# The EU's human rights obligations in relation to its data protection laws with extraterritorial effect

Mistale Taylor*

## Introduction

With the ubiquity of the internet and the rise of digitised personal data, data controllers and processors are processing ever more personal data, foregrounding the need to ensure that these data are protected. The EU, compared with most states, strongly advocates the importance of protecting personal data. Indeed, the EU has the world's longest standing and is also often considered to have the strictest, and certainly the most influential, data protection law. The EU pushes its approach to data protection aggressively and has therefore gained dominance as a legal actor in this field.[1]

A form of territorial extension is evident in data protection law.[2] The law of one jurisdiction, namely the EU, has become and is becoming the rule in other places for several reasons, including economic ease, accession goals, convenience, regulatory arbitrage, and potentially the protection of human rights. EU representatives often use fundamental rights rhetoric to promote its data protection law. This legal diffusion even suggests an overriding data protection norm; however, there is no clear evidence of the existence of such an all-encompassing, widely accepted norm outside the EU. This research looks at the EU's obligations to protect the fundamental right to data protection extraterritorially under international human rights law (IHRL). It conceives of the EU as a duty bearer: the Union exercises jurisdiction, will become a party to the European Convention on Human Rights (ECHR) and is arguably becoming a human rights actor in its own right.

Whilst data protection in the EU was initially conceived of in market terms, it is increasingly connected with fundamental rights. The growing weight of the fundamental right to data protection in the EU is arguably linked to the increased territorial extension of EU data protection law. This raises questions of how to apply a fundamental right in the EU to a virtual, borderless space and ultimately third states. This research focusses mostly on IHRL to determine the obligatory, as an extension of the permissive, application of law in public international law (PIL) terms, that is, the exercise of prescriptive jurisdiction. It asks to what extent the EU is obliged to exercise territorial extension of its laws to protect the fundamental right to data protection for its citizens. The research begins by looking briefly at the extraterritorial

## Key Points

- A form of extraterritoriality is evident in EU data protection law.
- International human rights law, as a subset of public international law, can help determine what are arguably the EU's obligations to safeguard the fundamental right to data protection extraterritorially.
- The EU could be understood to have positive and negative obligations to respect, protect, and fulfil its citizens' right to data protection.
- As the fundamental right to data protection evolves to carry more weight in the EU, this could amplify the EU's obligations under human rights law to protect its citizens' personal data when such data are processed outside EU territory.

* Mistale Taylor, Faculty of Law, Utrecht University, Utrecht, the Netherlands. PhD candidate at Utrecht University and Senior Research Associate at Public International Law and Policy Group.
The author would like to thank Professor Cedric Ryngaert for comments on an earlier draft and participants at the Symposium on Extraterritoriality and Data Protection (Utrecht University, 6 May 2015) for their feedback. The research that resulted in this publication has been funded by the Dutch Organisation for Scientific Research under the VIDI Scheme. This article also forms part of the RENFORCE/CLEER project on The External Effects of European Union Law.

1 'Selling one's own legal doctrines globally is more than just an effort to gain influence for isolated purposes. It incorporates recognition that a global technology ultimately seeks unified global policy solutions and that an aggressively pushed approach has the potential to become the dominant one, or even the only viable one. Within this legal "global scene," the negotiation of Internet-related laws and policies is likely to occur in a fiercely competitive arena'.—Steven R Salbu, 'The European Union Data Privacy Directive and International Relations' (2002) 35 Vand J Transnat'l L 655, 688.

2 See Joanne Scott, 'The New EU "Extraterritoriality"' (2014) 51 CML Rev 1343, 1350; Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' (2014) 62 Am J Comp L 87.

dimension of EU data protection law; next, it justifies using a PIL and IHRL approach to examine the fundamental right to data protection; it then delineates the EU's obligations to protect the fundamental right to data protection extraterritorially under IHRL; and ends by looking at the consequences of the right's evolution within the EU. It is not inconceivable that as the fundamental right evolves to be accorded more importance within the EU legal order, the EU's obligations to safeguard this right extraterritorially could intensify.

## The extraterritoriality of EU data protection law

This research asserts that whilst the EU's relevant actions in relation to its data protection laws do not amount to extraterritorial jurisdiction in the strict sense, they constitute the territorial extension of EU law.[3] The territorial extension of EU law as a concept requires a territorial nexus to a situation but acknowledges that conduct or circumstances in third states have a significant influence on how a regulator applies the relevant EU law to the situation.[4] This research uses the term extraterritoriality (implying something with a nature or effect beyond a territory, not completely a-territorial) and territorial extension interchangeably.

For data protection purposes, EU territory is understood to be physical. The EU Charter applies when member states are implementing EU law.[5] As data processing acts, such as cross-border data transfers happen under the Data Protection Directive (DPD), which member states implement into their national law, the EU Charter can apply to such transfers. It can also apply where the DPD explicitly lends itself to extraterritorial application.[6]

As detailed below, EU data protection laws generally have extraterritorial effect, as opposed to regulating extraterritorial conduct. Data protection laws in, for example, the USA, Brazil, and Australia can also have extraterritorial effect.[7] This research focusses specifically on the extraterritoriality of EU data protection law, however, because none of the aforementioned states qualify data protection as a fundamental right. As the EU bestows this status upon data protection, this gives rise to certain obligations that could necessitate or justify the extraterritorial application of its laws.

## Data protection as a fundamental right in the EU

The question can be raised of whether, based on IHRL, the EU has an obligation to protect the right to data protection extraterritorially for EU citizens, specifically when their personal data are processed beyond the territorial borders of the EU. Fundamental rights are generally considered human rights rooted in a constitution. This research uses 'human rights' as an overarching or PIL term and 'fundamental rights' in specific EU examples.

