Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States

Federico Fabbrini*

On April 8, 2014, the European Union Court of Justice ("ECJ") delivered a milestone ruling on the protection of human rights in the digital age. In the case of Digital Rights Ireland*, the ECJ declared the Data Retention Directive—an EU legislative act requiring telecommunications service providers to retain for up to two years all metadata from every EU citizens' emails, text messages, and telephone calls, and to make these available to national security agencies for investigatory purposes—to be in violation of the rights to privacy and data protection enshrined in the European Union Charter of Fundamental Rights. The purpose of this Article is to examine the ECJ's decision, making it accessible to an international audience. The Article explains the decision's context and content by surveying the European Union's ("EU") constitutional framework for privacy and data protection and detailing the ECJ's legal reasoning. It clarifies how the ECJ's decision in* Digital Rights Ireland *builds upon previous national security cases and discusses its implications for the protection of human rights in a developing technological era—both in the EU and globally. As the Article argues, the ECJ's ruling striking down the Data Retention Directive will shape the EU's approach to issues of privacy and data protection. However, as the Article suggests, the ECJ's ruling may also carry some lessons for other countries, especially the United States. As U.S. institutions and the American public debate possible reforms of the U.S. surveillance program,* Digital Rights Ireland *makes a strong case for strengthening—rather than weakening—privacy protections in light of the greater capacity of governments to use new technology to systematically monitor individuals. It also underlines how the distinction between retention of metadata by private companies and by*

* Associate Professor of European & International Law, iCourts (Center of Excellence on International Courts), Faculty of Law, University of Copenhagen, and Coordinator of the Research Group on "Constitutional Responses to Terrorism" within the International Association of Constitutional Law. Email: Federico.Fabbrini@jur.ku.dk. This research is funded by the Danish National Research Foundation Grant no. DNRF105.

government agencies does not make a real difference, as it is the retention itself—not the status of the retaining institution—that alters the relationship between citizen and government in a way that is inimical to democratic society. As such, the ECJ's ruling provides a model to reaffirm and update privacy rights in the new digital age.

Introduction

The revelations of a secret program of dragnet surveillance of electronic communications by the U.S. National Security Agency ("NSA") have sparked a global debate about data protection and privacy rights in the struggle against terrorism. In a harsh report published in January 2014, the Civil Liberties Committee of the European Parliament accused the NSA of systemic infringement on the privacy rights of EU citizens and called for a profound overhaul of the transatlantic legal framework of cooperation in the field of counterterrorism.[1] At the same time, in December 2013, a special review group established by the U.S. President presented a report advancing forty-six far-reaching recommendations to reform the NSA's surveillance authority to strike a better balance between liberty and security in the digital age.[2] Under pressure from a lower court,[3] and bi-partisan concerns in both houses of Congress,[4] President Obama publicly outlined a new plan for U.S. government electronic surveillance, which, while confirming some of the authority currently granted to the NSA,[5] sought to allay the fears of civil rights advocates and prevent the consolidation of a surveillance state.[6] A key piece in the reform puzzle advanced by President Obama is the decision to remove from governmental control the retention of metadata of elec-

1. Comm. on Civil Liberties, Justice and Home Affairs, Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs, Eur. Parl. Doc., 17–19, 2013/2188(INI) (Jan. 8, 2014), *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN, *archived at* http://perma.cc/KHA7-YNL2 (calling upon U.S. authorities to prohibit blanket mass surveillance activities and bulk processing of personal data).

2. *See generally* The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, *archived at* http://perma.cc/8FM4-QV77.

3. Klayman v. Obama, 957 F.Supp.2d 1, 37 (D.D.C. 2013) (ruling that the plaintiffs were likely to succeed in showing that NSA telephone metadata program was unconstitutional).

4. *See, e.g.*, USA Freedom Act, H.R. 3361, 113th Cong. (2013), S. 1599, 113th Cong. (2013) (a bill jointly sponsored by U.S. Senator Patrick Leahy and U.S. Representative Jim Sensenbrenner purporting to end the program through which the NSA vacuums up the metadata generated in electronic communications).

5. *See* USA Patriot Act § 215, 50 U.S.C. § 1861 (2012) (regulating access to business records for foreign intelligence and international terrorism investigations).

6. *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) transcript *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence, *archived at* http://perma.cc/EJ7D-7CD2.

tronic communications by shifting it to private companies. Under the proposal, the U.S. government would no longer retain information about the date, time, length, and location of phone calls or emails for future counterterrorism investigation purposes. Rather, this data would be handled by telecommunications providers and made available by them to national security and law enforcement authorities based only on justified reasons.[7]

Yet on April 8, 2014, only a few months after President Obama released his recommendations, the Grand Chamber of the ECJ delivered a milestone decision, ruling that the EU legal regime for data retention—which relied on private companies handling metadata generated in the course of electronic communications for law enforcement purposes, exactly as envisaged in the Obama plan—violated the right to data protection and privacy enshrined in the EU Charter of Fundamental Rights.[8] The ECJ judgment striking down the Data Retention Directive[9] provides a clear-cut rebuttal to the idea that data protection and privacy rights will be better secured from government interference by simply shifting the retention of metadata generated through electronic communications to the private sector. Thus, the judgment provides a remarkable warning to U.S. policymakers, offering guideposts that are worth considering as the United States moves toward an overhaul of its surveillance regime in the coming years.

The purpose of this Article is to analyze the ECJ's decision in *Digital Rights Ireland Ltd v. Minister for Communication et al, and Kärtner Landesregierung*, and discuss its significance for an international audience. The Article examines the legal regimes established by the EU to protect data while at the same time retaining information considered relevant for the fight against terrorism. It contextualizes the ECJ's decision by exploring the broader challenges that the adoption of the Data Retention Directive raised in a number of EU member states. Further, it evaluates the implications that the ECJ's ruling will have in the EU, and considers what lessons it might offer to the United States. The Article maintains that *Digital Rights Ireland* represents a milestone decision—arguably the most advanced court pronouncement to date—in the area of privacy rights in the digital age. The effects of the ECJ's decision may extend beyond the borders of the EU by enshrining in clear, more-explicit-than-ever language the idea that core constitutional protections of privacy rights must be strengthened—not weakened—in an era of increasing digitalization in which governments have acquired greater technological capacity to surveil citizens on a mass scale. Thus, the ECJ's decision provides arguments for further trans-

7. *Id.*

8. Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238.

9. Council Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks, 2006 O.J. (L 105) 54 [hereinafter Data Retention Directive].

national enhancement of personal data and privacy rights protections and may serve as a model for other jurisdictions to consider in their own reform processes.

Specifically, the ECJ's judgment casts doubts on the plans ongoing in the United States to transfer the management and retention of personal metadata to the private sector. As the ECJ unequivocally indicates, the suggestion that data retention by telephone and internet service providers will reduce the risk of abuse does not hold true. If direct governmental control over the personal metadata of every citizen may be reminiscent of George Orwell's *1984*,[10] the retention of data by private companies is also liable to interfere with the private life of citizens in a way that, according to the ECJ, is not strictly necessary in a democratic society for the prevention of crime or the protection of national security. Viewed from this perspective, the ECJ's judgment therefore opens up an entirely new set of questions about whether constitutional systems based on the rule of law should authorize the systematic collection of personal data, either by national security agencies or by private companies. Ultimately, the ECJ's decision in *Digital Rights Ireland* makes a strong case in favor of strengthening privacy protections in the digital age and abandoning sweeping programs of data retention that alter at their roots the relationship between citizens and government in a democratic society.

Part I of this Article outlines the EU legal regime for the protection of privacy in electronic communications, examines the context and content of the Data Retention Directive, and summarizes the challenges that were raised against this EU piece of legislation at the national and supranational level. Part II focuses in depth on the ECJ's judgment in *Digital Rights Ireland* and explains its reasoning. Part III evaluates the ECJ's decision, arguing that it constitutes a watershed for privacy and data protection in Europe, and considers its implications for the EU and its member states. Part IV then discusses the implications of the ECJ's judgment from a broader, global perspective, considers the latest proposals advanced in the United States to overhaul the NSA surveillance regime, and suggests lessons the ECJ's decision may offer for those proposals.

I. The EU Data Protection and Data Retention Frameworks

In the multilevel European architecture for the protection of fundamental rights,[11] the right to privacy is entrenched in the laws and constitutions of the member states, in the European Convention on Human Rights

10. *See generally* George Orwell, Nineteen Eighty-Four (1949).

11. *See generally* Federico Fabbrini, Fundamental Rights in Europe: Challenges and Transformations in Comparative Perspective (2014) (examining the European multilevel system for the protection of fundamental rights in comparison with the U.S. federal system).

("ECHR"), and in the Treaties and legislation of the EU.[12] At the state level, the right to privacy and data protection is explicitly recognized in the constitutions of a number of EU member states, notably those enacted in Central and Eastern Europe after the end of the Cold War,[13] where practices of systemic government surveillance were commonplace.[14] In other member states, especially in Western and Southern Europe, where privacy and data protection are not textually enshrined in domestic basic laws, constitutional courts have consistently interpreted their domestic laws as protecting these rights.[15] Moreover, all member states of the EU are subject to the ECHR, Article 8 of which protects everyone's "right to respect for his private and family life, his home and his correspondence."[16] In its case law, the European Court of Human Rights ("ECtHR") has progressively expanded the scope of the right to privacy, holding that Article 8 of the ECHR also safeguards a right to data protection.[17]

Yet, whereas the ECtHR has often extended—within the framework of the ECHR—a margin of appreciation[18] to the member states when privacy rights have clashed with national security concerns,[19] EU law has signifi-

12. For a comprehensive survey of the legal instruments and mechanisms for the protection of privacy in the European multilayered human rights system, see Eur. Union Agency for Fundamental Rights, *Data Protection in the European Union: the Role of National Data Protection Authorities* (May, 2010) *available at* http://fra.europa.eu/en/publication/2012/data-protection-european-union-role-national-data-protection-authorities, *archived at* http://perma.cc/W8VM-WXJF.

