2015

Transatlantic Privacy Regulation: Conflict and Cooperation

Francesca Bignami
George Washington University Law School, fbignami@law.gwu.edu

Giorgio Resta
Università degli Studi di Roma Tre, Law Department

TRANSATLANTIC PRIVACY REGULATION: CONFLICT AND COOPERATION

FRANCESCA BIGNAMI*

GIORGIO RESTA**

I
INTRODUCTION

Regulatory differences in the data privacy arena have been a recurring source of contention in transatlantic trade relations. In the 1990s, the focus was primarily on differences in the rules governing market actors. Over the past decade, however, the focus has expanded to include the public sector and the policies regulating the collection and use of personal data by government actors, particularly national security agencies. This article surveys the considerable history of transatlantic relations in the privacy area and the attempts that have been made to reconcile legal and policy differences in the interest of trade liberalization and police and national security cooperation. It then turns to the current dispute over National Security Agency (NSA) surveillance and discusses the factual and legal underpinnings of the dispute. The article demonstrates how this latest episode in transatlantic privacy both underscores longstanding legal differences and reveals fresh ones. The article concludes with observations regarding the impact of the NSA dispute on transatlantic privacy relations and on trade relations more broadly speaking.

II
HISTORY OF DATA PRIVACY IN TRANSATLANTIC RELATIONS

A. Regulatory Differences and Similarities

In narrating the history of data privacy, the point of departure is generally taken to be the Code of Fair Information Practices set forth in an expert report commissioned by the United States Department of Health, Education, and Welfare and published in 1973.[1] To understand the current transatlantic dispute, however, it bears taking one step back, to begin with the judgment of the German

This article is also available at http://lcp.law.duke.edu/.

* Professor, George Washington University Law School. We thank Ira Rubinstein and the other participants in the symposium on New Approaches to International Regulatory Cooperation for their helpful comments.

** Professor, University of Roma Tre Law Department. This article is a collaborative project that reflects the equal contribution of each of the authors. Part II was originally written by Francesca Bignami and Part III by Giorgio Resta.

1. U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS., RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

Constitutional Court in the *Microcensus* case. In 1969, the Court found that the personal information collected in large data banks was constitutionally protected under Articles 1 and 2 of the Basic Law (human dignity and the free development of personality).[2] That litigation involved a challenge to the federal census, which the Court ultimately upheld, but only on condition that the information remain anonymous.[3] This early case was followed, over ten years later, by the celebrated *Census Act* case in which the Court recognized a broad "right of informational self-determination ("informationelles Selbstbestimmungsrecht").[4] With the right of informational self-determination, the Court significantly extended its earlier jurisprudence. The Court recognized that the right of informational self-determination covered all personal information, and it abandoned the distinction that had been made in the *Microcensus* case between private information and information in the public domain. The Court also stated that the right came into being at the time of collection—at the moment that the individual was asked to give up the information—and not simply once it was used or misused by state actors and other types of data processors.

The extraordinary possibilities of modern information technologies underpinned this conceptualization of the right of informational self-determination. In language reminiscent of a recent report by the United States Privacy and Civil Liberties Oversight Board,[5] the German Court wrote in 1983 that

> [t]he [individual's decisional] authority needs special protection in view of the present and prospective conditions of automatic data processing. It is particularly endangered because . . . the technical means of storing highly personalized information about particular persons today are practically unlimited, and [information] can be retrieved in a matter of seconds with the aid of automatic data processing, irrespective of distance. Furthermore, such information can be joined to other data collections—particularly when constructing integrated information systems—to produce a partial or virtually complete personality profile, with the person concerned having insufficient means of controlling either its veracity or its use.[6]

In the *Census Act* case, the Court also expanded on the test that applies to all measures that interfere with basic rights, including privacy. Generally speaking, any interference with one of the rights protected under the Basic Law must be authorized by parliamentary law, serve a legitimate purpose, and satisfy the proportionality test, i.e. suitability, necessity, and proportionality *stricto sensu*.[7] In the case of the right of informational self-determination, the Court further

2. *Microcensus Case*, 27 BVerfGE 1 (1969), *translated and reprinted in* DONALD P. KOMMERS & RUSSELL A. MILLER, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 356–58 (3d ed. 2012).

3. *See generally id.*

4. *Census Act Case*, 65 BVerfGE 1, Dec. 15, 1983, *translated and reprinted in* DONALD P. KOMMERS & RUSSELL A. MILLER, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 408–09 (3d ed. 2012).

5. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014) [hereinafter REPORT ON USA PATRIOT ACT].