The EU wants to protect its citizens who are data subjects. EU citizens are rights holders and potential victims of having their right to personal data protection violated when their personal data are transferred or processed outside of EU territory. Moreover, they are addressees of the EU's data protection norm. EU data protection law with extraterritorial effect focusses on protecting individuals rather than the EU itself or member states. Especially in the cybersphere, it is important to note that an EU citizen's right to data protection could conceivably be violated 'even in absence of any detriment to the affected individual'.[8]

Data protection has noticeably been moving away from being referred to as an economic necessity to being promoted within the EU and abroad as a fundamental right. Linking data protection to human rights is not a new concept, but it is growing in popularity. Already in 1997, somewhat prophetically, did a conference of data protection commissioners acknowledge that, in the data protection sphere, they should not doubt the EU's 'political will (. . .) to protect the fundamental human rights of citizens'.[9] Although the proposed General Data Protection Regulation seeks both to promote fairness of competition and protect fundamental rights, EU politicians are increasingly pushing the Regulation using fundamental rights rhetoric.[10] Enshrining data protection

3 Scott (n 2), at 1350; Scott (n 2), at 87.

4 Scott (n 2), at 90.

5 Article 51(1) of the Charter of Fundamental Rights of the European Union (OJ C 364 of 18 December 2000) (hereinafter 'EU Charter').

6 Articles 4 and 25 of 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 L 281 31) (hereinafter 'Data Protection Directive').

7 Christopher Kuner, 'Internet Jurisdiction and Data Protection Law: An International Legal Analysis' (2010) 18 Int'l JL & IT 176, 192, 193.

8 Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harv lnt'l L J 81, 134 ***citing*** *Huvig v France* App No. 11105/84 (ECHR, 24 April 1990) 35.

9 James M Assey, Jr and Demetrios A Eleftheriou, 'The EU-US Privacy Safe Harbor: Smooth Sailing or Troubled Waters?' (2001) 9 Catholic Univ of America CommLaw Conspectus 145, 145 ***citing*** Ulf Bruhan, 'Data Protection in Europe: Looking Ahead, Address Before the Nineteenth International Conference of Privacy Data Protection Commissioners', September 1997, quoted in Peter P Swire and Robert E Litan, 'None of Your Business: World Data Flows Electronic Commerce, and the European Privacy Directive' (1998) 12 Harv JL & Tech 46.

10 For example, Director for Fundamental rights and Union citizenship in the Directorate-General for JUSTICE of the European Commission, Paul Nemitz, at ERA conference on Safeguarding the Fundamental Right to Data Protection, 29–30 October 2014, stated, *inter alia*, that we should 'not accept that our rights are undermined by what technology allows us to do'.

as a fundamental right in the EU bestows obligations upon the EU, which could provide a legitimate justification, or at least an explanation, for the territorial extension of its law. Most questions of the extraterritorial application of human rights have centred on military occupation in conflict situations, so the extraterritorial applicability of the right to data protection presents a new problem. The following looks at the changing nature of data protection in the EU.

## The nature of the right to data protection and associated obligations

According to Article 3(5) of the Treaty on European Union (TEU) and Court of Justice of the European Union (CJEU) jurisprudence, it can be understood that the EU is obliged to respect international human rights duties in accordance with international treaties or customary international law.[11] This section uses the lens of PIL to look at the nature of the right to data protection as it is enshrined in EU law. Data protection is subjective and not an absolute human right. The right to data protection provides direct protection from the state and indirect protection for individuals from other individuals. To outline the EU's human rights obligations in external and extraterritorial situations, this research uses IHRL as a subset of PIL. This approach is justified *infra*.

### Under public international law

Despite being a supranational organization and not a state, it is accepted that PIL norms apply to the EU.[12] Article 3(5) TEU confirms that '(i)n its relations with the wider world, the Union (. . .) shall contribute to (. . .) the protection of human rights (. . .) as well as to the strict observance and the development of international law'.[13] Article 21 TEU adds that '(t)he Union's action on the international scene shall be guided by the principles (of) the universality and indivisibility of human rights (and) respect for the principles of (. . .) international law'.[14] The TEU mentions contributing to the strict observance and development of international law, and respecting its principles, which is not as strong as, for example, outright requiring the EU to adhere to PIL. CJEU jurisprudence further confirms the EU's obligations *vis-à-vis* PIL. The Court in *Air Transport Association of America* repeated the TEU's above provisions on international law and went further: '(the EU) is bound to observe international law in its entirety, including customary international law, which is binding upon the institutions of the European Union'.[15]

Certain internal market and fisheries cases exemplify how the EU sometimes adheres to a concept of jurisdiction under PIL.[16] For instance, in fisheries case *Kramer*, the CJEU applied an EU Regulation 'in so far as the Member States have similar authority under public international law' to fishing on the high seas.[17] These cases show that EU courts and law 'have drawn inspiration from PIL jurisdiction to establish the relevance and applicability of EU norms in extraterritorial situations'.[18] It has even been asserted that CJEU judges have sometimes extended the scope of EU law beyond PIL conceptions of jurisdiction to effectively implement EU rights and obligations.[19] Whilst it is noteworthy that scholars have observed the CJEU extending the scope of EU law to protect fundamental rights, this research limits itself to the premise that the TEU and case examples confer an obligation on the EU to observe PIL. Moreover, in a data protection context, the Article 29 Working Party and scholarship have confirmed that PIL is the ideal framework in which to analyse jurisdiction over data protection.[20]

11 Lorand Bartels, 'The EU's Human Rights Obligations in Relation to Policies with Extraterritorial Effects' (2015) 25 EJIL 1071, 1078; see also 'In its relations with the wider world, the Union shall uphold and promote its values (see Art. 2, TEU) (. . .) It shall contribute to (. . .) the protection of human rights (. . .) as well as to the strict observance and the development of international law' Article 3(5) of Consolidated Version of the Treaty on European Union Art. 6, 26 October 2012, 2012 O.J. (C 326) (hereinafter 'TEU'); *Air Transport Association of America and Others v Secretary of state for Energy and Climate Change*, Case C-366/10, 21 December 2011, paras 101 and 102.