13. *See, e.g.*, Konstytucja Rzeczypospolitej Polskiej, Apr. 2, 1992, art. 47 (Pol.) (stating that "[e]veryone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life"); Romania Const. art. 26 (stating that "[t]he public authorities shall respect and protect the intimate, family and private life").

14. *See, e.g.*, Timothy Garton Ash, The File: A Personal History (1997) (discussing surveillance by secret police in East Germany).

15. *See, e.g.*, Corte Cost. (Constitutional Court), 26 marzo 1990, n. 139, Racc. uff. corte cost. 1990, Vol. 94, 801 (It.) (stating that the Italian Constitution protects a right to privacy); Conseil Constitutionnel [CC] [Constitutional Court] decision No. 94-352DC, Jan. 18, 1995 (Fr.) (stating that the right to privacy is implied in the constitutional sources of law through which the court reviews legislation). On the jurisprudence of the German Constitutional Court recognizing a right to data protection, see *infra* text accompanying notes 62–66.

16. Convention for the Protection of Human Rights and Fundamental Freedoms [ECHR], art. 8, Nov. 4, 1950, E.T.S. No. 5.

17. *See generally* Lee Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, 6 Int'l J. L. & Info. Tech. 247 (1998) (discussing rulings by the European Court of Human Rights [ECtHR] in the field of privacy and data protection).

18. The margin of appreciation is a doctrine that the ECtHR has developed to accord a degree of discretion to the contracting parties when implementing the ECHR. In practice, the application of the margin of appreciation means that the ECtHR employs a deferential standard of review to states' action. *See generally* Thomas A. O'Donnell, *The Margin of Appreciation Doctrine: Standards in the Jurisprudence of the European Court of Human Rights*, 4 Hum. Rts. Q. 474 (1982); Judith Resnik, *Federalism(s)' Forms and Norms: Contesting Rights, De-Essentializing Jurisdictional Divides, and Temporizing Accommodations, in* Nomos LV: Federalism and Subsidiarity 393 (James Flemming & Jacob Levy eds., 2014) (comparing the margin of appreciation to techniques of judicial deference in the United States).

19. *See* Weber & Saravia v. Germany, App. No. 54934/00 2006-XI Eur. Ct. H.R., ¶¶ 137–38 (2006). The ECtHR rejected as manifestly ill-founded the complaint raised against the German legislation, which regulated the powers of the federal intelligence agencies to record foreign telecommunications in the course of strategic monitoring operations, holding that it was "satisfied that the respondent State, within its fairly wide margin of appreciation in that sphere, was entitled to consider the interfer-

cantly boosted the protection of privacy.[20] In particular, the EU Charter of Fundamental Rights ("The Charter"), enacted in 2000 and entered into force in 2009 as a constitutional document that legally binds EU institutions and the member states (when acting within the scope of EU law), has codified in EU primary law two provisions dealing with privacy and data protection. Pursuant to Article 7 of the Charter (entitled "Respect for Private and Family Life"), "[e]veryone has the right to respect for his or her private and family life, home and communications."[21] At the same time, Article 8 of the Charter (entitled "Protection of Personal Data") reads:

> Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.[22]

Confirming the centrality that data protection plays in the legal order of the EU,[23] Article 16 of the Treaty on the Functioning of the EU ("TFEU"),[24] introduced by the Treaty of Lisbon, which entered into force in 2009,[25] restates that "[e]veryone has the right to the protection of personal data concerning them" and empowers the EU legislature—the European Parliament jointly with the Council—to:

> [L]ay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.[26]

---

ences with the secrecy of telecommunications resulting from the impugned provisions to have been necessary in a democratic society in the interests of national security." *Id.*

20. *See* Maria Tzanou, The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement (2012) (unpublished Ph.D. thesis, European University Institute) (on file with author).

21. Charter of Fundamental Rights of the European Union art. 7, 2010 O.J. (C 83) 391, 393 [hereinafter Charter of Fundamental Rights].

22. *Id.* art. 8.

23. *See generally* Stefano Rodotà, *Data Protection as Fundamental Rights*, *in* REINVENTING DATA PROTECTION 77 (Paul de Hert et al. eds., 2009).

24. Consolidated Version of the Treaty on the Functioning of the European Union, May 9, 2008, 2008 O.J. (C 115) 47 [hereinafter TFEU].

25. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1 [hereinafter Treaty of Lisbon].

26. TFEU, *supra* note 24, art. 16.

At the legislative level, since 1995 the EU has been endowed with a comprehensive framework regulating privacy and data protection in the context of commercial transactions.[27] Adopted at the time under the power of the EU to regulate the functioning of the internal market, Directive 95/46[28]—the so-called Data Protection Directive—introduced an obligation for member states to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data"[29] within their jurisdictions.[30] The Data Protection Directive specifies that personal data shall be processed only on the basis of "qualitative principles," including the requirement that data collection be proportionate to the purpose for which it is undertaken,[31] and generally subject to the consent of the data subject.[32] It prohibits the processing of sensitive data, such as those revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . [information] concerning health or sex life."[33] Additionally, it

27. *See* Julia Fromholz, *The European Union Data Privacy Directive*, 15 Berk. Tech. L.J. 461, 462 (2000). *See generally* Spiros Simitis, *From the Market to the Polis: the EU Directive on the Protection of Personal Data*, 80 Iowa L. Rev. 445 (1995).

28. 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 [hereinafter Data Protection Directive].

29. *Id.* art. 1.

30. *Id.* art. 4 ("Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State . . . (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law . . .").

31. *Id.* art. 6(1) ("Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.").

32. *Id.* art. 7 ("Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).").

33. *Id.* art. 8(1).

requires that data users be informed about the collection,[34] and empowers users to obtain access to the data and to demand rectification, blocking, or erasure of the data when needed.[35] Since the adoption of the 2001 EU regulation on the protection of individuals with regard to the processing of personal data by the Community institutions, which also established the European Data Protection Supervisor, EU institutions must also respect the same principles when processing personal data.[36]

Sectorial pieces of legislation have expanded the protections of privacy and personal data to newly emerging, or particularly sensitive, technological sectors.[37] Hence, Directive 2002/58 updated the principles of the Data Protection Directive to the electronic communication sector, harmonizing member states' laws to ensure an equivalent level of protection of fundamental rights and freedoms—in particular, the rights to privacy and confidentiality—with respect to processing of personal data in electronic communications.[38] An EU Council Framework Decision on the protection of personal data in the framework of police and judicial cooperation in criminal matters[39] was adopted in 2008 in the field of Justice and Home Affairs ("JHA")—an area of EU policymaking in which special rules applied until the entry into force of the Lisbon Treaty in 2009.[40] Moreover, specific pieces of EU data protection legislation apply to other programs of police cooperation between the EU member states, such as the Council decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime,[41] and the Council decision establishing the European Police Office ("Europol").[42]

Yet the EU data protection framework allows for certain exceptions authorizing member states to restrict the rights proclaimed in the Data Protection Directive for reasons of national security. This exception is a consequence of the division of competences between the EU and the mem-

34. *Id.* art. 10.

35. *Id.* art. 12.

36. Commission Regulation 45/2001/EC, The Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data, 2001 O.J. (L 8) 1; *see also* Hielke Hijmans, *The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority*, 43 Comm. Mk. L. Rev. 1313, 1314 (2006).

37. *See generally* Konrad Lachmayer, *Rethinking Privacy Beyond Borders: Developing Transnational Rights on Data Privacy*, 20 Tilburg L. Rev. 78 (2015).

38. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector 2002 O.J. (L 201) 37.

39. Council Decision 2008/977/JHA, 2008 O.J. (L 350) 60 (EC).

40. *See generally* Eulalia Sanfrutos Cano, *The End of the Pillars? A Single EU Legal Order After Lisbon*, *in* Law and Outsiders 67 (Cian Murphy et al. eds., 2011) (explaining the evolving rules for the adoption of legislation in the field of JHA, which required unanimity in the Council until the entry into force of the Lisbon Treaty in 2009 and are now subject instead to normal voting rules).

41. Council Decision 2008/615/JHA, 2008 O.J. (L 210) 1 (EC).

42. Council Decision 2009/371/JHA, 2009 O.J. (L 121) 37 (EC).

ber states, which is constitutionalized in the EU Treaties.[43] The EU has some authority to legislate in the field of security,[44] and has already adopted various measures coordinating member states' law enforcement activities or establishing *tout-court* EU counterterrorism and security policies.[45] Nevertheless, under Article 4(2) of the EU Treaty, "national security remains the sole responsibility of each Member State."[46] The Data Protection Directive therefore allows the member states to adopt legislative measures to restrict the scope of their obligations and rights provided in the Directive if they are:

> [N]ecessary measure[s] to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters.[47]

In the aftermath of 9/11, some EU member states introduced exceptions to EU data protection rules. In particular, they required internet and telephone service providers to retain metadata about electronic communications and to make them available to law enforcement agencies if needed.[48] These exceptions resulted in a patchwork of state legislations during the early twenty-first century, which derogated to varying degrees from EU data protection principles and established different rules on the retention of data by electronic communication providers.[49]

It was with the aim of harmonizing these different national laws that the Data Retention Directive was adopted in 2006.[50] As clarified in the recitals of the Directive, "[s]everal Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably."[51] However:

---

43. *See generally* Robert Schütze, From Dual to Cooperative Federalism: The Changing Structure of European Law (2009).

44. Treaty of Lisbon, *supra* note 25, art. 3(2) ("The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to. . . the prevention and combating of crime.").

45. *See generally* Valsamis Mitsilegas et al., The European Union and Internal Security (2003).

