new data transfer mechanisms that are also based on the application of EU data protection standards in third countries. For example, under the GDPR codes of conduct and certification mechanisms that result in the application of EU data protection law to the processing of personal data outside the EU may serve as a legal basis for transfer.[103]

The direct application of EU data protection law to third countries is also demonstrated by the fact that data protection authorities (DPAs) of the EU Member States have asserted their enforcement authority to investigate whether parties in third countries comply with EU law with regard to data transferred from the EU. The first such case occurred in 1996, when Citibank consented to have an on-site audit of its data processing facilities in the US conducted by the Berlin Data Protection Commissioner's office.[104] The Spanish Data Protection Agency has also conducted an audit of a third-party data processor located in Colombia regarding compliance with Spanish legal requirements for data transfers,[105] and the Italian Data Protection Authority has obtained the consent of Google to audit the company's compliance with EU data protection law on its premises in California.[106]

EU data protection law also exercises global influence through the adoption by third countries of data protection laws based on the EU model. Dozens of countries worldwide have enacted data protection laws based on the model of Directive 95/46/EC,[107] leading it to be called 'by far the most influential international policy instrument' in the field of data protection.[108] Among the

---

protection law of the country (i.e., the EU Member State) where the data exporter is established; 2) the relevant provisions of a Commission adequacy decision when the data importer is based in a country where such decision applies; or 3) a set of data protection principles contained in the contract and based on EU law. See also Article 29 Working Party, 'Working Document Setting up a Framework for the structure of Binding Corporate Rules' (WP 154, 24 June 2008), at 10, providing that 'In any event data shall be processed in accordance to the applicable law as provided by the Article 4 of the Directive 95/46/EC and the relevant local legislation.'

[102] GDPR, *supra* note 39, at Chapter V.

[103] *Ibid.*, Arts. 40(3) and 42(2).

[104] C. Bennett and C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), at 98; P. Schwartz, 'Managing Global Data Privacy: Cross-Border Information Flows in a Networked Environment' (2009), <http://theprivacyprojects.org/wp-content/uploads/2009/08/The-Privacy-Projects-Paul-Schwartz-Global-Data-Flows-20093.pdf> (last visited 11 November 2016), at 11-12.

[105] See Agencia Española de Protección de Datos, 'Report on International Data Transfers: Ex officio Sectorial Inspection of Spain-Colombia at Call Centres', July 2007, <https://www.agpd.es/portalweb/jornadas/transferencias_internacionales_datos/common/pdfs/report_Inter_data_transfers_colombia_en.pdf> (last visited 11 November 2016).

[106] Essers, 'Google agrees to Italian privacy authority audits in the US', PC World, 20 February 2015, <http://www.pcworld.com/article/2887192/google-agrees-to-italian-privacy-authority-audits-in-the-us.html> (last visited 11 November 2016).

[107] See, e.g., Bradford, *supra* note 2, at 22-26; L. Bygrave, *Data Privacy Law: An International Perspective* (2014), at 208 (Kindle edition), stating 'the overwhelming bulk of countries that have enacted data privacy laws have followed, to a considerable degree, the EU model…'; Greenleaf, 'The influence of European data privacy standards outside Europe: implications for globalization of Convention 108', 2 *International Data Privacy Law* 68 (2012).

[108] Bennett and Raab, *supra* note 104, at 93.

developments that can be traced to the influence of the Directive are the adoption of data protection laws in Central and Eastern European countries that have acceded to the EU, the passage of federal privacy legislation in Canada in 2000, and the growth of privacy laws in Asian countries.[109] The influence of EU data protection law can also be seen in the adoption of data protection acts in some African countries[110] and the implementation of privacy standards and seal programs in the private sector.[111]

The influence of EU data protection law has been due in part to the perceived economic benefit that can accrue to countries that enact it and are then able to import personal data under an EU adequacy decision[112] (though whether an adequacy decision leads to economic benefits in practice does not seem to have been independently verified). The fact that EU data protection law is based on a set of clearly-structured instruments also makes it attractive to third countries, which often find it easier to use an existing text as a model rather than to draft new legislation from scratch.

D. INTERNATIONAL AGREEMENTS

The Internet is a relatively recent phenomenon, and there are few legally-binding international agreements or treaties dealing specifically with it.[113] However, the example of one of them, the UNCITRAL Convention on Electronic Communications,[114] shows how the relationship between the EU and its Member States influences the EU's approach to the conclusion of international agreements dealing with the Internet.

Both the European Commission and numerous Member States participated in the negotiation of the Convention.[115] Early in the drafting, concerns were

---

[109] *Ibid.*, at 117.

[110] See, e.g., République du Sénégal, loi sur la protection des données à caractère personnel, exposé des motifs, <http://www.centif.sn/loi_caractere_personnel.pdf>, at 1 (last visited 11 November 2016); Traça and Embry, 'An overview of the legal regime for data protection in Cape Verde', 1 *International Data Privacy Law* (2011) 1.

[111] Bennett and Raab, *supra* note 104, at 172.

[112] See New Zealand Privacy Commissioner, 'Privacy amendment important for trade and consumer protection' (26 August 2010), <https://www.privacy.org.nz/news-and-publications/statements-media-releases/updated-media-release-30-8-10-privacy-amendment-important-for-trade-and-consumer-protection/> (last visited 10 November 2016), quoting the New Zealand Privacy Commissioner as follows regarding amendments to the New Zealand Privacy Act: 'An EU adequacy finding is also likely to satisfy data export requirements of other countries. I believe New Zealand businesses are already losing some trading opportunities through a gap in our privacy laws. This change will allow New Zealand to compete on a secure basis for international data business'. See also Bennett and Raab, *supra* note 104, at 113-114.

[113] Examples include the Council of Europe Convention on Cybercrime 2001, ETS No. 185; the WIPO Copyright Treaty 1996, 2186 UNTS 121 (2004); and the WIPO Performances and Phonograms Treaty 1996, 2186 UNTS 203 (2004). See also Uerpmann-Wittzack, 'Internetvölkerrecht', 47 Archiv des Völkerrechts (2009) 261.

[114] See UNCITRAL Convention on the Use of Electronic Communications, *supra* note 36.

