Cornell International Law Journal Online

Data Duel:
Divergent EU and US Personal Information Collection Decisions

by Yujin Chun*

The European Court of Justice (ECJ), Europe's most senior court, ruled on April 8 that the 2006 EU Data Retention Directive (the Directive),[1] which required telecom companies to store user data for up to two years and to make that data available to law enforcement authorities upon request, was illegal.[2] The ECJ stated that the Directive seriously interfered with Europeans' fundamental right to a private life and the right to protect their personal data.[3] To bolster this finding, the ECJ claimed that the Directive's rules disproportionately diverged from its ends and that it lacked adequate safeguards for privacy.[4]

The decision comes as European leaders face demands for tougher data protection measures following revelations that U.S. spies eavesdropped on the conversations of EU leaders,[5] and only a day after the Supreme Court of the United States declined to take an early look at a constitutional challenge to the National

* Yujin Chun is a J.D. candidate at Cornell Law School, where she is the *Cornell International Law Journal*'s Associate on European Affairs and the Career Chair of the Briggs Society of International Law. She holds a B.A. in English from Duke University.

[1] Directive 2006/24, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC , 2006 O.J. (L 105) 54 (EC), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1396974047372&uri=CELEX:32006L0024

[2] Case C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine and Natural Res., 2014 E.C.R. --, *available at* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051; *see also* Press Release No 54/14, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others (Apr. 8, 2014) *available at* http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

[3] *Digital Rights Ireland*, 2014 E.C.R. --, at ¶ 56, 65.

[4] *Digital Rights Ireland*, 2014 E.C.R. --. At ¶ 62, 66.

[5] Aoife White, *EU Data-Retention Law Tramples on Privacy, Top Court Says,* BLOOMBERG (Apr. 8, 2014), http://www.bloomberg.com/news/2014-04-08/eu-data-retention-law-tramples-on-privacy-top-court-says.html.

Security Agency's (NSA) bulk collection of Americans' phone records.[6] This article examines, in turn, the recent legal decisions on data retention in the United States and Europe. It then considers what, if any, impact the ECJ decision may have in the United States, whose highest court has not yet addressed the divergent opinions on the issue.

On June 5, 2013, *The Guardian* reported on Edward Snowden's release of secret documents that exposed multiple U.S. government intelligence and surveillance programs' efforts to collect large swathes of data on American citizens.[7] In particular, the report disclosed an order from the Foreign Intelligence Surveillance Court (FISC), commanding the wireless telecommunications giant Verizon Business Network Services to produce, on a daily basis, all call detail records of its customers.[8]

In light of Snowden's disclosures, a group of subscribers of telecommunication and internet services implicated in the surveillance scheme challenged the constitutionality and statutory authorization of these practices.[9] Judge Richard J. Leon of the U.S. District Court for the District of Columbia held that the surveillance program probably violated the Fourth Amendment.[10] However, Leon tempered this condemnation—staying an injunction on data collection pending appeal—because of the weighty national security interests and the novelty of the constitutional issues.[11] In a bold response, the plaintiffs petitioned the Supreme Court of the United States, insisting that the case be heard there ahead of any activity on the appellate level.[12] Historically, such petitions are seldom granted. The trend held here: the justices rejected the request without comment.[13]

While Klayman, the case's named plaintiff, fears that the Justice Department is trying to stretch out the appeals process in his case,[14] there is actually a high demand for the ultimate decision on this issue. Just days after Klayman won his district court case, U.S. District Judge William H. Pauley III of New York reached the opposite conclusion in an American Civil Liberties Union case challenging the spying program, instead upholding the NSA operation as an effective "counter-punch" to terrorist acts.[15] There is some discord emanating from the presidency as well; President Barack Obama has also proposed that the NSA end its systematic collection of data and allow the phone

---

[6] Sam Hananel, *Supreme Court Declines to hear NSA Metadata Case*, HUFFINGTON POST (Apr. 7, 2014), http://www.huffingtonpost.com/2014/04/07/supreme-court-nsa_n_5104600.html.

[7] *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[8] Secondary Order at 2, In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services, No. BR 13–80 (FISC Apr. 25, 2013).