46. Treaty of Lisbon, *supra* note 25, art. 4(2).

47. Data Protection Directive, *supra* note 28, art. 13.

48. *See, e.g.*, Criminal Justice (Terrorist Offenses) Act, 2005, § 64, (Ir.) (Irish law requiring telecommunication providers to retain traffic for a period of three years for the purpose of preventing crime and safeguarding the security of the state).

49. *See* Data Retention Directive, *supra* note 9, pmbl; *see also* Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chi. J. Int'l L. 233 (2007–08).

50. Data Retention Directive, *supra* note 9, art. 1.

51. *Id.* recital 5.

> The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.[52]

To address this situation, the Data Retention Directive required member states to adopt domestic measures ensuring the retention of metadata generated by telecommunication service providers.[53] Specifically, Article 5 of the Data Retention Directive required member states to adopt legislation imposing on IT or telephone companies a duty to store and retain the data relating to the source, addressee, date, time, length, and type of communication[54]—although not the content of the communication itself.[55] As stated in Article 6, retention must last for a period of not less than six months and not more than two years.[56] Pursuant to Article 4 of the Directive, member states must regulate in national laws the conditions for access to this data in accordance with necessity and proportionality requirements, and consistent with EU and ECHR law.[57] Yet the Directive leaves discretion to member states in defining the conditions that justify access to the retained data, as indicated in the general formula of Article 1, which reads, "the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law."[58]

The Data Retention Directive brought about an important interference with the right to data protection.[59] In fact, the transposition of the Directive into the law of the EU member states raised a number of constitutional challenges in countries endowed with advanced domestic standards of privacy protection—including in Romania,[60] the Czech Republic,[61] and Ger-

52. *Id.* recital 6.

53. *Id.* art. 3.

54. *Id.* art. 5(1).

55. *Id.* art. 5(2).

56. *Id.* art. 6.

57. *Id.* art. 4 ("Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR.").

58. *See id.* art. 1.

59. *See generally* Arianna Vedaschi & Valerio Lubello, *Data Retention and its Implications for the Fundamental Right to Privacy: A European Perspective*, 20 Tilburg L. Rev. 14 (2015).

60. Curtea Constituţională [Constitutional Court] decision No. 1258, Oct. 8, 2009 (Romania) (holding that the national law implementing the Data Retention Directive violates constitutional and ECHR data protection principles).

61. Nález Ústavního soudu ze dne 22.5.2011, (ÚS) [Decision of the Constitutional Court of March 22, 2011], Pl. ÚS 24/10 (Czech) (holding the national law implementing the Data Retention Directive unconstitutional).

many.[62] The German case raised particular attention. The German Federal Constitutional Court (*Bundesverfassungsgericht*) has consistently ruled that the right to informational self-determination constitutes a fundamental right protected under the German Basic Law,[63] and recent case law has confirmed the great care with which the Constitutional Court scrutinizes legislation for compatibility with data protection principles.[64] Building on its established case law, the German Constitutional Court declared unconstitutional the German Act implementing the EU Data Retention Directive at the domestic level, holding that the Act created "a feeling of surveillance" and failed to put sufficient limits on the use that could be made of stored data.[65] However, the German Constitutional Court—just like sister national courts—explicitly refrained from ruling on the validity of the Data Retention Directive itself, and only required national legislatures to introduce domestic provisions that increased the safeguards and protections for privacy and personal data within the space permitted by the Directive.[66]

The Data Retention Directive was also directly challenged in front of the ECJ by Ireland.[67] However, the case focused on a technical question concerning its legal basis:[68] Ireland, in particular, doubted whether the EU institutions had rightly enacted the Data Retention Directive on the basis of the power to regulate the functioning of the internal market, as the Directive mainly pursued the aim of fighting crime and terrorism, and therefore ought to have been approved under the power of the EU to set rules in the area of JHA (which required, at the time, the unanimous consent of the member states represented in the Council).[69] As a result of this legal focus, Ireland did not raise the question of the compatibility between the Data Retention Directive and the right to data privacy. In fact, as I have argued

62. Bundesverfassungsgericht [BVerfG] (Constitutional Court) Mar. 2, 2010, 125 BVerfGE 261 (Ger.).

63. *See* Mikrozensusurteil, BVerfG Jul. 16, 1969, 27 BVerfGE 1, 6 (Ger.) (on the right to privacy in the field of statistics); Volkszählungsurteil, BVerfG Dec. 15, 1983, 65 BVerfGE 1 (Ger.) (on the right to informational self-determination in matters related to the census); for more information on Volkszählungsurteil, see Gerrit Hornung & Christoph Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, 25 Computer L. & Sec. Rev. 84, 86 (2009).

64. *See* BVerfG, Mar. 3, 2004, 110 BVerfGE 33 (on the right to privacy in domestic interception of communications); BVerfG, Apr. 4, 2006, 115 BVerfGE 320 (on the right to informational self-determination in the field of computer profiling); *see also* Hornung & Schnabel, *supra* note 63.

65. BVerfG, 125 BVerfGE 261; *see also* Christian De Simone, *Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive*, 11 German L.J. 291 (2010).

66. BVerfG, 125 BVerfGE 261.

67. Case C-301/06 Ir. v. Parliament and Council of the Eur. Union, 2009 E.C.R. I-953.

68. *See* Sara Poli, *The Legal Basis of Internal Market Measures with a Security Dimension: Comment on Case C-301/06, Ireland v. Parliament/Council*, 6 Eur. Const. L. Rev. 137 (2010).

69. *See* Council Decision 2008/615/JHA, 2008 O.J. (L 210) 1 (EC).

elsewhere,[70] Ireland was not concerned with issues of human rights, as it had one of the toughest state regimes on data retention for law enforcement purposes at the time, and was actually challenging the Data Retention Directive because it would have forced it to increase the domestic protections applying to the retention of personal data processed in the context of electronic communications. In the end, although the ECJ dismissed Ireland's complaint, ruling that the Data Retention Directive was correctly adopted on the basis of the inter-state commerce power of the EU,[71] it did not address the compatibility of the Directive with fundamental rights.[72] Ironically, however, the fatal challenge to the Data Retention Directive would come, once more, from Ireland—as well as from Austria.

II. The ECJ's Judgment

In 2012, the Irish High Court and the Austrian Constitutional Court (*Verfassungsgerichthof*) asked the ECJ to rule on the legality of the EU Data Retention Directive. In the multilayered EU constitutional architecture, individuals can raise facial challenges to EU legal measures that directly and individually affect them.[73] However, because the EU mostly adopts legislation that is then implemented by the member states,[74] the main avenue to challenge the legality of EU legislation is to begin proceedings in front of state courts.[75] Whenever the validity or interpretation of an EU measure is at stake, state courts of last instance have an obligation to refer the question to the ECJ, pursuant to what is called the preliminary reference procedure.[76] In the present case, both the Irish High Court and the Austrian Constitutional Court had been called on to rule by individual applicants—in the Austrian case the Court was also called upon by the government of Carinthia, a province in the Austrian federal system of government—who complained that the national implementing measures of the EU Data Re-

70. Federico Fabbrini, *Lotta al terrorismo e tutela dei dati personali nell'Unione Europea alla luce della sentenza Irlanda c. Parlamento e Consiglio*, 29 Quaderni Costituzionali 419 (2009).

71. Case C-301/06 Ir. v. Parliament, § 93.

72. *Id.* § 57.

73. *See* TFEU, *supra* note 24, art. 263 ("[A]ny natural or legal person may, under the same conditions, institute proceedings against a decision addressed to that person or against a decision which, although in the form of a regulation or a decision addressed to another person, is of direct and individual concern to the former."); *see also* Xavier Lewis, *Standing of Private Plaintiffs to Annul Generally Applicable European Community Measures*, 30 Fordham Int'l L.J. 1496 (2003).

74. *See* Daniel Halberstam, *Comparative Federalism and the Issue of Commandeering*, *in* The Federal Vision: Legitimacy and Levels of Governance in the United States and the European Union 213 (Kalypso Nicolaïdis & Robert Howse eds., 2001) (explaining that in most contexts, the EU delegates implementation of laws to the member states).

75. *See generally* Monica Claes, The National Court's Mandate in the European Constitution (2006) (explaining the role of national courts in enforcing EU law).

76. *See* TFEU, *supra* note 24, art. 267 (stating that the ECJ "shall have jurisdiction to give preliminary rulings concerning (a) the interpretation of the Treaties; [and] (b) the validity and interpretation of acts of the institutions of [the Community]" upon referral by a national court).

tention Directive violated fundamental principles of privacy and data protection.[77] Because these cases turned on a question of EU law, both the Irish High Court and the Austrian Constitutional Court sent a preliminary reference to the ECJ, "essentially asking the [ECJ] to examine the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter."[78]

Given the similarity between the cases, the ECJ decided to join the preliminary references by the Irish and Austrian courts. In December 2013, Advocate General ("AG") Cruz Villalón delivered his Opinion[79]—providing independent legal advice to the ECJ judges on how they should decide the case.[80] In his Opinion, the AG discussed the significance of Article 52 of the EU Charter of Fundamental Rights, which sets conditions for the limitations of the rights enshrined in the Charter.[81] The Opinion also reflected upon the differences between the right to privacy and the right to data protection, which he regarded as a species within the broader genus of privacy rights.[82] Ultimately, the AG recommended that the ECJ declare the Data Retention Directive, as a whole, incompatible with Article 52 of the EU Charter of Fundamental Rights, or that it strike down Article 6 of Directive 2006/24 (allowing retention of data for up to two years) as a violation of the right to privacy enshrined in Article 7 of the EU Charter of Fundamental Rights.[83] Signaling its attention to the case, the ECJ decided to hear the preliminary references as a Grand Chamber—a special 15-judge composition reserved for high-profile cases—and, on April 8, 2014, delivered its ruling.[84]

After summarizing the law and the facts, the ECJ began its analysis by underlining how Articles 7, 8, and 11 of the Charter of Fundamental Rights were relevant with regard to the question of the validity of the Data Retention Directive. The ECJ explained that the Data Retention Directive

77. Digital Rights Ir. Ltd v. Minister for Commc'n et al., [2010] 3 I.R. 251 § 52 (H. Ct.) (Ir.); Verfassungsgerichtshof [VfGH] [Constitutional Court], Nov. 28, 2012, Erkenntnisse und Beschlüsse des Verfassungsgerichtshofes [VfSlg] No. 19702/2012, art. 3, ¶ 1 (Austria).

78. Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238, § 23.

79. Opinion of Advocate General Villalón, Digital Rights Ireland Ltd v. Minister for Communication et al. and Kärtner Landesregierung et al., Joined Cases C-293/12 & C-594/12 [hereinafter Opinion of Advocate General Villalón].

80. *See* Protocol No. 3 on the Statute of the European Court of Justice, art. 20, 2010 O.J. (C 83) 210, 215 (stating that as a general rule, the ECJ shall decide cases only after having received a submission from the Advocate General, save for when a case raises no new point of law). The Advocate Generals' opinions often play an influential role in the ECJ's deliberations; however, the Advocate Generals' opinions technically have no binding effect. Paul Craig and Gráinne de Búrca, EU Law: Texts, Cases, and Materials 62 (5th ed. 2011). There are multiple cases in which the ECJ has not followed the Advocate General's opinion in its ruling. *See, e.g.*, *id.* at 405, 663.

81. Opinion of Advocate General Villalón, *supra* note 79, § 89.

82. *Id.* § 61.

83. *Id.* § 159.

84. Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238.

required the collection and storage of metadata produced in electronic communications and stated that:

> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[85]

Hence, although Directive 2006/24 did "not permit the retention of the content of the communication,"[86] according to the ECJ, "it is not inconceivable that the retention of the data in question might have an effect . . . on their exercise of the freedom of expression guaranteed by Article 11 of the Charter."[87] At the same time, the retention "directly and specifically affects private life and, consequently, the rights guaranteed by Article 7 of the Charter. Furthermore, such retention of data also falls under Article 8 of the Charter because it constitutes the processing of personal data . . . ."[88]

Having clarified that Articles 7, 8 and 11 were relevant in the case, the ECJ started reviewing the Directive, focusing specifically on the possible violation of the rights to privacy and data protection.[89] Following the approach that is also customary in the ECHR,[90] the ECJ raised the following questions: first, whether the Data Retention Directive constituted an interference with Articles 7 and 8 of the EU Charter of Fundamental Rights; and second, whether such interference was justified. On the first point, the ECJ quickly settled the issue, holding that the obligation imposed by Articles 3 and 6 of Directive 2006/24 to retain the metadata "constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter."[91] Furthermore, according to the ECJ, that national authorities could access these data "constitute[d] a further interference with that fundamental right."[92] Likewise, the ECJ underlined how the Directive also restricted Article 8 of the Charter of Fundamental Rights,[93] and it emphasized how the interference produced by Directive 2006/24 was "wide-ranging" and

85. *Id.* § 27.
86. *Id.* § 28.
87. *Id.*
88. *Id.* § 29.
89. *Id.* § 70 (In light of its finding concerning Articles 7 and 8 of the Charter, the ECJ did not find it necessary to rule whether the Data Retention Directive was also in violation of Article 11 of the Charter.).
90. Klass and Others v. Germany, App. No. 5029/71, 28 Eur. Ct. H.R. (Ser. A), §§ 41, 46 (1978) (assessing first whether a law authorizing the secret services to carry out secret monitoring of postal and telephone communications constitutes an interference with Article 8 of the ECHR and, second, whether such interference is justified).
91. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, § 34.
92. *Id.* § 35.
93. *Id.* § 36.

"particularly serious."[94] Citing the AG's opinion, in particular, the ECJ underlined how "the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance"[95]—a concern originally voiced by the German Constitutional Court.[96]

On the second question, whether the interference with the right guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights was justified, the ECJ set aside the argument raised by some of the parties that Directive 2006/24 violated the essence of the right to privacy. The ECJ acknowledged that the Data Retention Directive pursued a legitimate "objective of general interest,"[97] namely the "fight against serious crime,"[98] and the "fight against international terrorism in order to maintain international peace and security."[99] However, the ECJ ruled that the Data Retention Directive interfered with the right to privacy in a disproportionate way. Summarizing the conventional multi-tier test developed in its case law (and in comparative constitutional law more generally) used to verify the proportionality of a measure restricting fundamental rights,[100] the ECJ recalled that "the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives."[101] At the same time, citing the ECtHR,[102] the ECJ clarified that the nature of its review would be stricter in this case, "in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24."[103]

According to the ECJ, the Data Retention Directive met the first tier of the proportionality analysis—the so-called "suitability test." Directive 2006/24, in fact, was suited to the objective of expanding national authorities' "opportunities to shed light on serious crime."[104] Yet according to the ECJ, the Data Retention Directive did not pass the second tier of the proportionality analysis—the so-called "necessity test." As the ECJ put it:

94. *Id.* § 37.
95. *Id.* § 37.
96. *See supra* text accompanying note 65.
97. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, § 44.
98. *Id.* § 41.
99. *Id.* § 42.
100. *See generally* Alec Stone Sweet & Jud Mathews, *Proportionality, Balancing and Global Constitutionalism*, 47 Colum. J. Transnat'l L. 72 (2008–09).
101. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, § 46.
102. *See* S. and Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04, [2008] Eur. Ct. H.R. 1581, § 134 (2008) (finding the United Kingdom in violation of Article 8 of the ECHR).
103. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, § 48.
104. *Id.* § 49.

> [T]he fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.[105]

In particular, the ECJ underlined that the Data Retention Directive set up a regime that failed to limit interference with privacy rights "to what is strictly necessary,"[106] suggesting emphatically that, on the contrary, the Data Retention Directive "entail[ed] an interference with the fundamental rights of practically the entire European population."[107]

In the ECJ's view, five major faults doomed the legality of Directive 2006/24. First, the Directive did not set any limit on the personal scope of application: the Directive "affects, in a comprehensive manner, all persons using electronic communications services . . . . It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[108] Second, the Directive did not set any limits on the possibility of national authorities accessing the data retained by private companies, and failed to specify conditions that justify the use of these data for law enforcement purposes: "[o]n the contrary, Directive 2006/24 simply refer[red], in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law"[109] and did not make access dependent "on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities . . . ."[110] Third, the Directive did not set a sufficiently restrictive timeframe for the retention of data: "Article 6 of Directive 2006/24 requires that . . . data be retained for a period of at least six months, without any distinction . . . between the categories of data set out in Article 5 . . . on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned."[111] Fourth, the Directive did not provide for sufficient safeguards relating to the security and protection of the data retained by private providers of electronic communications.[112] Finally, the Directive

105. *Id.* § 51.
106. *Id.* § 56.
107. *Id.*
108. *Id.* § 58.
109. *Id.* § 60.
110. *Id.* § 62.
111. *Id.* § 63.
112. *Id.* § 66.

did "not require the data . . . to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security . . . is fully ensured."[113]

In light of these serious flaws in the Data Retention Directive, the ECJ ruled that "the EU legislature ha[d] exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter"[114] and struck down the Directive, making it immediately inapplicable in the EU legal order.[115]

III. The ECJ and the Protection of Human Rights in the Digital Age

The decision by the ECJ in *Digital Rights Ireland* constitutes a watershed for the protection of human rights in the digital age. The ruling crowns a decade of progressive jurisprudential developments in the field of human rights, in which the ECJ has established itself as a leading forum for the protection of fundamental rights and liberties. Yet it also constitutes a major leap forward, which is likely to shape the way in which the EU defines its counterterrorism strategy for years to come, and to influence how courts and political branches strike the balance between liberty and security, globally.

As I have argued in my book, *Fundamental Rights in Europe*,[116] in recent years, the ECJ's jurisprudence has become a benchmark for the protection of fundamental rights in the European multilevel human rights system. Inspired by the Charter of Fundamental Rights (adopted in 2000, and binding since 2009),[117] and subject to a virtuous dynamic of competition with the ECtHR,[118] the ECJ has lately delivered a series of remarkable decisions on human dignity,[119] non-discrimination on the basis of gender[120] or sexual

113. *Id.* § 68.
114. *Id.* § 69.
115. *Id.* § 71.
116. *See generally* Fabbrini, *supra* note 11 (especially chapter 1).
117. Dinah Shelton, *Remedies and the Charter of Fundamental Rights of the European Union*, *in* The European Charter of Fundamental Rights: Politics, Law and Policy 349, 349 (Steve Peers and Angela Wards eds., 2004); Aida Torres Pérez, Conflicts of Rights in the European Union: A Theory of Supranational Adjudication 23 (2009).
118. *See* Lech Garlicki, *Cooperation of Courts: The Role of Supranational Jurisdictions in Europe*, 6 Int'l J. Con. L 509, 511 (2008); Sionaidh Douglas-Scott, *The European Union and Human Rights After the Treaty of Lisbon*, 11 Hum. Rts. L. Rev. 645, 678–82 (2011).
119. *See* Case C-36/02, Omega Spielhallen-und Automatenaufstellungs-GmbH v. Oberbürgermeisterin der Bundesstadt Bonn, 2004 E.C.R. I-9609 (recognizing a fundamental right to dignity as a justification for the limitation of the freedom of movement of goods).
120. *See, e.g.*, Case C-285/98, Tanja Kreil v Bundesrepublik Deutschlan, 2000 E.C.R. I-69 (declaring a provision of the German Constitution prohibiting women from serving in the military incompatible with EU law); Case C-46/07, Comm'n v. Italy, 2008 E.C.R. I-151 (declaring a provision of the Italian social security legislation setting up a different retirement age for men and women incompatible with EU law).

orientation,[121] freedom of expression,[122] social rights,[123] and political entitlements.[124] Moreover, the ECJ has been at the forefront of the protection of privacy and personal data,[125] as recently demonstrated by its decision in *Google Spain v. Agencia Española de Protección de Datos.*[126] In this case, the ECJ held that the Charter of Fundamental Rights secured a "right to be forgotten" and ruled that the operator of a search engine could be required to remove information about a data subject at her request, even if the information available online about the data subject was not unlawful.[127]

In its capacity as the constitutional court of the EU legal order,[128] the ECJ is empowered to review compliance with EU human rights both by the EU institutions and by the EU member states.[129] Much like in the United States, therefore, both the "federal" political branches of government and the component states must respect constitutional human rights and can be held accountable before the ECJ. Traditionally, the ECJ has been able to review whether legal measures adopted by EU member states comply with EU human rights law, either when the states implemented EU law (that is, when they used appropriate domestic legislative or administrative measures

121. *See, e.g.*, Case C-117/01, K.B. v. Nat'l Health Serv. Pensions Agency and Sec'y of State for Health, 2004 E.C.R. I-541 (recognizing the rights of transsexuals); Case C-423/04, Richards v. Sec'y of State for Work and Pensions, 2006 E.C.R. II-3585 (also recognizing the rights of transsexuals).