6. *Census Act Case*, 65 BVerfGE 1 (1983), *supra* note 4, at 409.

7 DONALD P. KOMMERS & RUSSELL A. MILLER, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 67 (3d ed. 2012).

specified that the legislative basis for personal data processing must be clear and precise and that, to satisfy proportionality, there must be organizational and procedural safeguards capable of preventing infringements of the right[8]

This constitutional frame has shaped both the jurisprudence of other constitutional courts—in particular the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU)—as well as positive lawmaking in Germany and at the European level. Both the ECtHR and the European Court of Justice have recognized that the right to privacy, guaranteed under Article 8 of the European Convention of Human Rights, covers personal data and is triggered whenever public or private entities gather information that can be associated with an individual.[9] Both courts use the same the jurisprudential framework of (1) a basis in law, (2) clearly defined, legitimate purposes, and (3) proportionality to analyze data-protection challenges, as will be discussed in connection with NSA surveillance.

In the legislative sphere, the fundamental right to data privacy has shaped the design of data-protection legislation in most European jurisdictions. Within Germany, the Court's first judgment in the *Microcensus* case provided much of the impetus for the first federal data-protection law. A small coalition party, the Free Democratic Party, took on the issue of new technologies and democracy, and, drawing on the case and the work of a number of prominent legal scholars, pressed for privacy legislation.[10] A government bill was introduced in May 1973, and after a long series of parliamentary debates, mostly centered on the extent of private-sector coverage and the design of the enforcement system, a federal law was finally passed in January 1977.[11] That law—together with a series of sectoral laws specific to areas such as telecommunications and the police—served as the constitutionally required legislative act authorizing the interference with the right to privacy. The law set down the conditions for the use and sharing of personal information, most of which turned on the proportionality requirement that the data processor handle the information only insofar as "necessary" to accomplish the original purpose of the data operation.[12] Further, it established a legal

8. *Id.* at 410–11.

9. *See, e.g.*, Amann v. Switzerland, 30 Eur. Ct. H.R. 843, 858 (2000). Since the entry into force of the Lisbon Treaty in 2009, the right to privacy is protected under Article 7 of the European Charter of Fundamental Rights and the right to personal data protection is recognized specifically under Article 8 of the European Charter of Fundamental Rights.

10. *See, e.g.*, ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY: REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 51–52, 63–69 (2008) (describing the role of Free Democratic Party); Klaus Flachmann, *Kreditwirtschaft und Datenschutz*, 26 ZEITSCHRIFT FUR DAS GESAMTE KREDITWESEN 56 (1973) (noting and criticizing role of legal academics and the theoretical tenor of the policy debates); Spiros Simitis, *Chancen un Gefahren der elektronischen Datenverarbeitung*, 16 NEUE JURISTISCHE WOCHENSCHRIFT 673, 675, (1971) (providing an example of legal scholarship); Steinmuller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider, Grundfragen des Datenschutze Gutachten im Auftrag des Bundesmnisteriums des Innern, July 1971 (BT-Drucksache VI/3826) (legal scholarship).

11. COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 77–90 (1992); DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES 22–24 (1989).

12. Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], 1977.

framework for oversight and enforcement.[13]

The Court's second judgment in the *Census Act* case also triggered parliamentary action, resulting in a series of amendments to the federal data-protection law in 1990.[14] In line with that case, some of the amendments were designed to extend privacy rights to the entire gamut of data processing activities: for instance, in the public sector, the collection of personal data—not simply the storage and use of personal data—was regulated for the first time.[15] Other amendments were designed to improve enforcement of the right: the independence of the Federal Data Protection Commissioner was improved,[16] state authorities acquired new enforcement powers,[17] individuals were expressly given the right to vindicate their privacy rights in court, and the rules on proving damages were relaxed for lawsuits brought against both private and public bodies.[18]

Turning to the positive law at the European level, both the Council of Europe Convention 108 (Convention 108) and the EU Data Protection Directive were shaped by the rights framework. This is particularly clear in the Directive, proposed in 1990 and adopted in 1995.[19] Although the Directive was based on the market harmonization competence in the EC Treaty, designed to facilitate data flows and trade in Europe, it was essentially conceived as a measure that would improve protection of the fundamental right to privacy throughout Europe.[20] The main proponents of the Directive were national data-protection officials with a mission to safeguard the right to privacy, and they ensured that the purpose, structure, and text of the Directive were rooted in the logic of rights.[21] Thus the Directive declared as its object that the "member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[22] In line with the constitutional law on rights, the Directive serves as the law that authorizes the interference with the right to privacy implicated by any collection and use of personal information and, in accordance with the constitutional duty of clarity and precision, it sets down the exhaustive list of purposes for which such interference is allowed.[23] And it satisfies the constitutional requirement of proportionality by limiting data processing to that which is necessary to accomplish the stated

13. BDSG, 1977 §§ 17–42; BENNETT, *supra* note 11, at 180; FLAHERTY, *supra* note 11, at 25.

14. BDSG, 1990.

15. *See id.* at § 13.