[115] See UNCITRAL, Working Group IV (Electronic Commerce), Forty-first session, New York, 5-9 May 2003, Provisional List of Participants, UN DOC A/CN.9/WG.IV/XLI/INF.1.

expressed by the Commission about the effect that the Convention could have on the EU acquis communautaire,[116] particularly the EU E-Commerce Directive 2000/31/EC.[117] In response to these concerns, the following 'disconnection clause' was incorporated into the Convention:

> 1. A regional economic integration organization that is constituted by sovereign States and has competence over certain matters governed by this Convention may similarly sign, ratify, accept, approve or accede to this Convention. The regional economic integration organization shall in that case have the rights and obligations of a Contracting State, to the extent that that organization has competence over matters governed by this Convention. Where the number of Contracting States is relevant in this Convention, the regional economic integration organization shall not count as a Contracting State in addition to its member States that are Contracting States.
>
> 2. The regional economic integration organization shall, at the time of signature, ratification, acceptance, approval or accession, make a declaration to the depositary specifying the matters governed by this Convention in respect of which competence has been transferred to that organization by its member States. The regional economic integration organization shall promptly notify the depositary of any changes to the distribution of competence, including new transfers of competence, specified in the declaration under this paragraph.
>
> 3. Any reference to a 'Contracting State' or 'Contracting States' in this Convention applies equally to a regional economic integration organization where the context so requires.
>
> 4. This Convention shall not prevail over any conflicting rules of any regional economic integration organization as applicable to parties whose respective places of business are located in States members of any such organization, as set out by declaration made in accordance with article 21.[118]

The Convention was agreed on in 2005 and entered into force in 2013, but thus far neither the EU nor any of the Member States have signed it.[119] The reason for this lies in the EU's unhappiness with the final version of Clause 17(4), which requires either regional organizations (i.e., the EU) or their State members (i.e., the EU Member States) to make declarations under Article 21 in order to opt out of

---

[116] See Killian, *supra* note 36, at 408.
[117] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 OJ L178/1.
[118] UNCITRAL Convention on the Use of Electronic Communications, *supra* note 36, at Art. 17.
[119] See <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html> (last visited 14 November 2016).

application of the Convention to parties located in other State members.[120] The Commission objected to this wording, and demanded that it be replaced by a formulation under which EU law would automatically take precedence over the Convention without the need for declarations to be made.[121] Thus far neither the EU nor any Member States have signed or ratified the Convention.

E. PRIVATE INTERNATIONAL LAW

Rules of EU law on applicable law and jurisdiction (referred to here as private international law) can have external effect even when they are adopted mainly to further internal goals, since they impact disputes or relationships that have connections with third countries.[122] Private international law has thus become 'the key to the private law of global affairs in a multi-jurisdictional world'.[123]

Data protection law is a useful paradigm for examining the territorial scope of EU law as it relates to the Internet. Data protection in EU law is a self-contained area with regard to applicable law and jurisdiction, since these are determined under Directive 95/46/EC rather than under instruments dealing specifically with private international law, at least insofar as administrative enforcement of the law by the DPAs is concerned.[124] Under the GDPR, the territorial scope of application of data protection law will be expanded to include the processing of personal data of individuals in the EU by a data controller or data processor not established in the EU where the processing activities are related to the offering of goods or services to such individuals in the EU or the monitoring of their behaviour.[125] The GDPR will thus extend the geographic reach of EU law to apply directly to the Internet activities of many parties in third countries. The new ePrivacy Regulation would also apply to providers of electronic communications services not established in the EU when they provide such services to end users in the EU.[126]

The broad jurisdictional scope of EU data protection law on the Internet can be seen in two judgments of the Court of Justice. In *Google Spain*,[127] the Court found that EU data protection law granted individuals a right to suppress search

---

[120] See Killian, *supra* note 36, at 411-414.
[121] *Ibid.*
[122] See Mills, *supra* note 100, at 542.
[123] Basedow, *supra* note 1, at 35.
[124] See Case C-230/14, *Weltimmo*, 1 October 2015 (ECLI:EU:C:2015:639), at paras. 23, 51-52, finding that for the purposes of data protection law, Art. 4 of the Directive determines choice of law and Art. 28(6) determines jurisdiction. See also Brjkan, 'Data protection and European private international law: observing a bull in a China shop', 5 *International Data Privacy Law* (2015) 257.
[125] GDPR, *supra* note 39, Art. 3(2).
[126] ePrivacy Regulation, *supra* note 40, at Art. 3(1).
[127] See *Google Spain*, *supra* note 78, at paras. 42-61. See also Kuner, 'The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges', in B. Hess and C. M. Mariottini (eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection* (2015) 19, at 27-31.

engine results in certain situations, even though the servers on which the search engine operated were based in California. The French data protection authority (the CNIL) has interpreted the judgment to apply to searches performed on web sites in all domains globally (this issue is currently the subject of litigation in the French courts).[128] And in *Schrems*, the Court of Justice applied EU data protection law to the transfer of personal data to the US for processing there.[129]

F. OTHER AREAS

EU law has extended its global reach with regard to the Internet in other fields as well, only two of which will be considered here.

In *L'Oréal v. eBay*, the Court of Justice applied EU trade mark law to the sale on an Internet auction site of a trade-marked product in a third country when such sale was targeted at customers in the EU.[130] The Court thus extended the reach of EU law to third countries when failing to do so would have an impact on the effectiveness of EU rules.[131] And in May 2016 a number of leading Internet companies (including Google, Facebook, Twitter, and Microsoft) agreed to apply EU rules on hate speech following pressure from the EU Member States and the European Commission.[132]

6. MECHANISMS OF GLOBAL REACH

A. INTRODUCTION

EU law exerts its global reach by means of different mechanisms. Sometimes they are exercised intentionally, whereas in other situations they may apply as an afterthought or as part of some other phenomenon. These mechanisms are often intermingled, so that it can be difficult to determine which one applies in a

---

[128] See 'Right to be delisted: the CNIL Restricted Committee imposes a €100,000 fine on Google', 24 March 2016, <https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google> (last visited 10 November 2016).
[129] See *Schrems*, *supra* note 69, at paras. 45-46.
[130] *L'Oréal SA and Others v. eBay International AG and Others*, Case C-324/09, [2011] ECR I-6011 (ECLI:EU:C:2011:474).
[131] See Jääskinen and Ward, 'The External Reach of EU Private Law in the Light of *L'Oréal versus eBay and Google and Google Spain*', in Cremona and Micklitz, *supra* note 81, location 4843, at location 5123 (Kindle edition).
[132] See D. Robinson, 'Web giants sign up to EU hate speech rules', *Financial Times*, 31 May 2016, <https://www.ft.com/content/e8fb1690-26fc-11e6-8ba3-cdd781d02d89#axzz4ACePo5cX> (last visited 10 November 2016), noting that 'The move comes after EU ministers demanded that the bloc work with IT companies to "counter terrorist propaganda" during an emergency meeting in the aftermath of the Brussels terror attacks' and 'This push to codify the handling of illegal hate speech online has been led in Brussels by Vera Jourová, the commissioner responsible for justice'.

particular case, or they may apply in combination. But enough evidence exists to allow classification of the different mechanisms.