122. *See, e.g.*, Case C-112/00, Schmidberger, Internationale Transporte und Planzüge v. Republik Österreich, 2003 E.C.R. I-5659, §91 (recognizing the right to freedom of expression as a justification for the restriction of the freedom of movement); Case C-380/05, Centro Europa 7 Srl v. Ministero delle Comunicazioni e Autorità per le garanzie nelle comunicazioni, 2008 E.C.R. I-349 (declaring a provision of the Italian media law which did not ensure pluralism in the broadcasting system incompatible with EU law).

123. *See, e.g.*, Case C-184/99, Grzelczyk v. Centre public d'aide sociale d'Ottignies-Louvain-la-Neuve, 2001 E.C.R. I-6193 (recognizing the right of migrant students to obtain social security benefits in the host state); Case C-438/05, Int'l Transp. Workers' Fed'n and Finnish Seamen's Union v. Viking Line ABP and OÜ Viking Line Eesti, 2007 E.C.R. I-10779 (recognizing a fundamental right to strike).

124. *See, e.g.*, Case C-300/04, Eman & Sevinger v. College van burgemeester en wethouders van Den Haag, 2006 E.C.R. I-8055 (holding a Dutch law restricting the franchise to the EU Parliament of Dutch citizens residing in Aruba incompatible with EU law).

125. *See, e.g.*, Joined Cases C-465/00, C-138/01 & C-139/01, Rechnungshof v. Österreichischer Rundfunk and Others, 2003 E.C.R. I-4989 (holding that the provisions of the Data Protection Directive are directly applicable in that they may be relied on by an individual before the national courts to oust the application of rules of national law that are contrary to those provisions); Case C-518/07, Comm'n v. Germany, 2010 E.C.R. I-1885 (ruling that Germany violated the Data Protection Directive because it failed to ensure the independence of the national data protection supervisor while implementing the measure at the national level, as required by the Directive).

126. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (May 13, 2014) (not yet reported).

127. *See id.* ¶ 82. *See generally* Eleni Frantziou, *Further Developments in the Right to Be Forgotten*, 14 Hum. Rts. L. Rev. 761 (2014).

128. *See* Monica Claes & Maartje de Visser, *The Court of Justice as a Federal Constitutional Court: A Comparative Perspective*, *in* Federalism in the European Union 83, 100 (Elke Cloots et al. eds., 2012).

129. *See generally* Zdenek Kühn, *Wachauf and ERT: On the Road from the Centralized to the Decentralized System of Judicial Review*, *in* The Past and Future of EU Law: The Classics of EU Law Revisited on the 50th Anniversary of the Rome Treaty 151 (Miguel Maduro & Loic Azoulai eds., 2010).

to carry out a requirement of EU law),[130] or when they derogated from it (that is, when they sought an exception permitted by EU legislation to avoid applying an EU norm).[131] In recent years, however, the ECJ has expanded its reach in ways analogous to the incorporation by the U.S. Supreme Court of the U.S. Bill of Rights to the states,[132] extending the doctrine of the scope of application of EU law to apply its oversight to almost all state measures that bear some relation to EU law. It has also tightened the intensity of its scrutiny.[133]

At the same time, whereas in the past the ECJ had been accused of adopting a more demanding standard when reviewing EU member states' laws as opposed to when reviewing the law enacted by the EU institutions,[134] more recently the ECJ has proved itself willing and able to subject EU legal measures to strict scrutiny for compliance with EU human rights law.[135] In the area of national security in particular, the ECJ has turned out to be a bastion for the protection of human rights—despite the pressures emerging from the EU political branches of government for judicial deference and accommodation of counterterrorism concerns.[136] As Italian Constitutional Court Justice Marta Cartabia put it, in reference to national security issues:

> The EU judiciary experimented with its capacity of being rigorous in the protection of rights in one of the most thorny fields, given the fact that the seriousness of the international situation tends to attenuate sensitivity toward the rights of the suspected terrorists and produces a stronger propensity toward the demand for security rather than toward that for liberty and justice.[137]

---

130. *See* Case 5/88, Wachauf v. Bundesamt Ernahrung und Forstwirtshaft, 1989 E.C.R. 2609 (reviewing a member state's measure to ascertain whether it complies with EU human rights law).

131. *See* Case C-260/89, Elliniki Radiophonia Tileorassi AE (ERT) v. Dimotiki Etairia Pliroforissis and Siotirios Kouvelas, 1991 E.C.R. I-2925 (reviewing action by a member state derogating from EU law for compliance with EU human rights law).

132. *See generally* Robert Schütze, *European Fundamental Rights and the Member States: From "Selective" to "Total" Incorporation?*, 14 Cambridge Y.B. of Eur. Legal Stud. 337 (2012).

133. *See* Case C-617/10, Aklagare v. Åkerberg Fransson (Feb. 26, 2013) (not yet reported) (reviewing a Swedish measure concerning fines for tax evasion under EU human rights standards according to a theory that the case fell within the scope of application of EU law because the EU had adopted measures regulating taxes). On the question of the scope of application of the Charter *vis-à-vis* member states, see Koen Lenaerts, *Exploring the Limits of the EU Charter of Fundamental Rights*, 8 Eur. Const. L. Rev. 375 (2012).

134. *See generally* Jason Coppel & Aidan O'Neill, *The European Court of Justice: Taking Rights Seriously?*, 12 J. Legal Stud. 227 (1992).

135. *See* Cian Murphy, EU Counter-Terrorism Law: Pre-emption and the Rule of Law 237–38 (2012); *see also* Christina Eckes, EU Counter-Terrorist Policies and Fundamental Rights: The Case of Individual Sanctions 127–83 (2009).

136. *See generally* Federico Fabbrini, *Judicial Review of United Nations Counter-Terrorism Sanctions in the European Multilevel System of Human Rights Protection: A Case Study in Ineffectiveness*, *in* Shaping Rule of Law Through Dialogue 147, 178 (Filippo Fontanelli et al. eds., 2009).

137. Marta Cartabia, *L'ora dei diritti fondamentali nell'Unione Europea*, *in* I diritti in azione 13, 51 (Marta Cartabia ed., 2007) (translated by author from Italian: "I giudici comunitari hanno sperimentato la loro capacità di essere rigorosi nella tutela dei diritti su uno dei terreni più spinosi, dato che la gravità

Most prominently, in the *Kadi* saga, the ECJ delivered an unequivocal reaffirmation of the importance of human rights in the context of national security by voiding the blacklisting of an individual suspected of financing terrorism who had been designated as a terrorist without due process of law.[138] Overruling a decision by the EU Court of First Instance, which had declined to review the EU blacklisting regime based on the argument that it was necessitated and justified by United Nations ("UN") law,[139] the ECJ ruled in *Kadi I* that the EU, even when implementing the UN counterterrorism sanctions regime, was required to abide by EU constitutional principles of human rights protection.[140] Rejecting the view that the fight against international terrorism granted a blank check to the political branches of government, the ECJ declared the blacklisting of the plaintiff violated due process rights, the right to effective remedy, and the right to property, and it directed the European Commission to remedy these flaws. Following a new administrative decision relisting the plaintiff as a suspected terrorist,[141] the ECJ, in *Kadi II*,[142] once more declared the blacklisting regime invalid, holding that the process given to the plaintiff did not meet the EU human rights standard. As the ECJ explained, this standard requires adequate disclosure of evidence, including secret evidence, to allow the accused to defend himself and the ECJ to review the legality of the decision in full.[143] Bringing to a close a decade of litigation, the ECJ struck a fatal blow to the EU anti-terrorism financing regime and confirmed its commitment to a robust protection of human rights, even in the context of national security.[144]

The ECJ's judgment in *Digital Rights Ireland* builds on the *Kadi* line of case law, expanding the oversight of the ECJ into the area of government surveillance. Globally, since 9/11, surveillance has been, together with anti-

---

della situazione internazionale tende ad attutire la sensibilità verso I diritti dei sospetti terroristi e genera una maggiore propensione verso le esigenze della sicurezza piuttosto che verso quelle della giustizia e della libertà.") (discussing hermeneutical effects of the Charter of Fundamental Rights on the case law of the ECJ).

138. Fabbrini, *supra* note 11, ch. 2 (providing further details on the *Kadi* saga from a comparative perspective with the United States).

139. Case T-315/01, Kadi v. Council & Comm'n, 2005 E.C.R. II-03649, § 181.

140. Joined Cases C-402/05 P & C-415/05 P, Kadi & Al Barakaat, 2008 E.C.R. I-6351; *see also* Opinion of Advocate General Maduro, Joined Cases C-402/05 P & C-415/05 P, Kadi & Al Barakaat, § 37 (inviting the ECJ to exercise its role as a constitutional court and ensure respect for the rule of law).