16. *See id.* at § 22(1).

17. *See id.* at § 38(5).

18. *See id.* at § 8.

19. EP and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

20. *See* Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 834–44 (2005) [hereinafter *Transgovernmental Networks*].

21. *See* NEWMAN, *supra* note 10, at 74.

22. EP and Council Directive 95/46, *supra* note 19, art. 1.

23. *Id.* art. 7.

purpose and by establishing a set of organizational and procedural guarantees to protect against privacy violations.[24]

Turning to the United States, there it is indeed appropriate to begin the historical account of data privacy with the Code of Fair Information Practices. This included a number of principles that remain prominent in contemporary privacy law: transparency in the use and processing of data; an individual right of access to and, if appropriate, correction of personal data; the duty (on the part of data users) to ensure the accuracy of personal data; the obligation to adopt security measures to prevent fraudulent uses of data; and a limitation on uses to the purposes for which the personal information was originally collected.[25] The Fair Information Practices were adopted in the U.S. Privacy Act of 1974 and in numerous sector-specific U.S. laws.[26] When, in 1980, a set of data-protection guidelines was adopted by the Organization for Economic Cooperation and Development, a number of the American legal principles were included.[27] These guidelines, in turn, influenced the negotiations on Convention 108.[28] And today, they are reflected in national privacy regulation in Europe, which give prominence to transparency, access, accuracy, security, and use limitations.

Even though widespread adoption of Fair Information Practices has produced significant convergence in this policy area, not only between the United States and Europe but among jurisdictions globally, the historical trajectory on the American side of the Atlantic has also followed a distinctive path that has generated regulatory conflict with Europe and has given rise to a series of diplomatic efforts to render the two systems compatible. The first significant difference was and continues to be the absence of constitutionalization of the policy area. Even though the periodic expert reports that have been commissioned in response to public concern over information technologies have generally canvassed the constitutional law in the domain of privacy and have underscored the importance of privacy for liberal values, they have all stopped short of recognizing that there is, or should be, a constitutional right to data privacy.[29] The failure to reach such a conclusion is understandable because the Supreme Court's jurisprudence does not squarely support such a conclusion. All of the older cases suggest that such a right does not exist,[30] and even though the most recent decisions of the Court in the area indicate that the tide might be turning in light of the dramatic developments that have occurred in digital technologies, there still does not appear to be a solid

24. *See* Francesca Bignami, *Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy*, 59 AM. J. COMP. L. 411, 435–41 (2011) [hereinafter *Cooperative Legalism*].

25. RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, *supra* note 1, at 33–46.

26. DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW: CASES & MATERIALS 655–60 (2009).

27. *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, 8.

28. *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 75 (2003).

29. For recent examples, see generally LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGY (2013) [hereinafter LIBERTY AND SECURITY]; REPORT ON USA PATRIOT ACT, *supra* note 5.

30. *See generally* Smith v. Maryland, 442 U.S. 735 (1979); Whalen v. Roe, 429 U.S. 589 (1977); United States v. Miller, 425 U.S. 435 (1976).

majority in favor of a constitutional right to data privacy.[31]

The second difference, related to the first, is the more limited safeguards for privacy in positive law. This is evident across a number of legislative enactments and, to use the constitutional framework described earlier, takes two primary forms. First, the substantive limits on collection, use, sharing, and retention of data that are loosely connected to the proportionality requirement of necessity are generally more relaxed in the United States than in Europe.[32] To grossly oversimplify, in U.S. law, more information—from the collection phase to the erasure phase—is generally viewed as better than less information. Therefore, although U.S. and European law share similar commitments to transparency of databases, access to and correction of one's personal data, reliability of personal information, and digital security, U.S. law contains fewer restrictions on how much personal data may be collected, how such data may be used, and how long that data may be kept. Second, in the United States, the enforcement of privacy law is largely entrusted to private litigants and courts, not administrative agencies. This is especially true for privacy regulation of the public sector, which lacks a powerful set of administrative overseers comparable to European data-protection authorities.[33] The importance of courts, as opposed to administrative agencies, in the U.S. regulatory scheme has undermined public oversight because of the difficulty of analogizing privacy harms to traditional torts and the many doctrinal obstacles this has created for litigants seeking redress through the courts.[34]