12 Violeta Moreno-Lax and Cathryn Costello, 'The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing, Oxford 2014) 1663 ***citing*** Michael P Scharf, *The Law of International Organisations* (2nd edn, Carolina Academic Press, Durham 2007); and Christiane Alhborn, 'The Rules of International Organizations and the Law of International Responsibility' (2011) 8 IOLR 397.

13 Bartels (n 11), at 1073.

14 Article 21 of the TEU.

15 *Air Transport Association of America and Others v Secretary of state for Energy and Climate Change*, Case C-366/10, 21 December 2011, paras 101 and 123.

16 For an overview of examples, see Moreno-Lax and Costello (n 12), at 1664–1666 ***citing,*** eg *Ingrid Boukhalfa v Federal Republic of Germany*, Case C-214/94, 30 April 1996, para. 22 and Cornelis Kramer and others, Joined Cases 3, 4, and 6/76, 14 July 1976, paras 30–33. See also *Commission of the European Communities v French Republic*, Case 167/73, 4 April 1974.

17 Cornelis Kramer and others, Joined Cases 3, 4, and 6/76, 14 July 1976, paras 30–33.

18 Moreno-Lax and Costello (n 12), at 1667.

19 Ibid.

20 'While public international law only applies directly to relations between states, its role as the basic limiting standard of the international legal order provides the testing ground for jurisdictional rules affecting private parties in different states as well; indeed, the Article 29 Working Party has recognized that jurisdiction under data protection law should be evaluated under public international law'.—Kuner (n 7), at 184 ***citing*** Article 29 Working Party, WP 56 (n 13) 2, stating that 'whether national (data

## Under international human rights law

IHRL as a subset of PIL can be used to delineate the nature of the EU's obligations to protect the fundamental right to data protection when applying EU law extraterritorially. If they are binding under the EU treaties or customary international law, the EU must respect international human rights obligations.[21] Broadly speaking, there is '(n)o formal hierarchy between human rights and "ordinary" international law'; however, human rights instruments should either predominate or general treaties should be interpreted 'in conformity with human rights'.[22] This exemplifies the inextricable link between IHRL and PIL.

Granted, the EU Charter is not an EU treaty, but it is an important human rights instrument. In terms of subject matter, the EU Charter comes close to a human rights treaty: with an underlying foundation of preserving an individual's human dignity, it aims to safeguard that individual's rights.[23] Furthermore, whilst the ECHR and European Court of Human Rights (ECtHR) jurisprudence are not directly binding on the EU, the rights in that treaty are closely connected to those in the EU Charter. The TEU establishes that the human rights the ECHR guarantees amount to general principles of EU law.[24] Although it applies them indirectly, the CJEU often cites the ECHR and ECtHR jurisprudence in its judgements.[25] By stating that the meaning and scope of rights in the Charter shall be equivalent to the corresponding rights in the ECHR, Article 52(3) of the Charter connects the rights it contains to those enshrined in the ECHR.[26] The CJEU has referred to this Article when considering relevant case law of the ECtHR.[27]

Recent UN developments also help anchor the right to data protection in an IHRL context. Since, and probably in most part due to, the 2013 Snowden revelations, the right to privacy has featured on the UN's agenda. In 2013, the UN General Assembly adopted a resolution on the right to privacy in the digital age.[28] In 2015, the UN Human Rights Council appointed a Special Rapporteur on the right to privacy.[29] The UN General Assembly resolution focusses heavily on the right to privacy and, within that framework, mentions only the 'collection of personal data' and not, for instance, the right to data protection, cross-border data transfers or data retention. However, it 'firmly puts the issue of electronic surveillance within the framework of international human rights law', which further strengthens the impetus to use an IHRL approach to analyse the EU's data protection obligations.[30]

## The extraterritorial application of human rights instruments

Numerous scholars have written extensively on the extraterritorial application of human rights treaties, but few have attempted to apply human rights treaties to potential interferences with the right to data protection as distinct from the right to privacy.[31]

### Jurisdiction under international human rights law

In the context of a discussion on extraterritoriality and the fundamental right to data protection, it has been argued that 'jurisdiction' under IHRL is different from 'jurisdiction' under PIL.[32] The ECtHR's pronouncements in *Banković* that jurisdiction in human rights treaties equates to jurisdiction in general PIL have

protection) law applies to situations with links to several countries' is 'a general question of international law'.

21 Bartels (n 11), at 1078.

22 Anne Peters, 'Surveillance Without Borders? The Unlawfulness of the NSA-Panopticon, Part II' (*EJIL: Talk!*, 2 November 2013) <http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/> accessed 20 August 2015.

23 Marko Milanovic, *The Extraterritorial Application of Human Rights Treaties* (OUP, Oxford 2011) 3.

24 Article 6(3) of the TEU.

25 Council of Europe, *Accession by the European Union to the European Convention on Human Rights* (June 2010), 2 <http://echr.coe.int/Documents/UE_FAQ_ENG.pdf> accessed 20 August 2015.