141. Commission Regulation 1190/08, Amending for the 101st Time Council Regulation (EC) No 881/2002, 2008 O.J. (L 322) 25.

142. Joined Cases C-584/10 P, C-593/10 P & C-595/10 P, Council, Comm'n and U.K. v. Kadi (July 18, 2013) (not yet reported).

143. *See generally* Federico Fabbrini, *Global Sanctions, State Secrets and Supranational Review: Seeking Due Process in an Interconnected World*, *in* Secrecy, National Security and the Vindication of Constitutional Law 284, 291 (David Cole, Federico Fabbrini & Arianna Vedaschi eds., 2013) (discussing the problem of secret evidence).

144. *See generally* Federico Fabbrini & Joris Larik, *Global Counter-Terrorism Sanctions and European Due Process Rules: The Dialogue Between the CJEU and the ECtHR*, *in* Kadi on Trial 137 (Matej Avbelij et al. eds., 2014).

terrorism financing and detention, the area in which executives and legislatures have frequently authorized new, pervasive policies aimed at preventing future terrorist attacks.[145] Since the London bombings of 7/7, national governments and supranational institutions in the EU have been particularly proactive in this field by adopting several pieces of legislation aimed at strengthening the monitoring tools of national security and law enforcement agencies.[146] The Data Retention Directive—the adoption of which had stalled for some time in the Council, and which was rushed through the political process precisely following 7/7—constituted the most comprehensive achievement of the EU in the field of surveillance. As explained in Part I, it harmonized national rules on the retention of metadata, obliging every member state to impose on IT and telephone service providers a far-reaching obligation to retain (from a minimum of six months, to a maximum of twenty-four), and make available on request, data concerning the date, time, length, origin, and destination of emails, phone calls, and text messages, albeit not their content.[147]

As the ECJ made crystal clear, the existence of a regime in which every digital interaction, of every citizen, is stored for future intelligence and law enforcement purposes is liable to chill human relations and profoundly affect the sphere of private and family life of every individual. With language that echoes U.S. Supreme Court Justice Sotomayor's concurring opinion in *United States v. Jones*,[148] the ECJ ruled that:

> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[149]

145. *See generally* Scott Matheson, Presidential Constitutionalism in Perilous Times 85–90 (2009) (indicating interrogation, surveillance, and detention as three main areas of new counterterrorism policies devised by the Bush Administration); Surveillance, Counter-Terrorism and Comparative Constitutionalism 95 (Fergal Davis et al. eds., 2014) (discussing program of surveillance in a global perspective).

146. *See* Maria Tzanou, *The EU as an Emerging 'Surveillance Society': The Function Creep Case Study and Challenges to Privacy and Data Protection*, 4 J. Int'l Const. L. 407, 410 (2010).

147. *See supra* text accompanying notes 47–58.

148. United States v. Jones, 132 S.Ct. 945, 956 (2012) (Sotomayor, J., concurring) (stating that surveillance, "by making available at a relative low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, choses to track—may alter the relationship between citizen and government in a way that is inimical to democratic society." (internal citations omitted)).

149. Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238, § 27.

From this point of view, therefore, the ECJ showed awareness of the pervasive effect of a metadata collection program,[150] and rejected the view that individuals lose their claim to privacy protection whenever they exchange information with telecommunication providers.[151] Rather, drawing from the view repeatedly advanced by the German *Bundesverfassungsgericht*,[152] the ECJ defended a view of privacy as protecting citizens against full-scale governmental surveillance in the public sphere as well.[153] As a result, *Digital Rights Ireland* advanced a broad view of the right to privacy and data protection, updating its scope and strengthening its safeguards to face the challenges of the digital age.

Moreover, although the ECJ did not deny the importance of fighting crime and protecting national security,[154] it advanced a strict proportionality framework, requiring that any interference with the broad understanding of privacy and data protection be strictly necessary to the attainment of the desired goal.[155] This requirement does not only place a high burden on the EU executive and legislative branches in devising a new data surveillance regime that could pass muster before the ECJ. De facto, it also rules out anything short of individualized, court-approved requests by national security and law enforcement authorities to collect and use metadata generated in electronic communications for specific searches.[156] Certainly, that the Data Retention Directive "entail[ed] an interference with the fundamental rights of practically the entire European population"[157] played a role in influencing the ECJ's conclusion. However, the detailed criticisms that the ECJ raised against the Data Retention Directive in the second tier of its

150. *See* Alan Rusbridger, *The Snowden Leaks and the Public*, THE N.Y. REV. OF BOOKS, Nov. 21, 2013, http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/, *archived at* http://perma.cc/PEQ7-4GZX (suggesting that metadata collection programs are pervasive by quoting former NSA General Counsel Stewart Baker, who stated that "[m]etadata absolutely tells you everything about somebody's life . . . . If you have enough metadata, you don't really need content. . . . [It is] sort of embarrassing how predictable we are as human beings.").

151. *See* Bert-Jaap Koops & Ronald Leenes, *'Code' and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 1 (2005).

152. *See supra* text accompanying notes 62–66.

153. *See* Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, § 56. The decision of the ECJ may soon be followed by a similar ruling by the ECtHR in Big Brother Watch and Others v. United Kingdom, App. No. 58170/13, currently pending (on the compatibility of mass surveillance of electronic communications by the British intelligence agency with Article 8 of the ECHR).

154. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, § 42 (Ironically, the ECJ only cites the *Kadi* decision to support the argument that EU institutions and member states have a duty to guarantee national security.).

155. *Id.* § 51. *See generally* Paul De Hert & S. Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action*, *in* REINVENTING DATA PROTECTION, *supra* note 23, at 3 (discussing the use of proportionality in the case law relating to privacy in the EU and ECtHR).

156. *But see* Fiona de Londras, *CJEU Strikes Down Data Retention Directive*, HUM. RTS. IN IR. BLOG (Apr. 8, 2014), http://humanrights.ie/civil-liberties/cjeu-strikes-down-data-retention-directive/, *archived at* http://perma.cc/N6YC-29YH (suggesting a reading of the decision of the ECJ in *Digital Rights Ireland* which leaves open other initiatives by the political branches in the retention of data).

157. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, § 56.

proportionality analysis[158]—too broad in scope, too permissive in access, and too long in time—foreclose many doors to EU policy-makers, and significantly constrain the ability of the EU institutions to reenact a comprehensive data retention regime. It is therefore uncertain whether the EU could pass a new Data Retention Directive, and, even if it could, its usefulness would be questionable.[159]

On April 11, 2014, the European Commission held a meeting to discuss the options available going forward.[160] The ruling of the ECJ comes at a time in which the EU institutions are deeply involved in a debate about overhauling the EU data protection regime. In 2012, the European Commission presented a package of legislative proposals aimed at updating the Data Protection Directive to account for new technology and establishing a new, comprehensive system for all data-processing activities.[161] The package included a General Data Protection Regulation, which would replace the Data Protection Directive and establish a uniform law throughout the EU,[162] and a Directive that would lay down a harmonized framework for all data processing activities by law enforcement authorities for law enforcement purposes, thereby reducing the differences between member states.[163] These new bills would introduce a modern, robust protection of data privacy in the EU, and would include, among other safeguards, the recognition of the data subject's right to be forgotten.[164] The Commission's proposals have proceeded slowly so far. Despite strong support in the European Parliament,[165] opposition to the bills has emerged in the Council,[166] which represents member states' governments and must vote by qualified

158. *See supra* text accompanying notes 105–113.

159. *See* Press Release, European Data Protection Supervisor, Peter Hustinx, The CJEU Rules that Data Retention Directive is Invalid (Apr. 8, 2014) (welcoming the decision of the ECJ and calling for further reflection on whether a new Directive should be adopted), *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/14-04-08_Press_statement_DRD_EN.pdf, *archived at* http://perma.cc/SKG6-HX3J.

160. *See* Cecilia Malström, European Commissioner, Home Affairs, Data Retention Directive: Commissioner Malmström's Statement on Today's Court Judgment (Apr. 8, 2014), *available at* http://europa.eu/rapid/press-release_STATEMENT-14-113_en.htm, *archived at* http://perma.cc/XZC4-LX2M ("The judgment of the Court brings clarity and confirms the critical conclusions in terms of proportionality of the Commission's evaluation report of 2011 on the implementation of the data retention directive. The European Commission will now carefully asses the verdict and its impacts.").

161. *See* Viviane Reding, *Tomorrow's Privacy: The Upcoming Data Protection Reform for the European Union*, 1 Int'l Data Privacy L. 3 (2011).

162. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25 2012).

163. Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data, COM (2012) 10 final (Jan. 25, 2012).

164. *See* Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88 (2012).

165. Eur. Parliament, Comm. on Civil Liberties, Justice and Home Affairs, Rep. on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), A7-0402/2013 (Nov. 22, 2013).

majority in favor of the proposals.[167] The ECJ's decision, however, may be a game-changer, weakening the arguments of those who have opposed reform so far and tipping the balance in favor of a new legislative framework strengthening the protections of privacy and personal data even further.[168]

In the short term, the ECJ's decision returns power to the EU member states. As explained above, before the enactment of the Data Retention Directive, member states could enact data retention measures as exceptions to the Data Protection Directive.[169] In fact, as emphasized in the first comments on *Digital Rights Ireland*, the ECJ decision does not automatically remove national implementing acts from the legal order,[170] except in Ireland and Austria, where the Irish High Court and the Austrian *Verfassungsgerichthof* have to apply the ECJ ruling that set aside their national laws implementing the Directive.[171] However, because national data retention laws are technically exceptions to the Data Protection Directive, they are subject to review for compatibility with EU human rights law.[172] Because *Digital Rights Ireland* leaves no doubt that the data retention regime is incompatible with the EU Charter of Fundamental Rights, it seems inevitable that the data retention measures adopted by the member states will also not withstand scrutiny. Every court, in any of the other EU member states, can set aside the national implementing acts of the Data Retention Directive—with no need for additional preliminary reference to the ECJ.[173] The effects of the ECJ judgment, therefore, are likely to spill over into national legal systems, ensuring a new, advanced standard of protection for privacy and personal data throughout the EU. Yet, the implications of the ruling may extend even beyond the borders of the EU.