To illustrate briefly the more limited statutory safeguards for privacy under U.S law, compare the U.S. Privacy Act of 1974 with the Council of Europe's Convention 108. The Privacy Act regulates the government's collection, use, and disclosure of all types of personal information. It contains the familiar transparency, access and correction, reliability, and security principles. However, there are relatively few substantive limits on what can be done with personal information. Agencies can collect any personal information that is relevant and necessary to the agency's legal purposes set down by congressional statute or presidential executive order.[35] The only type of personal information that requires special justification to be collected is personal data "describing how any individual exercises rights guaranteed by the First Amendment [right to freedom of expression and freedom of association]"[36] as opposed to the numerous categories of information considered to be sensitive in Convention 108, including racial

31. *See generally* Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945 (2012).

32. *See, e.g.*, FRANCESCA BIGNAMI, THE US LEGAL SYSTEM ON DATA PROTECTION IN THE FIELD OF LAW ENFORCEMENT: SAFEGUARDS, RIGHTS AND REMEDIES FOR EU CITIZENS 36 (2015) [hereinafter BIGNAMI, THE US LEGAL SYSTEM], http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf .

33. *Cooperative Legalism*, *supra* note 24, at 419.

34. Francesca Bignami, *European versus American Liberty: A Comparative Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 684–86 (2007) [hereinafter *European versus American Liberty*].

35. 5 U.S.C. § 552a(e)(1) (2012).

36. 5 U.S.C. § 552a(e)(7).

origin, criminal convictions, and health information.[37] Although the Privacy Act generally prohibits sharing with other government agencies without the consent of the individual involved, it makes a broad exception for "routine uses" disclosed to the public at the time the record system is created.[38] In contrast with the Convention, which says that personal data shall be "preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which those data are stored,"[39] the Privacy Act contains no provision regulating the length of data retention. Last, in the case of intelligence and law enforcement agencies, most of these substantive requirements can be avoided if, at the time that legal notice of the database is given (part of the transparency duty), the agency claims the exemptions available under the Act.[40] On the question of oversight, the Privacy Act confines enforcement to litigation and the courts: it gives individuals the right to sue the government for damages and, in some instances, to receive injunctive relief.[41] Government officials may also be criminally prosecuted for certain violations of the Privacy Act.[42] Although the original bill would have established an independent commission tasked with enforcement, similar to the model that took root in Europe in the 1970s, it was removed in the end as part of the compromise necessary to pass the Privacy Act.[43]

The third significant transatlantic difference that emerged early on and that persists still today is the absence, in the United States, of a comprehensive, privacy law applicable to the private sector. Like an independent commission, regulation of the private sector was proposed in the early days of the policy area: the original version of the Privacy Act would have regulated personal data processing in both the public and private sectors.[44] The Watergate scandal, however, was fresh in the minds of lawmakers, and the prospect of a government Big Brother was their principal fear.[45] For their part, industry groups and many privacy experts successfully opposed comprehensive privacy regulation on the grounds that it was too early to discern which kinds of privacy problems would emerge in the private sector.[46] They also argued that the diverse circumstances of various economic sectors would be handled best in tailored, sector-specific statutes rather than in a cross-cutting piece of legislation.[47] Therefore, even though privacy statutes have been enacted to regulate a wide array of market sectors—banking, telecommunications, health care, credit reporting, and so on—there is no single

37. *See* Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, no. 108 (Jan. 28, 1981), art. 6 [hereinafter *Convention 108*].

38. 5 U.S.C. § 552a(b)(3).

39. *Convention 108*, *supra* note 37, art. 5e.

40. 5 U.S.C. § 552a(j)–(k).

41. 5 U.S.C. § 552a(g).

42. 5 U.S.C. § 552a(i).

43. *See* S. 3148, 93d Cong. (1974) (original version with privacy commission); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (version without privacy commission); LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 at 119–24 (1976), http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

44. S. 3418, 93d Cong. § 201 (1974).

45. LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, *supra* note 43, at 4, 832, 893.

46. *See, e.g.*, *id.* at 68.