26 Article 52(3) of the EU Charter.

27 Allan Rosas, 'Is the EU a Human Rights Organisation?' Cleer Working Papers 2011/1 (2011).

28 UN GA Res. A/RES/68/167, The right to privacy in the digital age, 21 January 2014.

29 UN GA Res. A/HRC/28/L.27, 24 March 2015.

30 Milanovic (n 8), at 85.

31 Milanovic's research on the extraterritorial application of the right to privacy in a surveillance context makes a palpable connection between the right to privacy and applying human rights treaties extraterritorially. He uses 'foreign surveillance' to cover data processing ('the collection, storage, processing, and transfer of personal data to third parties') in the context of looking at the extraterritorial application of the right to privacy (Milanovic (n 8), at 86). It is, moreover, necessary and important to distinguish between the two rights when looking at extraterritorial jurisdiction over data protection law. This is in part due to the notable differences between the scope and limitations of both rights. The right to privacy has a broader scope for application and fewer limitations than the right to data protection. (Juliane Kokott and Christoph Sobotta, 'The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and ECtHR' (2013) 3 IDPL 222, 228.)

32 'Marko has argued cogently that the term "jurisdiction" as used in human rights treaties should be understood differently from its use in public international law'.—Christopher Kuner, 'Extraterritoriality and the Fundamental Right to Data Protection' (*EJIL: Talk!*, 16 December 2013) <http://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/> accessed 20 August 2015. Whilst Milanovic does say two concepts of jurisdiction (a classic PIL one and one often found in human rights treaties) 'may be related, but (. . .) cannot possibly be the same' (p. 33), he does not say there is a strict difference between the two, but rather that one has to choose between several concepts of jurisdiction under general international law. He is 'not arguing that the word "jurisdiction" should be given a special meaning autonomous to human rights law. Rather, the word has several different and equally ordinary

largely been criticised.[33] Both approaches, however, misconstrue the concept for our purposes. This research adheres to the notion that jurisdiction in IHRL is a manifestation of one of several ordinary meanings of jurisdiction under PIL, although it might be emerging that data protection law needs a unique form of jurisdictional trigger.[34]

Jurisdiction in PIL takes on a different meaning depending on the context in which it is used; we can accept that there are many, not one ordinary, meanings of jurisdiction.[35] Before analysing the EU's positive obligations to safeguard its citizens' fundamental right to data protection, it is important to determine how we can construe the form of jurisdiction the Charter's scope Article entails. Whilst it has been recommended, a PIL approach to this is not always favoured. The assertion that 'the discussion on the extraterritorial applicability of the Charter should be liberated from the often politically laden debate on borders and territory and brought to the less-statist space of EU competences and legality'[36] forgets that territorial sovereignty and the authority to legislate cannot possibly be divorced from political concerns. Furthermore, it sidelines the importance of physical EU territory in EU data protection law,[37] the EU's PIL obligations, and the basic premise of PIL being founded on territorial sovereignty, which are needed to continue a discussion on the extraterritoriality of the Charter.

## Applying different models of international human rights law jurisdiction to EU data protection law

It is useful to examine forms of IHRL jurisdiction documented by scholars who have researched that topic in a privacy, data protection, or cybersphere context. These forms of jurisdiction are apparent in various case law examples; however, this section will focus on theoretical conceptions of jurisdiction.[38]

Broadly speaking, extraterritorial IHRL jurisdiction can be exercised where a state has control over either foreign territory or a person.[39] These forms of jurisdiction under IHRL mirror the territorial (spatial) and personality (personal) principles of PIL jurisdiction. This suggests that IHRL and PIL concepts of jurisdiction are not necessarily different, which gives weight to the argument that IHRL jurisdiction is a manifestation of one general form of PIL jurisdiction. Each model of IHRL jurisdiction is discussed below. It is easier to apply some models to data protection than others, but none is completely ideal. This demonstrates the room, and perhaps need, to come up with a new way of obliging the EU to exercise jurisdiction over data protection law extraterritorially.

The spatial or territorial model, based on territory or effective control over territory, is difficult to apply to data protection because data are transferred in a virtual space from the EU to a third state. The DPD uses the location of a data controller to establish a territorial nexus to member state action. EU data protection law, however, can apply outside EU territory, over which the EU does not have effective control. Moreover, it would be difficult to determine precisely where and when an interference with someone's right to data protection occurred. A data subject's presence in the physical world is separate from an interference with his or her right to data protection in the virtual world.[40] Indeed, both the interference with human rights and the protection thereof can occur far from an individual's physical location. This could explain or justify the extraterritorial effects of EU data protection law as EU citizens on EU territory would have their right to data protection protected in third states.

The personal model could therefore offer a more useful solution. It focusses on jurisdiction over an individual under the authority and control of a state or other actor.[41] As the locations of both the data subject and the interference are irrelevant in the personal model, it could apply more effectively in a data protection context. Both models, however, present issues related to control.

To justify applying extraterritorial jurisdiction under the spatial model, someone has to exercise effective

meanings in general international law itself, and the question is hence which of these meanings—which of these *concepts*—the jurisdiction clauses of human rights treaties refer to' (p. 53). Wilde also reaches the same conclusion, see Milanovic (n 23), at 33, fn 52 ***citing*** Ralph Wilde, 'Triggering state Obligations Extraterritorially: The Spatial Test in Certain Human Rights Treaties' (2007) 40 ILR, 503, 508, 513, 514, see also Alexandra Ruth and Mirja Trilsch, 'Bankovic v. Belgium (Admissibility)' (2003) 97 AJIL 168, 171; Olivier De Schutter, 'Globalization and Jurisdiction: Lessons from the European Convention on Human Rights' (2006) 6 Balt YIL, 183; Alexander Orakhelashvili, 'Restrictive Interpretation of Human Rights Treaties in the Recent Jurisprudence of the European Court of Human Rights' (2003) 14 EJIL 529, 539 et seq.

33 See *Banković and Others v Belgium and Others* App No. 52207/99 (ECHR, 12 December 2001) and eg Wilde (n 32), at 513; Milanovic (n 23), at 262.