B. EMULATION AND LEARNING

One approach can be referred to as learning from EU law, or emulating it in domestic or international law-making. This can occur for various reasons, such as affinities in legal culture that make the EU example attractive to a third country, or the fact that EU law tends to be contained in legal instruments (such as directives, regulations, etc.) that on their face may seem easy to emulate.[133]

This emulation is encouraged by EU external action policy, which seeks to promote adoption of EU law in third countries in areas relevant to the Internet (such as data protection law), including financing technical assistance projects that allow experts from the EU to work with third countries.[134] For example, in 2011 such assistance was given by the EU to Mauritius, focused on 'ensuring the data protection accreditation of Mauritius with the European Union'.[135]

It can be difficult to distinguish learning or emulation from coercion. For example, what may seem to be the adoption of EU standards based on a voluntary decision by a third country may in fact be motivated by behind-the-scenes political pressure. In some cases, both third countries and the EU may not want to reveal the extent of the influence that EU law has had.

In certain areas EU law has become the leading model that other countries seek to emulate; a good example of this is data protection law. There are dozens of data protection laws in all regions around the world that have been inspired by the EU model,[136] and international organisations such as the Office of the UN High Commissioner for Refugees (UNHCR)[137] and the International Committee of the Red Cross (ICRC)[138] have also turned to EU law as an important source of inspiration when adopting data protection policies and guidelines. As such policies become more widely adopted among different international organisations and are considered to lead to binding obligations, they may gradually crystallize into

---

133 But see *infra* section 7C regarding the difficulty of replicating EU law outside the borders of the EU.
134 See Communication from the Commission, *supra* note 95, at 12. See also Pech, *supra* note 73, at 19.
135 See <http://eeas.europa.eu/delegations/mauritius/eu_mauritius/development_cooperation/technical_cooperation/index_en.htm> (last visited 13 November 2016).
136 See *supra* note 107.
137 UNHCR, 'Policy on the Protection of Personal Data of Persons of Concern to UNHCR', EJIL: *Talk!*, May 2015, <http://www.refworld.org/docid/55643c1d4.html> (last visited 14 November 2016). See Beck and Kuner, 'Data Protection in International Organizations and the new UNHCR Data Protection Policy: Light at the End of the Tunnel?', <http://www.ejiltalk.org/data-protection-in-international-organizations-and-the-new-unhcr-data-protection-policy-light-at-the-end-of-the-tunnel/#more-13568> (last visited 14 November 2016).
138 ICRC, 'ICRC Rules on Personal Data Protection', January 2016, <https://shop.icrc.org/publications/international-humanitarian-law/icrc-rules-on-personal-data-protection.html> (last visited 14 November 2016). See also Brussels Privacy Hub and International Committee of the Red Cross, *Handbook on Data Protection in International Humanitarian Action* (2017).

customary international law.[139] In such cases EU law may provide the basis for the progressive development of rules of public international law.

Courts in third countries have been influenced by judgments of the Court of Justice in cases involving the Internet. This influence has resulted in the export of European law, which has been described thusly:

> European judges 'export' European ideas outside Europe. Put differently, European courts' rulings, which are extensively quoted in an attempt to increase the legitimacy and persuasiveness of their own rulings, inspire and influence non-European Union judges.[140]

An example is the Court's *Google Spain* judgment, where it recognised the so-called 'right to be forgotten' (actually a right to suppression of results generated by Internet search engines).[141] This judgment has served as inspiration for courts in third countries, such as Canada.[142] The EU has generally viewed this influence as a one-way street in which EU standards are exported to third countries rather than vice versa, leading to what has been called a 'Europeanization' of the regulation of the Internet.[143]

EU legal standards have also influenced private sector practices in third countries, as can be seen in the example of data protection law.[144] Among the reasons for such influence are the need to conform to EU standards in order to compete in Europe; the power of the European market; the importance of privacy in the public consciousness; and the need to ensure that EU law is not undermined by lower standards elsewhere.[145]

C. INTERNATIONAL NEGOTIATION

The EU participates actively in a number of international fora dealing with Internet law and regulation. This includes UN-based organisations dealing with Internet governance, such as the IGF; other multilateral organisations, such as the Council of Europe and the OECD; international legal harmonization organisations such as UNCITRAL; and many others. In the scope of such

---

[139] See with regard to the development of rules of customary international law as a process of 'crystallization', H. Thirlway, *The Sources of International Law* (2014), at 66 (Kindle edition).
[140] Kowalik-Bańczyk and Pollicino, 'Migration of European Judicial Ideas concerning Jurisdiction over Google on Withdrawal of Information', 17 *German Law Journal* (2016) 315, at 333.
[141] *Google Spain*, *supra* note 78, at paras. 62-99.
[142] See Kowalik-Bańczyk and Pollicino, *supra* note 140.
[143] *Ibid.*, *supra* note 140, at 335.
[144] See K. Bamberger and D. Mulligan, *Privacy on the Ground* (2015), at 65, noting with regard to a survey of company privacy officers in the US that 'respondents explained that European law plays a large role in shaping such company-wide privacy policies', and that 'the influence of US law was evidenced by specific activities such as Safe Harbor certification'.
[145] Bradford, *supra* note 2, at 24-26; Shaffer, 'Globalization and Social Protection: the Impact of EU and International Rules in the Ratcheting Up of US Privacy Standards', 25 *Yale Journal of International Law* (2000) 1, at 81-88.

participation, the EU exercises its influence, which includes promoting its values and interests. This involves a process of competition against the values and interests of other regions, which can be seen in Internet-related areas such as data protection, where there is often competition between the EU and the US to push their respective views.[146]

EU activity at the international level is also motivated by political factors. For example, during the negotiation of the GDPR, I observed the EU using its influence in the Council of Europe to prevent amendments to Convention 108 from being approved, based on the perception that this would 'steal the thunder' of the EU if reformed data protection rules were adopted at the international level before the EU adopted its GDPR. This shows how EU action in international negotiation can be motivated, at least in part, by the desire to successfully realize its internal legislative projects, and to overshadow similar multilateral projects.