---

166. Press Release, Council of the Eur. Union, Doc. 14149/13 (Oct. 7–8, 2013) (explaining that the Council has been unable to arrive at a general approach on the new data protection legislative package).

167. *See* Consolidated Version of the Treaty on European Union art. 16, Dec. 13, 2007, 2012 O.J. (C 326) 01 (stating that the Council, which represents the member states, must generally approve EU legislation by qualified majority and explaining how to calculate this qualified majority).

168. However, the occurrence of a terrorist attack may change the balance, strengthening arguments in favor of more security and surveillance. *But see* Federico Fabbrini, *The Role of the Judiciary in Times of Emergency: Judicial Review of Counter-Terrorism Measures in the United States Supreme Court and the European Court of Justice*, 28 Y.B. OF EUR. L. 664 (2009) (suggesting that the time factor is the main determinant in explaining responses to terrorism—meaning that in the aftermath of a terrorist attack, political branches react, and courts are more willing to defer, whereas in the long term, judges raise the bar in reviewing national security measures).

169. *See supra* text accompanying notes 46–47.

170. *See* Innocenzo Genna, *Messy Consequences for National Legislations Following Annulment of EU Data Retention Directive*, LONDON SCH. OF ECON. & POL. SCI. MEDIA POL'Y PROJECT (Apr. 8, 2014), *available at* http://blogs.lse.ac.uk/mediapolicyproject/2014/04/08/messy-consequences-for-national-legislations-following-annulment-of-eu-data-retention-directive/, *archived at* http://perma.cc/C6XL-C589.

171. *See* VfGH [Constitutional Court], Jun. 27, 2014 G47/2012 (applying the ruling of the ECJ to strike down the Austrian act implementing the Data Retention Directive).

172. *See supra* text accompanying note 129.

173. *See* Case 283/81, CILFIT & di Gavardo SpA v. Ministry of Health, 1982 E.C.R. 3415 (holding that state courts do not need to send a reference to the ECJ when the legality or illegality of a measure is clear).

IV. The United States and the Reform of the Government Surveillance System: Lessons from the EU

The ECJ's judgment comes at a key moment in the U.S. conversation about privacy and government surveillance.[174] Following the Snowden revelations about U.S. government surveillance, a major debate has started among the U.S. public, and between the U.S. institutions, regarding the balance between liberty and security in the digital era.[175] In particular, disclosure of a vast secret program of dragnet collection of metadata about phone calls, text messages, and emails of U.S. citizens and foreign persons by the NSA, pursuant to authority allegedly granted by the USA PATRIOT Act, has led to calls for an overhaul of the U.S. surveillance regime in every branch of the U.S. government. Some lower federal courts have ruled that the government metadata collection program likely violates the U.S. Constitution's Fourth Amendment prohibition on unreasonable searches and seizures.[176] Members of Congress in both houses have advanced bills curbing the authority of the NSA and proposing new privacy protections for electronic communications.[177] Moreover, President Obama delivered a speech in January 2014, in which, while re-affirming the importance of data mining and intelligence gathering for national security purposes, he acknowledged the need to reform the surveillance system to allay the anxiety of people wary of government overreach.[178]

Coming at the height of this conversation, the ECJ's decision in *Digital Rights Ireland* may yield some valuable lessons for the ongoing debate in the United States.[179] As David Cole and I have argued elsewhere, the legal regimes of privacy and national security in the EU and the United States have, despite several differences, important points of similarity, which render meaningful for each of them to learn from each other.[180] The ECJ's judgment dealt with a question of EU law and does not have any legal effect in the United States. However, the factual issues in the case, and the legal principles invoked by the ECJ, present striking analogies with the situation in the United States.

---

174. *See, e.g.*, David Cole, *The Three Leakers and What to Do About Them*, The N.Y. Rev. of Books, Feb. 6–19, 2014, at 7, http://www.nybooks.com/articles/archives/2014/feb/06/three-leakers-and-what-do-about-them/, *archived at* http://perma.cc/XBQ8-8UD6; Ryan Lizza, *State of Deception*, The New Yorker, Dec. 16, 2013 (discussing debates triggered by recent revelations of NSA surveillance activities).

175. *See, e.g.*, Cole, *supra* note 174; Lizza *supra* note 174.

176. *See* Klayman v. Obama, 957 F.Supp.2d 1 (D.D.C. 2013).

177. *See* USA Freedom Act, H.R. 3361, 113th Cong. (2013), S. 1599, 113th Cong. (2013).

178. *See* Obama, *supra* note 6.

179. *See* Gregory Schaffer, *Globalization and Social Protection: The Impact of the EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standards*, 25 Yale J. Int'l L. (2000) (discussing the previous influence of EU law on the conception of privacy and related protections in the United States).

180. *See* Federico Fabbrini and David Cole, *Bridging the Transatlantic Divide? The European Union, the United States and the Protection of Privacy Across Borders*, *in* Constitutionalism Across Borders in the Struggle Against Terrorism (Federico Fabbrini & Vicki Jackson eds., forthcoming 2015).

To begin with, the Data Retention Directive had established in the EU a regime akin to the surveillance program that the NSA produced in the United States—one in which the metadata (but not the data) of every citizen's phone calls, text messages, or emails were retained and stored for future law enforcement and counterterrorism purposes.[181] The two programs were inspired by similar desires to empower national security agencies with effective tools to counter terrorist threats by identifying digital patterns of interactions and links between individuals.[182] Therefore, the analogies of the facts at play in *Digital Rights Ireland* render the EU experience of practical value in the U.S. debate.

Moreover, the ECJ reviewed the Data Retention Directive in light of the principles of privacy and data protection, which are equally cherished in the United States.[183] Today, the EU Charter of Fundamental Rights and the TFEU include much more explicit recognitions of the rights to privacy and data protection[184] than the Fourth Amendment to the Constitution of the United States, which safeguards "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[185] However, despite these textual differences—which are a result of the fact that the U.S. Bill of Rights dates to the end of the eighteenth century, whereas the EU Bill of Rights dates to the dawn of the twenty-first century—the same values of privacy as a protection *against government interference* underpin constitutional jurisprudence in both the EU and the United States.[186] In fact, the U.S. Supreme Court anticipated its European counterparts by holding, as early as 1967, that the Fourth Amendment protects a reasonable expectation of privacy.[187] Additionally, the example of the U.S. Constitution has often been taken as a model for constitution-making in Europe.[188] From this point of view, therefore, the constitutional standards that the ECJ invoked in *Digital Rights Ireland* also provide a valuable reason

181. *See supra* text accompanying notes 47–58.

182. *See* Press Release, Council of the European Union, Doc. 11116/05 (July 13, 2005), *available at* http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/85703.pdf, *archived at* http://perma.cc/ZM88-AW4S (condemning the terrorist attacks of 7/7 and communicating its intention to move ahead with the approval of the Data Retention Directive as a way to counter terrorism threats); *see also* Executive Order No. 12333, 3 C.F.R. 200 (1981), *as amended last by* Executive Order No. 13470 3 C.F.R. 13470 (2008), *available at* https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf, *archived at* http://perma.cc/TQ2T-GA5D (authorizing surveillance for national security purposes).

183. *See generally* Fabbrini & Cole, *supra* note 180.

184. *See supra* text accompanying notes 20–25.

185. U.S. Const. amend. IV.

186. *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1966, 1988–89 (2013) (rejecting the idea of a dichotomy between EU and U.S. privacy law). *But see* James Whitman, *The Two Western Culture of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151 (2004) (emphasizing that, historically, the foundation of privacy in the United States has been liberty whereas in the EU, the foundation has been dignity).

187. Katz v. United States, 389 U.S. 347, 360 (1967).

188. *See generally* Heinz Klug, *Model and Anti-Model: The United States Constitution and the Rise of "World Constitutionalism,"* Wis. L. Rev. 597 (2000).

for U.S. policymakers to take into account the recent legal developments in the EU.

What lessons may the ECJ's judgment give the United States, at a time when it is profoundly reconsidering its system of electronic surveillance? I suggest that there are at least two key guideposts that the United States may take from the EU—or may ignore at its own peril. First, the ECJ's decision provides a model for the U.S. Supreme Court to follow that favors adjusting mechanisms of privacy and data protection to the challenges of the digital age. As explained in Part III, the ECJ held that the feeling of surveillance generated by vast metadata collection is inimical to privacy and democracy, and it suggested that individuals ought to be protected when they interact with others through the means of new technological devices.[189] Moreover, the ECJ required that interferences with privacy rights be subject to a higher level of scrutiny with respect to their necessity and proportionality, even when they are carried out for national security purposes.[190] Interestingly, the U.S. Supreme Court has recently signaled interest in similar ideas. In *United States v. Jones*, the Court unanimously found that GPS surveillance of a vehicle exceeding the scope of a warrant both geographically and temporally constituted a "search" pursuant to the Fourth Amendment,[191] and several justices separately questioned the requirement of secrecy as a pre-condition for privacy.[192] In *Kyllo v. United States*,[193] Justice Scalia, writing for the Court majority, recognized the need to adapt Fourth Amendment doctrine to preserve traditional expectations of privacy from advances in technology.[194] And more recently in *Riley v. California*,[195] the Supreme Court unanimously ruled that law officers must obtain a warrant to search cellular phone data.[196]

However, several still-valid U.S. constitutional doctrines limit the protection of privacy in the digital world. For instance, the U.S. Supreme Court has never overruled the conventional view that once individuals share their data with electronic service providers, they waive their privacy claim.[197] Further, that view is still widespread in U.S. legal practice—consider, for example, the recent decision of a federal district court to uphold

189. *See supra* text accompanying notes 148–153.