34 Milanovic (n 23), at 53.

35 Ibid.

36 Moreno-Lax and Costello (n 12), at 1682.

37 Article 4 of the Data Protection Directive.

38 To see relevant case law on spatial jurisdiction, see eg Milanovic (n 8), at 112 and 113, and for the personal model, see 114–118 of the same.

39 See eg Maarten den Heijer, *Europe and Extraterritorial Asylum* (Hart Publishing, Oxford 2012) 29.

40 Milanovic (n 8), at 124 ***citing*** Carly Nast, 'Interference-Based Jurisdiction Over Violations of the Right to Privacy' (*EJIL: Talk!*, 21 November 2013) <http://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/> accessed 20 August 2015.

41 Milanovic (n 23), at 173.

control over territory. Similarly, under the personal model, someone has to exercise authority or control over an individual. If we conceive of individuals as imbued with informational self-control over personal data, this could move closer to a form of control over persons.[42] It is difficult, however, to establish who has control and should therefore exercise jurisdiction over 'personal data' or a 'data subject'.

Milanovic outlines the positive and negative obligations of jurisdiction in the context of applying them to human rights treaties to safeguard the right to privacy extraterritorially.[43] He argues that, whilst it is not flawless, the positive and negative obligations model is the most effective jurisdictional model in offering simple and straightforward guidance on how human rights treaties apply to questions of foreign surveillance.[44] As data protection and foreign surveillance are linked, given their virtual, cross-border nature and connections with the right to privacy, Milanovic's positive and negative obligations model is valuable in the context of this research.

Under this model, a state would have a positive obligation to secure or ensure human rights, even by preventing third-party violations where it has effective control over an area.[45] A state would also have a negative obligation to respect human rights by not interfering with the rights of individuals unless sufficiently justified.[46] This obligation would not have to reach any jurisdictional threshold as it would not be limited to a specific territory or area of control.[47] Milanovic proposes the following rule: 'the state obligation to respect human rights is not limited territorially; however, the obligation to secure or ensure human rights is limited to those areas that are under the state's effective overall control'.[48] In terms of data transfers, however, there are still difficulties with what constitutes effective control: what qualifies as authority, power or control? Manual, physical, or coercive power is almost irrelevant in light of the technological capacity to process personal data today.[49] Perhaps an EU member state or EU body, acting as a data controller, could be understood as exercising effective control over someone's personal data, but this is extremely abstract, which could lead to legal uncertainty and inconsistencies.

To better protect, for instance, the rights to privacy and data protection, it could thus be necessary to reinterpret control in the cyber age to determine what would trigger human rights obligations. It is worth considering a form of virtual control[50] or a widening of the definition of control from the factual to the functional.[51] That said, parts of the positive and negative obligations can apply to the Charter to determine the reach of the EU's fundamental rights obligations more precisely.

## Positive and negative obligations to respect–protect–fulfil human rights

In IHRL, there are discrete types of obligations or duties when safeguarding human rights: namely, those to respect, protect, and fulfil.[52] In short, one could argue that the duty to respect a right bestows a negative obligation of conduct on the EU, the positive obligation to protect is one of the conducts that extend to third-party violations, and the obligation to fulfil entails a positive obligation of result. These obligations could extend extraterritorially. In its scope Article, the EU Charter articulates that when member states are implementing EU law, such as the DPD, '(t)hey shall therefore *respect* the rights, *observe* the principles and *promote* the application thereof in accordance with their respective powers' (emphasis added).[53] These powers can extend beyond EU borders, thus invoking extraterritorial human rights obligations. Respect–protect–fulfil duties are a feature of IHRL. It is inconsequential that the EU Charter contains a reference only to 'respect'. Indeed, human rights treaties generally include no explicit

42 Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (2014) 63 ICLQ 569, 595.

43 Milanovic (n 8), at 118 and 119.

44 The model is not perfect, but it is 'clear, predictable, precludes the vast majority or arbitrary outcomes and provides a relatively stable balance between considerations of universality and effectiveness'.—Milanovic (n 8), at 119.

45 Milanovic (n 8), at 119.

46 Ibid.

47 Ibid.

48 Milanovic (n 23), at 263.

49 Milanovic (n 8), at 120.

50 Peters (n 22); more concretely, if the effective control test is redundant when applied to cross-border data transfers, Margulies' proposed 'virtual control' test to determine state responsibility (pp. 514 and 515). His is a broad concept that asserts that virtual control qualifies as exercising control (abstract). For instance, if a state funded or supported an act by a private group that, in his example, conducted a cyberattack, that state would be responsible for the attack (abstract). This test, however, is difficult to transpose onto interferences with the right to data protection. In such interferences, a state does not necessarily fund or support a specific act by a private actor. More common interferences would be, for example, a US company using EU citizens' data for a non-specified purpose or the US Department of Homeland Security retaining EU citizens' data for an excessive period of time. Can attributing state responsibility determine who has the authority to exercise extraterritorial jurisdiction? See P Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 Melb J Int'l L 496, 519.

51 See eg den Heijer (n 39), at 48.

52 Martin Scheinin, 'Characteristics of Human Rights Norms' in Catarina Krause and Martin Scheinin (eds), *International Protection of Human Rights: A Textbook* (Åbo Akademi University Institute for Human Rights, Turku 2009), 19, 27.

53 Article 51(1) of the EU Charter.

reference to states parties' respect–protect–fulfil duties.[54] This section will outline what these duties entail and discuss how they relate to data protection in the EU.