D. COERCION AND CONDITIONALITY

Another approach can be characterized as coercion, meaning pressuring third countries to adopt certain policies through the mechanism of conditionality, i.e., making access to resources or benefits conditional on compliance with the EU's policy requirements.[147] Coercion need not always be viewed negatively, as a polity may legitimately make the granting of legal and political benefits contingent on the meeting of certain conditions. Indeed, the EU makes accession conditional on accepting and implementing the acquis communautaire, which constitutes a form of coercion.[148] More direct exercises of coercion can be seen in actions such as the agreement of Internet companies in 2016 to adopt rules against hate speech following pressure from the Member States and the European Commission.[149]

Another example of this 'carrot and stick' approach is the use of adequacy decisions issued by the European Commission confirming that a third country offers an adequate level of data protection based on EU standards. The EU uses this approach in other areas as well, such as private international law, trade law, and environmental standards.[150] The 'carrot' in this approach is the offer of extending preferential status to third countries once their data protection standards are certified as being 'essentially equivalent' to those of EU law, which is considered to grant economic benefits by allow personal data to be transferred freely to such countries. The 'stick' is the fact that EU law permits the free flow of data to third countries only when they adopt EU standards, and that it is also

[146] See, e.g., Greenleaf, *supra* note 107, at 73, describing attempts by the US government and US companies 'to use their combined economic and political influence to limit the development of data privacy laws in other countries'.
[147] Gilardi, *supra* note 2, at 13 (all citations to online version).
[148] Regarding EU accession as a form of coercion see *ibid.*, at 14.
[149] See *supra* note 132.
[150] See Mills, *supra* note 100, at 542-543.

possible for the European Commission to reach a finding that they do *not* offer adequate protection[151] or that an existing adequacy decision should be repealed, amended, or suspended (though this has never been done).[152]

Providers of Internet data storage services have located their data centres in the EU in order to escape restrictions on international data transfers under EU law. As one news story puts it, global technology giants 'are racing to store their data on the Continent as new laws and privacy concerns drive investment decisions'.[153] Data storage companies also market their services based on having infrastructure located in the EU,[154] and global companies have started aligning their privacy policies with the GDPR.[155] These examples demonstrate the power of EU law to change the behaviour of commercial actors with regard to their Internet activities.

Passing judgment on whether the law of third countries is adequate based on EU standards risks entangling legal analysis with political factors. For example, in July 2010 the government of Ireland delayed an EU adequacy decision for Israel based on alleged Israeli government involvement in the forging of Irish passports.[156] The process of negotiating data protection adequacy assessments has also led to political tensions with third countries.[157]

E. BLOCKING RECOGNITION OF THIRD COUNTRY LEGAL MEASURES

EU law may block recognition of third country legal measures that conflict with its own values. This is a method of extending the global reach of EU law, since it is based on an assertion of EU values in relation to legal measures taken by a third country.

---

[151] Under the Directive 95/46/EC, the Commission may find that a third country does not provide an adequate level of data protection. See Directive 95/46/EC, *supra* note 38, Art. 25(3).
[152] See GDPR, *supra* note 39, Art. 45(5).
[153] Cerullus, 'It's raining cloud storage in Europe', *POLITICO*, 24 November 2016, at 20, <http://www.politico.eu/pro/its-commission-vs-the-market-on-data-flows/>, (last accessed 26 December 2016).
[154] See Martin-Jung, 'Wir sind NSA-Frei', *Frankfurter Allgemeine Zeitung*, 16 November 2016, at 26, in which the European head of Fujitsu states regarding the company's cloud storage services that 'We are located in Germany and have a German infrastructure, we are free of the NSA…' (author's translation).
[155] See Communication from the Commission, *supra* note 95, at 2.
[156] See Ihle, 'Ireland blocks EU data sharing with Israel', *JTA*, 8 July 2010, <http://www.jta.org/2010/07/08/news-opinion/world/ireland-blocks-eu-data-sharing-with-israel> (last visited 16 December 2016). Israel later received an adequacy decision from the European Commission. Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, [2011] OJ L27/39.
[157] See Stoddart, Chan, and Joly, 'The European Union's Adequacy Approach to Privacy and International Data Sharing in Health Research', 44 *The Journal of Law, Medicine & Ethics* (2016) 143 (concerning tensions with Quebec); Mucci, Cerulus, and Von Der Burchard, 'Data fight emerges as last big hurdle to EU-Japan trade deal', *POLITICO*, 9 December 2016, <http://www.politico.eu/article/eu-japan-trade-deal-caught-up-in-data-flow-row-cecilia-malmstrom/> (last visited 16 December 2016).

An example of this is Article 48 of the GDPR, which limits the enforceability of decisions of third country courts and administrative authorities in the EU, and reads as follows:

> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.[158]

This provision is similar to so-called 'blocking statutes'[159] that protect parties in the EU from what are viewed as exorbitant jurisdictional assertions by third countries. For example, French law prohibits the disclosure to foreign public authorities (such as courts or administrative authorities) of data or information if this would impair the important interests of France.[160] Member State data protection authorities have also refused to authorize the use of cross-border data processing networks in the EU when their implementation is based on third country legislation that violates EU data protection standards. In two cases the CNIL refused to authorize the use in France of electronic hotlines for the confidential, anonymous submission of employee complaints (commonly called whistleblowing hotlines) regarding questionable auditing or accounting matters in their operations outside the US, although many US companies regard use of such hotlines as being compelled by the US Sarbanes-Oxley Act.[161]

7. NORMATIVE QUESTIONS

A. INTRODUCTION

EU law does not use a single normative approach to exercise its global reach regarding the Internet. The lack of a comprehensive, overarching approach is not surprising in light of the Internet's relative novelty; the wide variety of EU

---

[158] GDPR, *supra* note 39, Art. 48.
[159] See regarding blocking statutes in general, Basedow, *supra* note 1, at 334-342; D. Cooper and C. Kuner, 'Data Protection Law and International Dispute Resolution', 382 *Recueil des cours/Collected Courses of the Hague Academy of International Law* (2017) (forthcoming).
[160] Loi n° 80-538 du 16 juillet 1980 relative à la communication de documents ou renseignements d'ordre économique, commercial ou technique à des personnes physiques ou morales étrangères.
[161] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 301(4)(A), (B). See regarding these two cases, Dowling, 'Sarbanes-Oxley Whistleblower Hotlines Across Europe: Directions Through the Maze', 42 *International Lawyer* (2008) 1.

institutions and legal instruments that deal with it; and the fragmented landscape of norms and actors involved in its governance and regulation. This accords with the general view that the manifestations of the global impact of EU law vary based on factors such as how difficult they are to realize and how significant they are.[162]

However, there is no doubt that in recent years the EU has made use of the increased legal powers available to it under the Treaty of Lisbon and the Charter of Fundamental Rights to extend its reach to Internet activities beyond its borders, as demonstrated by the growing number of legislative and regulatory initiatives adopted in recent years (e.g., the GDPR), and the increased willingness of the Court of Justice to assert EU values in its case law dealing with Internet-related topics (e.g., *Google Spain* and *Schrems*). In this regard, the Internet has served as a vehicle allowing EU law to assert itself in the wider world. The increasing global reach of EU law as it concerns the Internet raises some important normative questions that are dealt with below.

