doi:10.1017/aju.2019.80

SYMPOSIUM ON THE GDPR AND INTERNATIONAL LAW

THE GDPR AS *GLOBAL* DATA PROTECTION REGULATION?

Cedric Ryngaert[*] *& Mistale Taylor*[**]

The deterritorialization of the Internet and international communications technology has given rise to acute jurisdictional questions regarding who may regulate online activities.[1] In the absence of a global regulator, states act unilaterally, applying their own laws to transborder activities. The EU's "extraterritorial" application of its data protection legislation—initially the Data Protection Directive (DPD) and, since 2018, the General Data Protection Regulation (GDPR)—is a case in point.[2] The GDPR applies to "*the processing of personal data* of data subjects who are in the Union *by a controller or processor not established in the Union*, where the processing activities are related to: (a) the offering of goods or services . . . to such data subjects in the Union; or (b) the monitoring of their behaviour . . . within the Union."[3] It also conditions data transfers outside the EU on third states having adequate (meaning essentially equivalent) data protection standards.[4] This essay outlines forms of extraterritoriality evident in EU data protection law, which could be legitimized by certain fundamental rights obligations. It then looks at how the EU balances data protection with third states' countervailing interests. This approach can involve burdens not only for third states or corporations, but also for the EU political branches themselves. EU law viewed through the lens of public international law shows how local regulation is going global, despite its goal of protecting only EU data subjects.

Bases for Extraterritoriality

In 2014, the Court of Justice of the EU (CJEU) famously applied EU data protection legislation to a foreign service provider in the *Google Spain* case. It found the DPD applicable to Google, a U.S. company, on specific

* *Professor of Public International Law, Utrecht University (RENFORCE research programme).*

** *Senior research analyst, Trilateral Research, Ireland.*

[1] The Net and the Nation State (Uta Kohl ed., 2017); Dan Jerker B. Svantesson, Solving the Internet Jurisdiction Puzzle (2017).

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L. 281) 31; 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), 2016 O.J. (L 199) 1 [hereinafter GDPR].

[3] GDPR, *supra* note 2, art. 3(2) (emphasis added).

[4] *Id.*, art. 45(1) ("A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.").

grounds, in part because Google had an establishment in an EU member state.[5] The case confirmed a data subject's right to erasure ("right to be forgotten"), which could have notable ramifications for internet users beyond EU territory. The GDPR reinforced this broad reach of EU data protection law.

The "extraterritorial" application of EU data protection law nevertheless has identifiable jurisdictional bases under public international law. First, the long arm of EU data protection law, with its attendant extraterritorial impact, is arguably based on territoriality, as it is triggered by a territorial link of an activity or person with the EU. Under the GDPR, territoriality may even be the key principle, where application of the Regulation to entities not based in the Union is triggered by their targeting or monitoring those "in the Union." In the literature, this process has usefully been termed "territorial extension."[6] Second, the broad geographic reach of EU data protection legislation appears to be related to individual rights premised on someone's demonstrable affiliation to the EU, which would ordinarily be citizenship or residence. Thus, the EU's assertions may be justifiable under the passive personality principle, which allows the EU to protect EU citizens or residents, e.g., in the context of transfers of EU subjects' data to substandard jurisdictions. Often, in fact, the EU's assertions are based on a combination of the territoriality and the passive personality principles, as illustrated by the fact that a data subject needs to show a "terri-national" affiliation to the EU when filing a request with a website to erase her data.

Fundamental Rights Considerations

The law of jurisdiction normally operates on the basis of permissions. For EU data protection, this means that the EU may be *permitted* to extend the geographic scope of EU law on the basis of territoriality or passive personality. However, on closer inspection, as data protection rises to the level of a *fundamental right*, the EU's exercise of jurisdiction may not just be permissive (discretionary), but also *mandatory*. The character of data protection as a fundamental right may create particular obligations for the EU to protect the right to data protection extraterritorially. It is of note in this respect that, unlike international human rights treaties such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights (ECHR), the EU Charter on Fundamental Rights does not have a limiting jurisdictional clause.[7] Instead, the geographical scope of a fundamental right laid down in the Charter, such as data protection (Article 8), follows the scope of the EU's competences and the application of EU law.[8] The absence of a jurisdictional clause may pose fewer doctrinal limitations to the extraterritorial application of the Charter. Thus, it may inform the application of a "control" standard that is more relaxed as compared to the control standards used by, notably, the European Court of Human Rights to delineate the extraterritorial application of the ECHR.