### The obligation to respect

The obligation to respect connotes a negative obligation of conduct, whereby the EU would have to refrain from conduct that would infringe upon someone's enjoyment of the right to data protection. Specifically, this constitutes a negative obligation to respect an individual's right to data protection by *not* interfering with his or her privacy in the context of personal data. The Charter requires that the EU 'respect' human rights and under IHRL, the duty to respect would be inherent to that human rights instrument.[55]

According to Milanovic's aforementioned positive and negative obligations jurisdiction model, and his assertion that the EU's negative obligations could apply extraterritorially, the EU's duty to respect the fundamental right to data protection could provide a basis for the EU to apply this negative obligation extraterritorially. One conceivable manifestation of this duty to respect, which draws some parallels with the obligation to protect, could be the territorially unlimited or extraterritorial application of the 'negative obligation to refrain from conduct that would assist third parties in violating the right to privacy' or, in this instance, the right to data protection.[56]

This manifestation can be seen in the territorial extension of EU law through, for example, its adequacy decisions and bilateral negotiations. Specifically, personal data may only be transferred to third states with an adequate level of protection.[57] By not transferring personal data to third states with inadequate levels of data protection, the EU is, in theory, fulfilling its obligations to avoid conduct that would enable third states to interfere with its citizens' right to data protection. If the European Commission determines that a third state does not satisfy the DPD's adequacy requirement, the relevant member state shall take measures to prevent transfers to that state and the Commission 'shall enter into negotiations with a view to remedying the situation'.[58] As evident in negotiations between the USA and EU over data transfers in many different contexts, this provision shows that, through negotiating, the EU must attempt to encourage or ensure that a third state adopts at least some aspects of its high-level data protection law if that state wants to receive data from the EU at all. Accordingly, the DPD's adequacy requirement could be interpreted as necessitating an indirect application of EU law abroad. The Union's obligation to respect could be understood to apply initially as a negative obligation of conduct to refrain from transferring data to certain third states. If it then had to enter into negotiations with third states, the EU's obligation would become a positive obligation of conduct to protect, as outlined below.

### The obligation to protect

The obligation to protect is an obligation of conduct, wherein the EU would be obliged to ensure that a third party does not violate someone's right to data protection.[59] It can be asked whether this obligation to protect would apply if the third-party violator were located outside of EU territory or if the victim's personal data moved from the EU to a third state. The Charter requirement that member states promote the application of Charter rights and principles draws parallels with the duty to protect. They both imply a third party or an external actor (i) to whom the member state must promote the application of the right to data protection and/or (ii) whom the EU as a responsible party must prevent from violating its citizens' right to data protection.

Could this requirement oblige the EU to actively prevent third-party violations of its citizens' right to data protection in an extraterritorial context? Again using Milanovic's model, and his assertion that the EU's positive obligations would apply only in a place under its effective control, we run into a wall with the effective control threshold. Nonetheless, the general duty to protect citizens from third-party interferences that the Charter bestows upon the EU could legitimize the DPD's wide scope of application, regardless of effective control requirements. The *Google Spain* case illustrates how the CJEU and, by extension, EU member states are enabling this active protection.[60] Specifically, through the establishment of a subsidiary in Spain, Google, Inc., incorporated in a third state (the USA), was held responsible for potentially interfering with EU citizens' data protection

54 For example, the ICCPR uses such language as states parties 'undertake to respect and to ensure' (Art. 2(1)), and the ICESCR says each state party 'undertakes to take steps (. . .) (to achieve) the full realization of the rights' (Art. 2(1))—International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR); International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 (ICESCR).

55 Article 51(1) of the EU Charter.

56 Milanovic (n 8), at 124, fn 176, see, in that footnote, Milanovic's analogy to the *non-refoulement* rule in eg *Soering v United Kingdom*, App No. 14038/88 (ECHR, 7 July 1989) or *Judge v Canada*, Communication No. 829/1998, U.N. Doc. CCPR/C/78/D/829/1998 (2003).

57 Article 25(1) of the Data Protection Directive.

58 Article 25(4) of the Data Protection Directive.

59 See eg Center for Economic and Social Justice, 'Economic, Social and Cultural Rights – A Guide to the Legal Framework' <http://www.cesr.org/downloads/Legal%20Duties.pdf> accessed 20 August 2015.

60 *Google Spain v AEPD and Mario Costeja Gonzalez*, Case C-131/12, 13 May 2014.

rights. The Court was attempting to regulate how personal data are processed by search engines in third states, those being the potential rights violators.

### The obligation to fulfil

The obligation to fulfil implies a positive obligation of result, that is, an obligation to fulfil an individual's right to data protection by providing legal, regulatory, and enforcement mechanisms and resources.[61] Milanovic's suggestion that this obligation applies only in a place under a state's effective control makes more sense here. The EU ordinarily offers legal and enforcement data protection mechanisms within its own territory or in places under its effective control. It is hard to say that it is obliged to offer these abroad. That said, some EU Data Protection Authorities have attempted to enforce EU data protection law in third states by, for example, conducting audits to confirm that these states are complying with EU data protection law.[62] The obligation to fulfil is one of the results, so if these extraterritorial enforcement mechanisms resulted in effectively safeguarding the right to data protection for EU citizens, that obligation could be considered satisfied. Again, however, the EU cannot be said to have effective control over, for instance, Colombia, where the Spanish Data Protection Authority has conducted audits to ascertain compliance with EU data protection law.[63] Such obfuscation further strengthens the need to redefine effective control vis-à-vis personal data. In summary, there appear to be more concrete examples to justify the Charter's extraterritorial application when looking at the obligations to respect and protect.

## The increased weight of the fundamental right to data protection and subsequent ramifications for extraterritoriality

The CJEU has confirmed that the right to data protection is not absolute, but 'must be considered in relation to its function in society'.[64] There exist legal limitations on infringing the fundamental right to data protection, yet it must be balanced against other, often fundamental, rights. As it is a subjective right, the increased emphasis the CJEU and EU legislators have recently placed on the fundamental right to data protection could enhance the Union's obligations to safeguard that right beyond its borders. Article 52 of the EU Charter outlines the scope of application of the fundamental rights contained therein:

> Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[65]

This article recalls certain provisions in other human rights instruments, notably the International Covenant on Civil and Political Rights (ICCPR) and the ECHR, which allow restrictions on the exercise of certain rights if they are in accordance with the law, serve a legitimate purpose, and are necessary.[66] In light of the possibilities to limit the exercise of fundamental rights, it is necessary to examine the rights and freedoms against which the right to data protection is often weighed. These include, *inter alia*, the free flow of information, the right to access to documents, the right to freedom of expression, and security interests.