B. EU VALUES OR EU INTERESTS?

As described earlier,[163] in its external action the EU must uphold and promote its 'values', which the TEU lists as 'human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities'.[164] These are described later on in the TEU as the principles which the EU 'seeks to advance in the wider world',[165] and together seem to represent the core values of EU law.

However, in its external action the EU must also be guided by other concepts that are more political in nature. Thus, in its relations with the wider world the EU is required to uphold and promote its 'interests',[166] to define and pursue its 'common policies and actions',[167] and to safeguard its 'fundamental interests'.[168] As stated above, the Council is obliged to identify the EU's 'strategic interests' in the context of external action.[169] The TEU does not define these terms or state what the difference is (if any) between them.

The influence of legal values when the EU exerts its global reach can be seen in the judgments of the Court of Justice in Internet-related cases, and in EU legislation such as the GDPR. The influence of political factors can be seen in the following statement by the European Commission concerning the adoption of adequacy decisions covering the level of data protection in third countries:

---

[162] See Young, *supra* note 2, at 1237.
[163] See *supra* section 4A.
[164] TEU, *supra* note 8, at Art. 2.
[165] *Ibid.*, at Art. 21(1).
[166] *Ibid.*, at Art. 3(5).
[167] *Ibid.*, at Art. 21(2).
[168] *Ibid.*, at Art. 21(2)(a).
[169] See *supra* note 31.

> Under its framework on adequacy findings, the Commission considers that the following criteria should be taken into account when assessing with which third countries a dialogue on adequacy should be pursued:
>
> (i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
>
> (ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
>
> (iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
>
> (iv) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.[170]

It is not clear how basing a decision to initiate adequacy discussions with third countries on factors that are obviously political in nature is consistent with the insistence by the Court of Justice in *Schrems* that the Commission's discretion with regard to the adequacy of protection ensured by a third country 'is reduced', and that its review of the requirements stemming from EU data protection law and the EU Charter of Fundamental Rights should be 'strict'.[171] It seems that the EU would like to have its cake and eat it too by having one institution (the Court of Justice) insist on strict legal standards for adequacy decisions, while another one (the Commission) prioritizes discussions with third countries based on political factors. The entanglement of EU legal values with the EU's political interests can also be seen in the way the Court of Justice has defined the territorial scope of EU law on the Internet largely in terms of the policy objectives that the law seeks to pursue.[172]

The increasing importance of the Internet means that it is bound to become the subject of political disputes. However, as legal values become enmeshed with political considerations, or as the latter are presented as the former, the core values of EU law are diluted, and it becomes more difficult to develop a coherent normative basis for EU law as it relates to the Internet, particular when EU values are advanced as universal values.[173] The various political concepts that the EU is supposed to promote in its external action require further clarification, and their role should be more clearly distinguished from that of fundamental EU legal values. As the EU increasingly asserts its global reach regarding Internet-related issues, it will be important for it to differentiate between legal and political values, and to be more honest about when each applies and for what reason.

---

[170] Communication from the Commission, *supra* note 95, at 8.
[171] *Schrems*, *supra* note 69, at para. 78.
[172] See *infra* section 7E.
[173] See *infra* section 7C.

C. EU LAW AS UNIVERSAL VALUES

The EU increasingly asserts its values as universal, global standards for the Internet. This can be seen in the words of some of the leading figures involved in the adoption of the GDPR:

- Former EU Commissioner Viviane Reding: 'Europe must act decisively to establish a robust data protection framework that can be the gold standard for the world'.[174]
- MEP Jan-Philipp Albrecht, Rapporteur in the European Parliament for the GDPR: The GDPR will change 'nothing less than the whole world as we know it'.[175]
- An unnamed EU official: 'With these proposals, the EU is becoming the de facto world regulator on data protection'.[176]

In a lengthy newspaper interview following the *Schrems* judgment, President of the Court of Justice Koen Lenaerts left no doubt about the leading role which he believes EU law should play in the wider world:

> Europe must not be ashamed of its basic principles: The rule of law is not up for sale. It is a matter of upholding the requirements in the European Union, of the rule of law, of fundamental rights. If this is also affecting some dealings internationally, why would Europe not be proud to contribute its requiring standards of respect of fundamental rights to the world in general?[177]

EU law has arisen in a unique constitutional and institutional context,[178] which gives rise to a paradox: if EU law is unique and fundamentally different from other legal systems, then how can it be replicated elsewhere, and how can third countries be expected to adopt it? Many third countries have adopted legislation close to the EU model in areas such as data protection, but few have been found to have laws that are adequate and thus essentially equivalent to EU standards. Whether a norm

---

[174] See Reding, 'A data protection compact for Europe', 28 January 2014, available online at <http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm> (last visited 13 November 2016). See also Kuner, 'The European Union and the Search for an International Data Protection Framework', 2 *Groningen Journal of International Law* (2014) 55, at 57.

[175] Albrecht, 'How the GDPR will change the world', 3 *European Data Protection Law Review* (2016) 287, at 287.

[176] See T. Vogel, 'Reding seeks overhaul of data protection rules', *European Voice*, 15 December 2011, available online at <http://www.europeanvoice.com/article/reding-seeks-overhaul-of-data-protection-rules/> (last visited 13 November 2016).

[177] Popp, 'ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust', *The Wall Street Journal*, 14 October 2015, <http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/tab/print/> (last visited 10 November 2016).

[178] See, e.g., Rosas and Armati, *supra* note 35, at 4 (referring to 'the unique nature of the EU as a legal and constitutional order') and 12 (referring to the EU as 'a unique organisation') (Kindle edition).

is based on a fundamental legal value or on a political interest also affects the ability to assert it as being global or universal, since it would be unreasonable to expect third countries to accept the EU's political interests as universal values.

When a legal system strives for its standards to be accepted as universal values, it is inevitably engaged in a hegemonic struggle in which it seeks to have its own interests identified with the general interest.[179] The EU is engaged in such a struggle, as can be seen in the area of data protection, where the Commission cloaks efforts to promote the spread of EU law in the language of encouraging third countries and international organisations to adopt strong data protection standards.[180]

The promotion of EU law as a set of universal values can also backfire when third countries take the same approach towards the EU regarding their own law. As globalization proceeds, more countries are likely to insist on compliance with their legal requirements concerning conduct on the Internet. This can involve, for example, a third country allowing data transfers to the EU only when it (i.e., the EU) provides adequate protection based on third country law. Indeed, such requirements already exist in the provisions of some third country data protection laws that allow international data transfers only when the country to which data are transferred provides adequate protection.[181] Insisting on reciprocity on the part of the EU is logical from the point of view of third countries, and is a consequence of the EU's assertion of its own standards towards third countries. The EU should thus keep in mind the possibility of its own global reach mechanisms being imitated and used against it.