190. *See supra* text accompanying notes 154–155.

191. *See* 132 S.Ct. 945, 949 (2012).

192. *See id.* at 957 (Sotomayor, J., concurring) (stating that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"); *id.* at 962 (Alito, J., concurring) (suggesting that surveillance must be reviewed in light of the "expectation-of-privacy test").

193. 533 U.S. 27 (2001).

194. *See id.* at 33–34; *see generally* David Cole, *Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism*, *in* Surveillance, Counter-Terrorism and Comparative Constitutionalism, *supra* note 145, at 95.

195. 134 S.Ct. 2473 (2014).

196. *Id.* at 2494.

197. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (holding that a pen register that recorded the numbers dialed from an individual's home did not invade a legitimate expectation of privacy).

the NSA's bulk telephone metadata collection program precisely on these terms.[198] And, in *Jones*, Justice Alito suggested in his concurring opinion that developments in digital technology may lower the expectations of privacy and, in any case, that counterterrorism investigations may justify the sacrifice of privacy for the needs of security.[199]

Although the state of the law in the United States seems to be in flux, *Digital Rights Ireland* makes a strong case for also updating the protection of privacy in the United States in light of technological developments that dramatically increased the capacity of governments to surveil their citizens.[200] With arguments that are familiar to U.S. constitutional lawyers, the ECJ has emphasized the need for courts to act as a bulwark of human rights against the challenges posed by government surveillance.[201] The first lesson for the United States therefore seems to be that in the digital age, legal safeguards for privacy and personal data protection must be strengthened—not weakened—and that legal doctrines must evolve—rather than stagnate—in the face of new challenges.

Second, the ECJ's decision can provide food for thought to the U.S. political branches regarding the question of whether public authorities or private companies should be in charge of retaining personal data—in fact, whether either of them should have that control. As explained above, in the EU, the Data Retention Directive relied on private electronic communication providers for the retention of metadata.[202] Intelligence and law enforcement agencies of the member states did not directly control the data, but they could request access to it through private electronic communication providers, pursuant to criteria loosely defined in the Directive and subject to further state regulation.[203] In the United States, on the contrary, the government has been directly collecting and storing metadata through its once-secret electronic surveillance program, and much of the reform debate has focused on whether retention should actually be shifted away from the NSA toward private companies.[204] Following specific advice from the special review group he created,[205] U.S. President Obama indicated his will-

198. ACLU v. Clapper, 959 F.Supp.2d 724 (S.D.N.Y. Dec. 27, 2013).

199. *See* 132 S.Ct. 945, 962 (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy and many people may find the tradeoff worthwhile."); *id.* at 964 (recognizing the legitimacy of greater intrusion into privacy "in the context of investigations involving extraordinary offenses").

200. *See generally* Federico Fabbrini and Mathias Vermeulen, *GPS Surveillance and Human Rights Review: The European Court of Human Rights and the US Supreme Court in Comparative Perspective*, *in* Surveillance, Counter-Terrorism and Comparative Constitutionalism, *supra* note 145, at 134.

201. *See* James Balkin, *The Constitution in the Surveillance State*, 93 Minn. L. Rev. 1 (2009).

202. *See supra* text accompanying note 9.

203. *See supra* text accompanying notes 57–58.

204. *See* Fiona de Londras, *Privatized Counter-Terrorism Surveillance: Constitutionalism Undermined*, *in* Surveillance, Counter-Terrorism and Comparative Constitutionalism, *supra* note 145, at 73 (discussing the privatization of the struggles against terrorism).

205. *See* Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies, *supra* note 2, recommendation no. 5, at 27 ("[L]egislation

ingness to demand that internet and telephone companies undertake the task.[206] Legislation under consideration in Congress has also pointed in this direction as a solution to the problems raised by NSA surveillance.[207]

The lesson that the ECJ judgment in *Digital Rights Ireland* carries for the United States, however, is that the distinction between private and public retention does not matter. As the ECJ ruled with regard to a system in which private companies collect the metadata, it is the retention *in itself* that constitutes an infringement on the right to privacy.[208] In other words, the ECJ's decision poses a pressing question: namely, whether collection, retention, and storage of metadata that tells so much about an individual's personal life should be within the remit of the government's policy tools in the fight against terrorism at all.[209] As David Cole wrote: "the bigger issue is not who holds the data, but the very fact that the government is engaged in the dragnet collection of data on all of us, rather than conducting the more traditional targeted searches that the Constitution has long required."[210] As a report by the Privacy and Civil Liberties Oversight Board created by the U.S. Congress emphasized, the metadata retention program has not in a single instance made a concrete difference in the outcome of a counterterrorism investigation.[211] The ECJ's judgment in *Digital Rights Ireland* may therefore support those who question the usefulness of maintaining such a pervasive surveillance regime—regardless of whether the government or private companies retain the data.

In conclusion, the ECJ's ruling on the EU Data Retention Directive may carry valuable lessons for the United States. Despite differences, the cleavage between the United States and the EU on privacy and national security is less significant than what it is often thought.[212] The EU and the United States are two constitutional systems founded on equal respect for democracy, rule of law, and human rights, including privacy. Both have been at

---

should be enacted that terminates the storage of bulk telephony meta-data by the government . . . and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party.").

206. *See* Charlie Savage, *Obama Says N.S.A. Curbs Would Address Worries*, N.Y. Times, Mar. 25 2014, http://www.nytimes.com/2014/03/26/us/politics/obama-says-nsa-curbs-would-address-worries.html?_r=0, *archived at* http://perma.cc/F4TD-F98E (reporting remarks by President Obama in favor of requesting that private telephone companies retain the data).

207. *See id*.

208. Joined Cases C-293/12 & C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'n, 2014 E.C.R. I-238 ¶ 34.

209. *See generally* Balkin, *supra* note 187.

210. David Cole, *Can Privacy Be Saved*, The N.Y. Rev. of Books, Mar. 6–19, 2014.

211. *See* Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program 11 (2014), *available at* http://www.washingtonpost.com/world/national-security/independent-review-board-says-nsa-phone-data-program-is-illegal-and-should-end/2014/01/22/4cebd470-83dd-11e3-bbe5-6a2a3141e3a9_story.html, *archived at* http://perma.cc/M359-YETW (stating that, with regard to the U.S. metadata collection program, "we have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation").

212. *See* Cole & Fabbrini, *supra* note 180.

the forefront of the fight against terrorism and have devised analogous regimes to protect national security. In fact, EU and U.S. intelligence agencies are increasingly working together in disrupting possible threats.[213] However, the outrage following recent revelations about secret programs of dragnet surveillance of electronic communications has called for a new balance between liberty and security, both in the EU and the United States.[214] The ECJ ruling in *Digital Rights Ireland* can be of added value as the United States reconsiders its surveillance regime. In its decision, the ECJ indicated that privacy protection must be strengthened in the digital age, and suggested that private or public retention of metadata is not the problem, because it is the retention itself that threatens privacy rights. Given that a high standard of privacy and data protection in the United States is a precondition for a fruitful cooperation between the EU and the United States,[215] the ECJ may have offered a possible model for U.S. institutions to consider in their efforts to boost privacy protection and foster transatlantic cooperation.[216]

Conclusion

On April 8, 2014, the ECJ delivered a milestone ruling on human rights in the digital age. By striking down the EU Data Retention Directive as a disproportionate interference with the rights to privacy and data protection, *Digital Rights Ireland* strengthened the protection of personal data in the face of the challenges posed by rapid technological developments and reaffirmed the importance of human rights, despite pressures from the political branches to exploit opportunities opened by electronic communications for national security purposes. Whereas the Data Retention Directive had long caused concerns in the EU—as demonstrated by several national courts' decisions striking down the acts implementing the Directive at the state level—the ECJ's ruling removed the obligation of private companies to collect, store and make available to law enforcement agencies metadata related to internet and telephone communications. The effect of the ECJ's decision on the regime for the protection of privacy in the EU and its mem-

213. *See* Valsamis Mitsilegas, *The Transformation of Privacy in an Era of Pre-emptive Surveillance*, 20 Tilburg L. Rev. 35 (2015).

214. *See generally* Report on the US NSA Surveillance Programme, *supra* note 1; Report and Recommendations of the President's Review Group on Intelligence and Communication Technologies, *supra* note 2.

215. *See also* European Parliament President Martin Schulz, Statement Ahead of the Council Adopting the Negotiating Mandate on Transatlantic Trade and Investment Partnership with the United States (June 13, 2013), *available at* http://www.europarl.europa.eu/former_ep_presidents/president-schulz/en/press/press_release_speeches/press_release/2013/2013-june/html/schulz-on-negotiating-mandate-on-transatlantic-trade-and-investment-partnership, *archived at* http://perma.cc/UE4G-TJWG (indicating the importance of convergence in privacy protections in the EU and the United States as a condition for the success of the Transatlantic Trade and Investment Partnership).

216. *See generally* Cole & Fabbrini, *supra* note 180.

ber states is momentous, and may tip the balance in favor of new EU legislation, currently pending parliamentary approval, to update the EU data protection regime to meet the challenges of the new century. Yet—as this Article has suggested—the decision may exert influence outside the EU as well. In the United States in particular, as the debate triggered by the NSA revelations increasingly calls for an overhaul of the surveillance regime, *Digital Rights Ireland* offers lessons the U.S. Supreme Court, Congress, and the President may wish to consider. In the new world that globalization has made possible, the EU and the United States must remain at the forefront of the protection of privacy on a global scale.