The fact that EU fundamental rights law accords data protection a special status aimed at strongly protecting individuals has spurred some scholars to assert that the EU must go further than conducting a balancing test between that right and others; they claim that it may not be considered as subordinate or subject to other rights.[67] Recent CJEU jurisprudence appears to support this assertion. Some case examples that demonstrate the traction the right to data protection is gaining in the EU are the *Google Spain* and *Digital Rights Ireland* cases, both from 2014.[68]

61 Scheinin (n 52), at 27 and 28; on the positive and negative obligations associated with ECHR, Art. 8, see 'Article 8: The Right to Respect for Private and Family Life, Home and Correspondence' (2012) Human Rights Review 259.

62 Christopher Kuner, 'Extraterritoriality and International Data Transfers in EU Data Protection Law', University of Cambridge Faculty of Law Research Paper No. 49/2015, 11–12 ***citing*** 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/portalwebAGPD/jornadas/transferencias_internacionales_datos/common/pdfs/report_Inter_data_transfers_colombia_en.pdf> accessed 27 August 2015 and Loek Essers, 'Google Agrees to Italian Privacy Authority Audits in the US' (*PC World*, 20 February 2015).

63 Agencia Española de Protección de Datos, 'Report on International Data Transfers: Ex officio Sectorial Inspection of Spain-Colombia at Call Centres' (July 2007), 7–9 <https://www.agpd.es/portalwebAGPD/jornadas/transferencias_internacionales_datos/common/pdfs/report_Inter_data_transfers_colombia_en.pdf> accessed 27 August 2015.

64 Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* (2010) ECR I-11063, Judgment of the Court (Grand Chamber) of 9 November 2010, para. 48.

65 Article 52(1) of the EU Charter.

66 See, eg Article 22(2) of the ICCPR; Article 8(2) of the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended).

67 Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer, New York 2009), 77.

68 *Google Spain v. AEPD and Mario Costeja Gonzalez* (n 60); *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, 8 April 2014.

## The free flow of information

Firstly, the right to data protection should be balanced with facilitating the free flow of information or the right to freedom of information, and the right to freedom of opinion and expression.[69] Council of Europe Convention 108 and the DPD, *inter alia*, affirm the need to balance the fundamental freedom of the free flow of data with the right to data protection to establish an internal market.

The particular form of the right to erasure the CJEU established in the *Google Spain* case arguably threatens the public's right to information and the free flow of information. In this case, a Spanish national sought to be able to request that Google Spain or Google, Inc. remove apparently irrelevant search results about his past financial situation.[70] The Court considered questions of (i) the scope of application *ratione materiae* of the DPD, (ii) the territorial scope of the DPD, (iii) the responsibility of a search engine operator for the results it produces, and (iv) whether a data subject has the right to ask for these search results to be delisted.[71] The Court established that the DPD applied to the situation by asserting that a search engine was a data controller that processed personal data, even though such personal data had been published elsewhere by a third party.[72] Furthermore, the Court creatively established territorial jurisdiction over the situation as Google, Inc., the US-incorporated parent company, processes the relevant personal data and its subsidiary Google Spain only sells advertising space. The Court considered selling advertising space to constitute data processing 'in the context of the activities of an establishment of the controller on the territory of a member state', thus satisfying the DPD's applicable law provision.[73] Furthermore, the judgment established the right to erasure, deeming search engines responsible for removing certain links to third-party websites that publish information related to a data subject.[74] On the basis of the DPD and Articles 7 (right to privacy) and 8 (right to data protection) of the Charter, the Court formally established the right to erasure.[75] As such, an EU data subject can request that inaccurate, inadequate, irrelevant, excessive, or outdated search results related to him or her be delisted.[76] Notably, the Court pronounced that the Charter's rights to privacy and data protection 'override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name'.[77] This pronouncement clearly marginalizes both the market freedoms that the right to the free flow of information initially sought to enable and the public's access to information in favour of protecting personal data.

The judgment also exemplifies how fundamental rights, particularly the right to data protection, are quietly surpassing internal market freedoms and other rights with which they ought to be balanced. The Court stipulated that the only justified interference in these rights would be if the general public had a greater interest in accessing the information, such as if the data subject were a public figure.[78] It also follows earlier CJEU decisions that emphasize the right to data protection over the freedom of information.[79]

### The right to freedom of expression

In *Digital Rights Ireland*, the applicants successfully sought the annulment of the 2006 Data Retention Directive, which obliged telecommunications to retain communication data for between 6 months and 2 years for counter-terrorism purposes.[80] The legal grounds put forward for annulling the Data Retention Directive were three articles in the EU Charter, namely, the protection of private and family life (Article 7), the right to data protection (Article 8), and the right to freedom of expression (Article 11).[81] Article 11 was included as a ground for annulment based on the sentiment that individuals might not feel completely free to express themselves in an environment where they felt under constant surveillance. The Court found it unnecessary to discuss the right to freedom of expression because it had already determined the Data Retention Directive invalid on the basis of the right to private and family life, and the right

69 See eg Article 19 of the Universal Declaration of Human Rights, 10 December 1948, 217 A (III); Article 19(2) of the ICCPR; Article 1(2) of the Constitution of the United Nations Educational, Scientific and Cultural Organisation (UNESCO), 16 November 1945; Preamble of the UNESCO Florence Agreement on the Importation of Educational, Scientific and Cultural Materials, Florence, 17 June 1950.