D. DIVERGENCE BETWEEN THEORY AND PRACTICE

There is an important distinction between the spread of EU legal values and their protection in practice. For example, the fact that EU data protection law has influenced the adoption of data protection legislation around the world does not necessarily mean that this has led to a higher level of data protection on the

---

[179] See Koskenniemi and Leino, 'Fragmentation of International Law? Postmodern Anxieties', 15 *Leiden Journal of International Law* (2002) 553, at 561-562.

[180] See Communication from the Commission, *supra* note 95, at 10, where the Commission states that it will 'work with and assist countries interested in adopting strong data protection laws and support their convergence with EU data protection principles'; *ibid.*, at 12, where the Commission supports the 'swift adoption' of the modernized text of Council of Europe Convention 108 since the Convention 'will reflect the same principles as those enshrined in the new EU data protection rules and thus contribute to the convergence towards a set of high data protection standards;' and *ibid.*, at 16, stating that the EU will actively engage with third countries to explore adequacy findings 'with a view to fostering regulatory convergence towards the EU standards…'.

[181] See, e.g., Angola, Law no. 22/11 on the Protection of Personal Data, Art. 33; Economic Community of West African States (ECOWAS), Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (16 February 2010), Art. 36; Japanese Act on the Protection of Personal Information (as amended 2015), Art. 24; Macau Special Administrative Region (MSAR) of the People's Republic of China, Personal Data Protection Act (Act 8/2005), Art. 19. See also C. Kuner, *Transborder Data Flows and Data Privacy Law* (2013), at 65-66.

Internet. Determining the extent to which EU values are actually reflected in practice on the Internet would require a large-scale empirical study that has yet to be conducted.

EU law focuses on application of its norms to the Internet in a legal sense (e.g., the application of EU law to Internet-related activities, or the adoption by third countries of law based on EU models), rather than on an evaluation of whether the legal values that the EU seeks to export are upheld in practice. An example of this phenomenon can be seen in the proposed ePrivacy Regulation,[182] Article 3(2) of which requires parties not established in the EU that provide electronic communications services (i.e., many types of web sites, services that use connected devices, etc.) to users in the EU to designate a 'representative in the Union' in writing. The proposed Regulation describes the duties of representatives, but contains no details about how they should be appointed, what liability they have, and other important practical points. This proposal mirrors the system of representatives mandated in Directive 95/46/EU for data controllers not established in the EU,[183] which has also never been practically implemented.[184] There are well over 1 billion web sites on the Internet,[185] not even counting the many other types of services covered by the proposed Regulation, and the resources necessary for establishing and policing a system for the appointment and registration of representatives on such a huge scale would seem to be far beyond the capabilities of any EU or Member State institution. These provisions thus seem to be a textbook example of regulatory overreaching, i.e., of law being applied so broadly that it stands little chance of being enforced.[186]

In order for the application of EU law to be meaningful, it must be effective in practice as well as apply on paper, as the Court of Justice has recognized. For example, the CJEU in *Schrems* emphasized that protections provided for personal data transferred from the EU to third countries must 'prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union'.[187] EU law should put greater emphasis on determining not only whether its standards apply to Internet activity in a legal sense, but on whether the values that underlie them are fulfilled in practice. The first steps toward such an approach can be found in the annual review foreseen in the EU-US Privacy Shield, though the depth and scope of the review remain to be seen.[188]

---

[182] ePrivacy Regulation, *supra* note 40.
[183] See Directive 95/46/EC, *supra* note 38, Art. 4(2).
[184] See C. Kuner, *European Data Protection Law* (2007), at 133-134.
[185] See <http://www.internetlivestats.com/total-number-of-websites/> (last visited 11 January 2017).
[186] See Bygrave, *supra* note 107, at vi (Kindle edition).
[187] *Schrems*, *supra* note 69, at para. 74. See also paras. 39 (referring to the need for 'effective and complete' protection), 41 (referring to the importance of ensuring the 'effectiveness' of monitoring of compliance with the law by DPAs), and 81, 89, 91, and 95 (in which the Court stresses the need for protection of the fundamental right to data protection to be 'effective').
[188] See Commission Implementing Decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C(2016) 4176 final, OJ 2016 L2017/1, Recital 146. See also Communication from the

E. THE TERRITORIAL SCOPE OF EU LAW

The Internet raises questions about how the EU should act with regard to conduct that occurs outside its borders but has an effect within them.[189] It is easier to state that EU law should be given wide territorial application when important public policy interests are at stake[190] than to determine what the limits of such application are.

EU law adopts a schizophrenic attitude to the territorial application of law on the Internet. On the one hand, the EU and its Member States insist on limits to jurisdiction based on sovereignty when jurisdictional assertions against the EU by third countries are involved; this can be seen, for example, in the insistence by the EU and the Member States on using the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the Hague Evidence Convention)[191] as the exclusive means for discovery of evidence abroad,[192] and the enactment in some Member States of so-called blocking statutes[193] that restrict compliance with the extraterritorial scope of foreign discovery requirements. On the other hand, judgments such as *Google Spain* and *Schrems* demonstrate that EU law applies broadly to actions by third countries when this is necessary to defend EU substantive legal standards.[194]

The Court's current approach to defining the territorial scope of EU law on the Internet is largely based on the policy objectives that the law seeks to pursue. For example, the result of the Court's *Google Spain* judgment has been described as follows: 'the (territorial) scope of application of EU secondary law is determined by its policy objectives: a direct correlation can be established between the achievement of EU policies and the potential need to cover situations located in third states'.[195] The greater the paucity of guidance by the legislator as to the territorial scope of law, the higher the risk that courts will be left to determine it based on their interpretation of the EU's policy objectives of the moment.[196] Such a consequentialist approach risks sacrificing the coherence and consistency that are inherent in a legal (rather than a political) method of interpretation, and may result in the entanglement of legal values and political interests that has already been

---

Commission, *supra* note 95, at 9, stating with regard to adequacy decision that in the future, '[p]eriodic reviews will be held, at least every four years, to address emerging issues and exchange best practices between close partners'.

[189] See *supra* section 5E.

[190] See Jääskinen and Ward, *supra* note 131, at location 5246 (Kindle edition).

[191] Signed at The Hague, 18 March 1970, 847 UNTS 231.