Given the "virtual" nature of threats to data protection, the application of a functional "virtual" control standard may be apt.[9] Arguably, the EU incurs extraterritorial obligations when it exercises virtual control over an EU resident's data. This means that, insofar as the EU has the capacity to influence how data are treated abroad, it should harness this influence to have an EU data subject's data respected and protected. The EU should refrain from giving assistance to (extraterritorial) third parties' breaches (duty to respect) and should prevent such parties from

[5] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317, paras. 55–56 (Eur. Ct. Justice, May 13, 2014).

[6] *See* Joanne Scott, *Extraterritoriality and Territorial Extension in EU Law*, 62 Am. J. Comp. L. 87 (2014).

[7] Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1 (Dec. 18, 2000).

[8] Violeta Moreno-Lax & Cathryn Costello, *The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model*, *in* The EU Charter of Fundamental Rights: A Commentary 1662 (Steve Peers et al. eds., 2014).

[9] Peter Margulies, *The NSA in the Global Perspective: Surveillance, Human Rights and International Counterterrorism*, 82 Fordham L. Rev. 2137 (2014).

https://doi.org/10.1017/aju.2019.80 Published online by Cambridge University Press

committing breaches (duty to protect). This implies that the EU should construe EU data protection legislation in such a way that it safeguards the EU subjects' fundamental right to data protection against encroachment by third states and third state-based operators.

Foregrounding Data Protection

In practice, the EU may need to make sure that decisions and agreements on the transfer of data from the EU to third countries contain adequate data protection guarantees, or that foreign-based data controllers and processors targeting EU residents sufficiently protect the latter's data. All this may also explain why the CJEU has, in a string of well-known rulings with a transatlantic dimension, such as *Schrems,*[10] *Canada-EU PNR*,[11] and *Google Spain*,[12] so strongly emphasized the right to data protection over countervailing interests, such as security and the free flow of information. The CJEU thereby forced the EU to renegotiate agreements with third countries or forced foreign-based data controllers targeting the EU market to enhance the protection of EU residents' data. This trend looks set to continue. Pending and recent rulings cover questions on the reach of EU data protection jurisdiction abroad. One such request asks jurisdictional questions about which EU data protection supervisory authority may institute proceedings against, for instance, Facebook.[13] Another recent case pertained to the question of whether de-referenced Google links should be de-referenced across the EU or the global internet; should only those in the EU see redacted search results or should everyone—no matter from where they access Google—see redacted results?[14] The CJEU ruled that the scope of the DPD and GDPR did not require search engine operators to carry out de-referencing on all versions of the search engine.[15] Such broad de-referencing is not, however, prohibited.[16] The Court thus largely restrained its exercise of jurisdiction over foreign companies rather than foregrounding data protection at the expense of other important considerations.

Burdens and Pushback

While fundamental rights-inspired interpretations of data protection legislation may be welcome from an EU citizen's or resident's perspective, they may create additional and possibly unwelcome burdens for the EU political branches. These interpretations exert pressure on EU institutions not to neglect the protection of EU residents' data when entering into data transfer agreements with third countries or when allowing foreign operators to carry out commercial activities on the EU market.[17] In addition, and more importantly from a classic jurisdictional

[10] Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Eur. Ct. Justice, Oct. 6, 2015).

[11] Opinion 1–15 on Draft EU-Canada PNR Agreement, ECLI:EU:C:2017:592 (Eur. Ct. Justice, July 26, 2017).

[12] *Google Spain*, *supra* note 5.