70 *Google Spain v. AEPD and Mario Costeja Gonzalez* (n 60), at para. 15.

71 Ibid, at para. 20.

72 Ibid, at para. 41.

73 Ibid, at para. 60.

74 Ibid, at para. 88.

75 Ibid, at para. 99.

76 Ibid, at para. 90.

77 Ibid, at para. 88.

79 See eg Lynskey (n 42), at 576, 577, and 579 that discusses how one fundamental right (to data protection) consistently trumps the fundamental right to access to documents (Article 42 of the EU Charter) ***citing*** *European Commission v Bavarian Lager*, C-28/08, 29 June 2010.

80 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* (n 68).

81 Ibid, at para. 25.

to data protection.[82] As such, the Court sidelined the right to freedom of expression. Finding that the Data Retention Directive interfered with the right to freedom of expression would only have strengthened the Court's decision to annul the Directive. Accordingly, this case is not an example of the Court failing to conduct a proper balancing test, but it rather shows how it focussed far more on the right to data protection than the right to freedom of expression. The *Digital Rights Ireland* decision could thus suggest that issues related to privacy and data protection currently supersede those related to the freedom of expression.

### Security interests

The right to data protection is often necessarily weighed up against security interests and criminal law enforcement requirements.[83] Passenger Name Record agreements between the EU and the USA, Canada, and Australia establish a set of guidelines on processing EU citizens' airline passenger data and transferring it to the US Department of Homeland Security or comparable organizations in Canada and Australia.[84] The agreements aim to counteract terrorism and serious transnational crime. The ongoing negotiations between the EU and the USA over their Passenger Name Record agreement, where a pro-data protection (EU) and pro-security (USA) conflict is evident, exemplify an attempt at balancing the two interests. Furthermore, the EU is increasingly finding data protection issues in counter-terrorism instruments that require states to retain the personal data of EU data subjects. In light of the *Digital Rights Ireland* decision, the Canada–EU Passenger Name Record agreement has been submitted to the CJEU to determine its legality, further suggesting that data protection is gaining more weight compared with security interests.[85]

### A heavier right

The aforementioned examples could be a reflection of increased public concern for personal data protection since the Snowden revelations. If we recall that the legal limitations on infringing the fundamental right to data protection include the principles of proportionality and necessity, perhaps the EU's measures to protect its citizens' right to data protection beyond its borders could be understood as being increasingly necessary, thus justifying a different balancing test in terms of proportionality.

Nonetheless, it is yet to be seen to what extent the Court's decisions actually safeguard fundamental rights.[86] Data protection could be conceived of as what has been called a 'super right', but what this research will conceive of as a 'heavier' right in terms of balancing tests or prominence in decisions.[87] It is a right that has recently surpassed other rights or freedoms against which it ought to be balanced.

At least in the EU, data protection has evolved from being conceived of as an economic necessity, to a right in general, to a fundamental right, and to a right with such elevated status that it could potentially threaten the protection of other fundamental rights. This weight, however, could also further strengthen the EU's obligations to protect the right to data protection extraterritorially, especially as it is a subjective right.

Protecting a fundamental right is an oft-cited, but not the only, reason the EU is applying its data protection laws extraterritorially. It is perhaps the most effective way to justify EU extraterritorial action in terms of perceived legitimacy. No matter the real underlying reasons for the EU to apply its laws extraterritorially, the right to data protection is evolving to carry more weight and the EU is using it to prescribe or promote its legislation externally.

## Conclusion

In summary, the EU is territorially extending the application of its data protection laws. Under human and fundamental rights law, the EU's protective duty could apply in extraterritorial situations.

Data protection's evolution from economic necessity to autonomous, fundamental right, which has corresponded to the EU's territorial extension of its law to safeguard this right, could imply causality between the two developments. The former evolution of the right could at least explain or justify the latter extension of EU law. The changing nature of the right to data protection in the EU

82 Ibid, at para. 70.

83 Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, New York 2014) 233.

84 For example, Council of the European Union, Agreement between the USA and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, 8 December 2011.

85 European Parliament press release, 'MEPs refer EU-Canada air passenger data deal to the EU Court of Justice', 25 November 2014.

86 Placing so much emphasis on data protection as a human right might not actually protect or promote human rights. Note certain states, such as China and Russia, have strong privacy laws or internet firewalls, which completely stymie the rights to freedom of expression and the free flow of information. There have also been issues with implementing both decisions in member states.

87 '(T)he Court seems increasingly to consider data protection a "super-right" and should not forget the need to balance with freedom of expression'.—Christopher Kuner, 'A Super-Right to Data Protection? The Irish Facebook Case and the Future of EU Data Transfer Regulation' (*LSE Media Policy Project Blog*, December 2014) <http://blogs.lse.ac.uk/mediapolicyproject/2014/06/24/a-super-right-to-data-protection-the-irish-facebook-case-the-future-of-eu-data-transfer-regulation/> accessed 25 August 2015.

is especially relevant if one considers the EU's Charter obligations under IHRL. The obligation to respect the right to data protection in its actions with external effects implies a negative duty of conduct. Similarly, the EU's duties to protect and fulfil this right impose positive obligations on the Union. This could amount to a requirement that the EU protect and fulfil its citizens' fundamental right to data protection beyond its territorial borders, perhaps justifying the aggressive jurisdictional scope of the DPD.

As the fundamental right to data protection morphs to carry more weight in the EU, this could amplify the EU's obligations under human rights law to protect its citizens' personal data when such data are processed outside EU territory. To extrapolate this further, perhaps the EU is moving beyond being simply an economic and political union to something closer to a global fundamental rights actor or norm setter.

*doi:10.1093/idpl/ipv023*
*Advance Access Publication 28 September 2015*