[192] See Article 29 Working Party, 'Working Document 1/2009 on pre-trial discovery for cross border civil litigation' (WP 158, 11 February 2009), at 14. See also GDPR, *supra* note 39, Art. 48.

[193] For example, in France. See Loi n° 80-538 du 16 juillet 1980, *supra* note 160.

[194] See Cremona and Micklitz, *supra* note 81, at location 1523 (Kindle edition).

[195] S. Francq, 'The External Dimension of Rome I and Rome II: Neutrality or Schizophrenia?', in M. Cremona and H.-W. Micklitz (eds), *Private Law in the External Relations of the EU* (2016) location 3283, at location 3813 (Kindle edition).

[196] Jääskinen and Ward, *supra* note 131, at location 5253.

discussed below.[197]

EU law is still searching for a paradigm for its application to the Internet that is based on firm legal principles, secures the rights of EU individuals, and avoids jurisdictional overreach. That some limits to jurisdiction must exist is indicated by the Court of Justice's *Air Transport Association of America*[198] judgment, where it found that EU law should not apply to aircraft registered in third countries that fly over third countries or the high seas, but that it can exercise jurisdiction when an aircraft arrives or departs from a Member State.[199] This judgment indicates the outlines of a jurisdictional approach to the Internet as well, i.e., to avoid applying EU law to parties and situations outside its borders that have no contact or connection with the EU, but to extend its application to situations that have effect in the EU or on EU individuals. Of course, the application of such an approach would depend on resolving difficult questions such as what constitutes a sufficient contact or connection to justify the assertion of EU law, and what it means for conduct to have 'effects' regarding the EU. It will be up to the Court of Justice to define these parameters in greater detail as cases involving the Internet are brought before it or referred to it, which will no doubt happen with increasing frequency.

F. RESPONSIBILITIES TOWARDS THIRD COUNTRIES

In examining the global reach of EU law, the focus has almost invariably been on the degree of influence of EU law, i.e., on the power exercised by the EU. But along with influence and power goes responsibility, and this raises the question of whether the EU has responsibilities to third countries that adopt its standards. The existence of such responsibilities, particularly towards developing countries, finds support in the TEU, which requires the EU to foster 'the sustainable economic, social and environmental development of developing countries, with the primary aim of eradicating poverty'.[200] The Internet can be seen as a vehicle for fostering the economic and social development of third countries, and thus may be viewed as falling within this provision. Raising EU legal norms to the status of universal norms[201] also strengthens the case for the EU to assume greater responsibility for their effects when they are asserted globally.

EU law has been willing to exert its influence on third countries, but less inclined to learn from them. For example, the following has been stated regarding the judicial dialogue between the EU courts and courts in third countries:

---

[197] See *supra* section 7B regarding the entangelement of EU values and political interests. See also G. Beck, *The Legal Reasoning of the Court of Justice of the EU* (2012), at 119 (Kindle edition).
[198] Case C-366/10, [2011] (ECR-I-13755).
[199] *Ibid.*, at paras. 122-127.
[200] TEU, *supra* note 8, at Art. 21(2)(d).
[201] See *supra* section 7C.

> The European courts seem more inclined 'to teach' rather than 'to learn' when discussing the protection, *erga omnes* (towards everyone), of European constitutional values, even beyond the reaches of Europe. In other words, the European judicial dialogue remains European-value-based even when globalized.[202]

There is a growing realisation that 'as agents of humanity, sovereigns are obligated to take other-regarding considerations seriously into account in formulating and implementing policies…'.[203] It seems reasonable to conclude that this principle should also apply when one legal system exercises influence over others, particularly when it aims to have its values adopted as global standards. The global reach of EU law should not be purely a matter of power politics, i.e., of the EU seeing how far it can extend its influence towards third countries, but should subject it to responsibilities as well. These responsibilities are especially compelling with regard to developing countries, towards which there is a well-documented history of hegemony on the part of European legal systems.[204]

The EU's responsibilities towards third countries can be seen in the example of EU data protection law. 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 based on EU standards with all that entails can be a significant burden on their resources.[205] The GDPR is considerably longer and more complex than the Directive 95/46/EC that it will replace, and adopting data protection legislation that is essentially equivalent to the GDPR, or revising existing legislation to meet this standard, will require third countries to invest in a large-scale legislative project that could take many years.

If EU law is to be the 'de facto standard for the world', then the EU has certain responsibilities towards other countries that adopt it. Setting up EU law as an influential standard on a global basis should involve more than simply motivating other countries to adopt it and then leaving them to their own devices. Recognition of such responsibilities would ultimately be in the EU's own interest, since it would provide additional incentives for other countries to adopt EU law. The EU should thus implement measures to consider the effect on third countries of its rules, and to provide a mechanism for them to obtain information about EU law quickly and easily. This could include measures such as establishing an Internet portal with information on EU legal developments with particular

---

[202] Kowalik-Bańczyk and Pollicino, *supra* note 140, at 333.
[203] Benvenisti, 'Sovereigns as trustees of humanity: on the accountability of states to foreign stakeholders', 107 *American Journal of International Law* (2013) 295, at 300.
[204] See, e.g., M. Koskenniemi, *The Gentle Civilizer of Nations* (2001), at Chapter 2; Nunn, 'Law as a Eurocentric Enterprise', 15 *Law and Inequality* (1997) 323.
[205] See Madhub, 'The pioneering journey of the Data Protection Commission of Mauritius', 3 *International Data Privacy Law* (2013) 239, at 241-242.

relevance to third countries, and soliciting input from third countries to learn about the impact of EU law on them. The increased interaction with third countries produced by such measures could also benefit the EU by illuminating areas where it could learn from third country law, a possibility that the Commission seems to accept as far as data protection is concerned.[206]
Finding that the EU has certain responsibilities towards third countries that are influenced by its law raises another question, namely whether in applying its law to third countries the EU is setting standards for them that it is not prepared to live up to itself. Strictly speaking, the standards of EU law and those of third country law are two different matters, but in a moral sense, the legitimacy of EU law is undermined if the EU is viewed as holding third countries to higher standards than it is obligated to meet.

An example can be seen in the *Schrems* judgment, where the Court of Justice held the conclusion of adequacy decisions by the European Commission regarding the level of data protection in third countries to a high standard, particularly regarding access to data by third country intelligence authorities. However, Article 4 TEU grants competence for national security to the Member States, and there is widespread sharing of information by intelligence agencies of the Member States with third countries such as the US, both under the 'Five Eyes'[207] intelligence-sharing network (which includes Australia, Canada, New Zealand, the UK, and the US), and under bilateral arrangements involving Member States such as France[208] and Germany.[209] Thus, there are substantial gaps in legal protection against intelligence surveillance under EU law, which undermines the moral legitimacy of criticisms of third country standards. It would increase the influence of EU law on the international stage if the EU were to ensure that it can itself satisfy the standards that it expects third countries to meet.