[13] Brussels Court of Appeal, Facebook Ireland Ltd., Facebook Inc. and Facebook Belgium B.V.B.A. v. Belgian Data Protection Authority (DPA) 2018/AR/410, May 8, 2019 (considering the jurisdictional question of whether the Belgian DPA had the competence to initiate enforcement action against Facebook for violating EU data protection law, a case now before the CJEU). Initially, Facebook Belgium and, by extension, the Belgian authorities were found to have the required "inextricable link" to Facebook, but now it is contested that the Irish supervisory authority should initiate such a case because Facebook has its principal EU establishment there).

[14] Case C-507/17, Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 (Eur. Ct. Justice, Sept. 24, 2019), in which the French DPA had fined Google for not de-referencing globally links to websites about EU subjects who had successfully requested this de-referencing.

[15] *Id.* at para. 73.

[16] *Id.* at para. 72.

[17] Concerns over casting the net of human rights beneficiaries too wide, and thereby overburdening the state encumbered with extra-territorial obligations, have been central to the debate on the geographical scope of human rights treaties. *See* Samantha Besson,

https://doi.org/10.1017/aju.2019.80 Published online by Cambridge University Press

perspective, the "extraterritoriality" of EU data protection legislation, or rather its territorial extension, risks conflicts with third countries. Such countries may claim that they have an equally strong or even stronger link to a situation than the EU does. For instance, the United States may claim that it is entitled, on territorial security grounds, to request information about passengers boarding aircraft bound for the United States. It is not self-evident that the EU, in wishing to adequately protect these passengers' data, necessarily has the stronger jurisdictional link. Ultimately, the EU-U.S. stand-off over these records was "solved" on the basis of a passenger names records (PNR) agreement (which may, strictly speaking, however fall foul of EU data protection law given the concessions made by the EU). Even if it considers a data transfer agreement with a third country unlikely,[18] it is in any event advisable for the EU to take into account the legitimate interests of third countries. This mitigation exercise may be walking a fine line because the EU is required to guarantee the protection of EU residents' data, even in an extraterritorial context.

As it happens, data protection is a field in which unilateral assertions of jurisdiction have not often met with foreign sovereign protest. This state of affairs may raise the impression that such assertions are considered lawful and reasonable. An explanation for the absence of foreign sovereign protest is that such assertions are often brought to bear on private operators controlling and processing data. Typically, these operators have strong economic clout and may be viewed by foreign governments as being able to fend for themselves. That is, they are able to protest unlawful or unreasonable jurisdictional assertions on their own, without foreign sovereign intervention. Similar dynamics have been at play in the field of sanctions law, where European governments have sometimes left "their" corporations to their own devices when confronted with U.S. secondary boycotts.[19] Doctrinally speaking, however, private actors' protest about a state's or the EU's jurisdictional assertion does not "count" for the determination of the lawfulness of such assertions under customary international law. After all, for customary law to crystallize, *state* practice is required. Nevertheless, there are some instances of states—notably the United States—voicing concerns over the extraterritoriality of EU data protection legislation, although it is not always clear whether its concern amounts to protest on legal grounds. For instance, while the United States undeniably resisted the EU's attempts to apply EU data protection law to the PNR transfer from the EU to the United States, it is doubtful whether this resistance was based on a U.S. perception that the application of EU law to PNR amounted to an unlawful exercise of prescriptive jurisdiction. Similarly, with respect to data transfers, while the United States may have opposed the inclusion of strong EU-style data protection norms in the U.S.-EU Safe Harbor and its post-*Schrems* Privacy Shield,[20] it may not necessarily have viewed the extension of EU law to U.S.-bound data transfers as unlawful.[21]

The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amounts to, 25 LEIDEN J. INT'L L. 857 (2012).

[18] *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966 (2013).