[9] Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

[10] *Id.* at 37-38.

[11] *Id.* at 43-44.

[12] Sam Hananel, *Supreme Court Declines to hear NSA Metadata Case*, *supra* note 6.

[13] *Id.*

[14] *Id.*

[15] Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013).

companies to retain their records. The government would only be able to access the phone records after obtaining approval from the Foreign Intelligence Surveillance Court.[16]

The ECJ faced a similar challenge to surveillance, and ruled that such data collection constitutes a serious interference with the rights to data protection and privacy guaranteed by the EU Charter of Fundamental Rights.[17] In its decision, the court noted that even the threat of terrorism did not justify so sweeping an interference.[18] The Directive's wide-ranging and particularly serious interference with the fundamental right to data privacy, the court held, was not "precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[19] The court first pointed to how the Directive indiscriminately covers all individuals, all means of electronic communication, and all data, without any real consideration of the overall objective of combating serious crime.[20] Second, the court noted that the Directive fails to lay down any objective criterion to ensure that the authorities use the data collected solely for the purposes of crime prevention, detection, and prosecution.[21] Based on the lack of safeguards and the Directive's disproportionate interference with fundamental rights, the court struck down the Directive.[22] This decision freed member states from their obligation to implement the Directive's rules at national level and created political breathing room for the European nations to relax their own surveillance policies.[23]

While it is certainly possible that the Supreme Court of the United States may follow the ECJ's example, the impact of the ECJ decision in the United States already extends beyond individual rights into the realm of business. The "European Safe Harbor," a joint U.S.-EU framework, governs trans-Atlantic data commerce and the integration of the two communities' different privacy laws.[24] As a prerequisite to transferring data from EU states to the U.S., the transferring U.S. telecommunication company must certify that they follow the requisite privacy policies and programs in

---

[16] *See* Charlie Savage, *Obama to call for End to N.S.A.'s Bulk Data Collection*, N.Y. TIMES (Mar. 24, 2014), http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?partner=rss&emc=rss&smid=tw-nytimes&_r=0.

[17] *See* Press Release No 54/14, *supra* note 2.

[18] Case C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine and Natural Res., 2014 E.C.R. --, at ¶ 51, *available at* http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051 .

[19] *Digital Rights Ireland*, 2014 E.C.R. --, at ¶ 65.

[20] *Digital Rights Ireland*, 2014 E.C.R. --, at ¶ 58.

[21] *Digital Rights Ireland*, 2014 E.C.R. --, at ¶ 60.

[22] *Digital Rights Ireland*, 2014 E.C.R. --, at ¶ 65-69.

[23] Stephen Gardner, *ECJ Invalidates EU Data Retention Directive; Member State Laws Now Open to Challenge*, BLOOMBERG BNA (Apr. 14, 2014), http://www.bna.com/ecj-invalidates-eu-n17179889560/.

[24] Doug Bernard, *EU Data Retention Ruling May Roil US-European Relations,* VOICE OF AMERICA (Apr. 8, 2014), http://www.voanews.com/content/eu-data-retention-ruling-may-roil-us-european-relations/1888781.html.

line with the EU's more robust protections, creating a "safe harbor" for data privacy.[25] However, with the right to privacy established as a far stronger right in the EU, European countries have suspiciously viewed many of the U.S. privacy protections as empty words, full of sound and fury, signifying nothing—a suspicion that seems to have been confirmed with the Snowden leaks.[26] "Having one more element of differentiation between the U.S. and EU is just not helpful," says Bennet Kelley, founder of the Internet Law Center.[27] These vast gulfs between the two regions' privacy laws can thus make it difficult for companies to do business in both the U.S. and the EU.[28]

By striking down data retention in its highest court, U.S. law will parallel the ECJ's decision and, at the same time, facilitate more efficient commerce between the United States and Europe. As both continue to increase their dependency on electronic data and as international trade continues to proliferate, it is imperative that each court set a clear guideline on control and surveillance of electronic data; failure to do so will have a potentially long-lasting international impact. Europe has already taken a definitive step with the ECJ decision. It is time for the Supreme Court of the United States to follow.

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*