G. IS THE INTERNET CHANGING EU LAW?

A final consideration is whether the influence that EU law has on the Internet is reciprocal, i.e., whether the Internet is also changing EU law. The Internet forces legal systems to take account of what happens beyond their borders, and it is

---

[206] Communication from the Commission, *supra* note 95, at 12, stating 'the EU can benefit from the exchange of best practices and the experience of other systems with new challenges for the protection of privacy and emerging legal or technical solutions, including as regards enforcement, compliance tools (e.g. certification mechanisms, privacy impact assessments) or the protections for certain specific data sets (e.g. children's data)'.
[207] See regarding the Five Eyes alliance, G. Greenwald, *No Place to Hide* (2014), at locations 1581, 1854-1900 (Kindle edition).
[208] See Root, 'French intelligence involved in NSA spying in France', *Bloomberg News*, 29 November 2013, <http://www.bloomberg.com/news/articles/2013-11-29/french-intelligence-involved-in-nsa-spying-in-france-monde-says> (last visited 19 December 2016).
[209] See 'Geheimdienst-Kooperation: BND leitet seit 2007 Daten an die NSA weiter', *SPIEGEL ONLINE*, 8 August 2013, <http://www.spiegel.de/netzwelt/netzpolitik/geheimdienste-bnd-leitet-seit-2007-daten-an-die-nsa-weiter-a-915589.html> (last visited 19 December 2016).

possible that this engagement with developments in third countries can itself cause changes in EU law.

In fact, there is evidence that this is already happening with regard to the role of the Court of Justice. The Court's role is to serve as 'the ultimate authority for deciding any question concerning the interpretation or validity of EU law',[210] and in theory it does not pass judgment on the law of third countries.[211] In the interview he gave following the *Schrems* judgment, President Lenaerts stated about the judgment that 'We are not judging the U.S. system here, we are judging the requirements of EU law in terms of the conditions to transfer data to third countries, whatever they be'.[212]

However, it is surely disingenuous to claim that the *Schrems* case did not involve evaluation of third country legal standards. The judgment is based on an examination of US intelligence gathering practices and their effect on fundamental rights under EU data protection law,[213] as can be seen, for example, in the Court's mention of studies by the European Commission finding that US authorities were able to access data in ways that did not meet EU legal standards in areas such as purpose limitation, necessity, and proportionality.[214] The need to review third country standards is logically inherent in an evaluation of whether a Commission decision based on those standards results in protection that is essentially equivalent to that under EU law.

The need for the Court to review third country standards can also be seen in the opinions of Advocate General Bot in the *Schrems* case[215] and Advocate General Mengozzi in *Opinion 1/15*[216] (the latter case is based on a request for an opinion by the European Parliament concerning a draft agreement between the EU and Canada for the transfer of airline passenger name records). The opinion of Advocate General Bot contains an evaluation of questions of US law, such as whether limits on the supervisory powers of the US Federal Trade Commission (FTC) allow it to be considered an 'independent authority' under EU legal standards.[217] In *Opinion 1/15*, Advocate General Mengozzi indicated that some provisions of Canadian law had been brought before the Court,[218] and that some

---

[210] Beck, *supra* note 197, at 225 (Kindle edition).
[211] See *Opinion 1/15*, Opinion of Advocate General Mengozzi, 8 September 2016 (ECLI:EU:C:2016:656), at para. 163, stating 'the Court cannot express a view on the legislation or the practice of a third country…'.
[212] Lenaerts interview, *supra* note 177.
[213] See *Schrems*, *supra* note 69, at para. 93, where the Court seems to imply that data transferred to the US are subject to undifferentiated storage, access, and use.
[214] *Ibid.*, at para. 90.
[215] *Schrems*, Case C-362/14, Opinion of Advocate General Bot, 23 September 2015 (ECLI:EU:C:2015:627).
[216] See *supra* note 211.
[217] *Schrems*, Opinion of Advocate General Bot, *supra* note 215, at paras. 207-208.
[218] *Opinion 1/15*, Opinion of Advocate General Mengozzi, *supra* note 211, at para. 320, stating 'However, there is no reference in the agreement envisaged to the existence of that administrative appeal to the Canadian Privacy Commissioner, nor is its existence apparent from any provision of Canadian law brought to the knowledge of the Court'.

of the contentions of the parties required interpretation of issues of Canadian law.[219]

In its *Schrems* judgment, the Court virtually ordered national courts to make preliminary references of cases involving the adequacy of data protection in third countries to it,[220] so that there are likely to be an increasing number of such cases. Indeed, the Commission has indicated that in the future it will consider issuing additional adequacy decisions, including ones covering countries in regions such as East and South-East Asia that will pose difficult questions of comparison with EU law.[221] In addition, *Opinion 1/15* was not a preliminary reference but a request for an opinion submitted by the European Parliament under Article 218(11) TFEU, demonstrating the variety of cases in which the Court may need to deal with the law and legal standards of third countries.

The increased rapidity and volume of international communications caused by the Internet has led to increased complexity of international disputes and a greater need to take foreign law into account when resolving them. It thus seems that the Internet is changing the role of the Court by leading it to evaluate foreign legal systems in the course of answering questions of EU law. It is not apparent what would prevent the Court from considering foreign legal standards when that is inherently necessary to resolve the issues of EU law before it, aside from its traditional avoidance of referring to comparative and international law in its judgments.[222] Even if considering foreign legal standards goes beyond the Court's traditional role, it is important that it be openly acknowledged so that its function can be properly understood. However, the implications of this change need not be exhaustively explored here; for the purposes of this chapter, the main point is that the Internet is causing changes to a key element of EU law, namely the role of the Court of Justice.

The Internet is evolving rapidly, and the way that it interacts with EU law will no doubt change as well. At present, EU law has had significant influence on the Internet, but the Internet also poses a number of challenges for EU law. Thus, the story of the interrelationship between EU law and the Internet will continue to change to reflect both the values and interests of the EU, and nature of the Internet as a social, cultural, and legal phenomenon.

---

[219] *Ibid.*, at para. 156, mentioning a contention by the Council and the Commission that the international agreement in question between Canada and the EU 'reflects the obligation which the Canadian Constitution imposes on all Canadian public authorities to comply with a court order'.
[220] *Schrems*, *supra* note 69, at paras. 64-65.
[221] See Communication from the Commission, *supra* note 95, at 8.
[222] See de Búrca, 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?', 20 *Maastricht Journal of European and Comparative Law* (2013) 168, at 183.