[19] EU companies are barred from complying with U.S. secondary sanctions on the basis of Council Regulation (EC) No 2271/96 of 22 November 1996 Protecting Against the Effects of the Extra-Territorial Application of Legislation Adopted by a Third Country, and Actions Based Thereon or Resulting Therefrom, 1996 O.J. (L 309) 1. However, the Regulation does not provide for EU support in case an EU company faces enforcement action in the United States for non-compliance with U.S. secondary sanctions. *See generally* Tom Ruys & Cedric Ryngaert, *Secondary Sanctions: A Weapon out of Control? International Legality of, and European Responses to, US Secondary Sanctions* (Study for the European Central Bank, forthcoming 2019).

[20] *See, e.g.*, U.S. Mission to the European Union, Statement from U.S. Secretary of Commerce Penny Pritzker on EU-U.S. Privacy Shield (Feb. 2, 2016) (arguing that giving EU data protection law a broad scope would significantly impede upon individual rights and the free flow of information). *See* Commission Implementing Decision (EU) 2016/1250 of 12 July 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, 2016 O.J. (L 207) 1, 48–67.

[21] In *Schrems II*, an Irish judge authorized the U.S. government to file an amicus curiae brief in support of Facebook. The High Court Commercial Ireland, [2016 no. 4809] Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems [2017] para. 19

https://doi.org/10.1017/aju.2019.80 Published online by Cambridge University Press

Conclusion: Regional Regulation as Global Inspiration

As an instance of the "Brussels effect,"[22] the EU's unilateral exercise of jurisdiction in certain situations involving data protection has had ramifications for global corporations, governments, and internet users. EU data protection principles have migrated abroad, and have informed and even compelled changes in international or non-EU corporations' data protection practices,[23] as well as third countries' laws and practices,[24] depending on normative socialization and EU bargaining power.[25] EU data protection law, boosted by its extraterritorial application, has proved a global source of inspiration. It remains that the main trigger for third countries and operators to adopt data protection standards equivalent to EU standards is their fear of no longer having access to the EU market. Regardless of the reason for adoption, EU extraterritoriality shapes global standards on data protection. The normative question remains as to how assertively the EU should impose its data protection laws on foreign service providers or third states.

("The United States has a significant and *bona fide* interest in the outcome of these proceedings. At issue in the proceedings is the assessment, as a matter of EU law, of the applicant's law governing the treatment of EU citizens' data transfer to the US. The imposition of restrictions on the transfer of such data would have potentially considerable adverse effects on EU-US commerce and could affect US companies significantly."). In *Schrems II*, Schrems requested that the Irish Data Protection Commissioner halt data transfers between Facebook Ireland and Facebook Inc. on the basis of Standard Contractual Clauses, on the ground that the relevant data may be subject to U.S. mass surveillance in violation of EU data protection law. The CJEU heard arguments July 9, 2019. It is unclear what the U.S. government position is.

[22] The Brussels effect is defined as the "unprecedented and deeply underestimated global power that the EU is exercising through its legal institutions and standards," which "it successfully exports . . . to the rest of the world." Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012).

[23] *See, e.g.*, Facebook CEO Zuckerberg stating that the GDPR protections would in spirit (although not necessarily in detail) extend worldwide. Alex Hern, *Facebook Refuses to Promise GDPR-Style Privacy Protection for US Users*, GUARDIAN (Apr. 4, 2018).

[24] *See, e.g.*, Agreement on the Use and Transfer of Passenger Name Records (PNR) to the US Department of Homeland Security (DHS) of 2011 2012 O.J. (L 215) 1, 13, which provides for judicial redress for EU data subjects "in the US."

[25] Relatively weak EU bargaining power may result in agreements between the EU and third countries that insufficiently protect EU subjects' data transferred abroad. *See, e.g.*, Opinion 1–15 on Draft EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 232 (Eur. Ct. Justice, July 26, 2017) (ruling that parts of the agreement did not comply with the EU fundamental rights to respect for private life and protection of personal data). It is likely that also the EU-U.S. PNR Agreement violates EU fundamental rights. Such agreements would have to be renegotiated to make them compatible with EU fundamental rights law.

https://doi.org/10.1017/aju.2019.80 Published online by Cambridge University Press