47. S. REP. NO. 93-1183, at 19–20 (1974).

omnibus law capable of capturing the data practices, sectors, and emerging technologies that fall in between the cracks of the individual statutes.[48]

B. Regulatory Conflict and Cooperation

Although many aspects of European and U.S. privacy regulation are being debated at present and may change in the near future, the deep-seated differences analyzed in the previous section are unlikely to disappear anytime soon and are vital to understanding the regulatory conflicts and attempts at harmonization of the past twenty years. Conflict with the United States has involved largely the European Union as opposed to individual member states. When privacy regulation first became a salient issue in transatlantic relations, in the mid-1990s, attention was mostly focused on the private sector and market actors. By the mid-2000s, however, U.S. government actors also came under scrutiny for their use of personal data to screen for suspected security threats as well as related criminal offenses. The following narrates both sets of disputes through to the revelations of NSA surveillance in summer 2013.

1. Regulation of the Market: Safe Harbor

The divergent U.S. and EU approaches to privacy regulation first emerged as a salient problem and a potential threat to transatlantic trade in the mid-1990s. Like many of the early national data-protection laws that had preceded it, the 1995 EU Directive contained a blocking provision that required national authorities to prohibit data transfers to jurisdictions without adequate privacy guarantees.[49] In view of the lack of comprehensive marketplace regulation in the United States, U.S. firms with European operations feared that the U.S. legal framework would not be considered adequate and that, as a result, data transfers from Europe to the United States would be deemed illegal.[50] In response, the U.S. Department of Commerce initiated negotiations with the European Commission and the two sides reached an agreement on "Safe Harbor" privacy principles that, if adopted by U.S. organizations, would entitle those organizations to a presumption of "adequacy" under the Directive.[51] The Safe Harbor agreement took effect in 2000, as did the Commission decision granting those firms that adhered to the Safe Harbor principles an adequacy finding.[52] Under the Safe Harbor agreement, the legal basis for collecting and using personal information is consent. Consent is assured by giving the consumer "notice" of personal data practices and by allowing the consumer "choice" respecting disclosures to third parties and uses of personal

48. Examples of sector-specific statutes include the Right to Financial Privacy Act, Pub. L. No. 95-630 (1978), the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2012), and the Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

49. EP and Council Directive 95/46, *supra* note 19, arts. 25–26.

50. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 69–79 (2000).

51. *See* Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000).

52. *Id.*

data that are incompatible with the original purpose of data collection. The Safe Harbor principles, in line with the Fair Information Practices discussed earlier, also include a right of individual access and correction, data security, limitations on use and data transfers, and independent dispute settlement as an enforcement mechanism. Firms that wish to invoke Safe Harbor must incorporate these principles in their privacy policy, make their privacy policy public and ensure that it is readily available to consumers, and self-certify their adherence to Safe Harbor on an annual basis with the Department of Commerce.[53] Since firms hold themselves out as subscribing to the Safe Harbor principles, a violation of the principles can be sanctioned by the Federal Trade Commission (FTC) under its powers to bring enforcement actions against unfair or deceptive acts or practices.[54]

There has been considerable debate over the effectiveness of Safe Harbor, both as a vehicle for bringing U.S. corporate practices into line with EU law and as a tool for safeguarding consumer privacy. In the first years after Safe Harbor came into force, relatively few firms signed up, but today over 3,200 have self-certified with the Department of Commerce.[55] Although a number of observers have called into question whether the firms that hold themselves out as complying actually do so, the FTC has recently begun taking a more proactive approach to enforcement. The well-publicized settlement orders against Google, Facebook, and Myspace all included Safe Harbor counts.[56] Additionally, the FTC has brought over a dozen enforcement actions against firms that claimed Safe Harbor membership but failed to renew their self-certification with the Department of Commerce.[57]

More broadly, there has been skepticism over whether consent—that is, notice and choice—operates as an effective device for safeguarding privacy. This skepticism applies not only to Safe Harbor but to U.S. and EU privacy regulation broadly speaking, which also rely heavily on consent.[58] The privacy notices, which describe what will be done with personal information, are unwieldy, incomprehensible, and generally go unread by consumers. Even if privacy notices were comprehensible and effective disclosure might therefore exist, consumer choice is significantly limited by the very expansive interpretation of what uses are

53. *See id.*

54. *See id.*

55. *See Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of the EU Citizens and Companies Established in the EU*, at 4, COM (2013) 847 final (Nov. 27, 2013) [hereinafter *Safe Harbor*].

56. Complaint at 8, MySpace LLC, FTC File No. 102 3058, No. C-4369 (F.T.C. Aug. 30, 2012); Complaint at 19, Facebook, Inc., FTC File No. 092 3184, No. C-4365 (F.T.C. July 27, 2012); Complaint at 7, Google Inc., FTC File No. 102 3136, No. C-4336 (F.T.C. Oct. 13, 2011).

57. *See* orders referenced at https://www.ftc.gov/news-events/press-releases/2014/06/ftc-approves-final-orders-settling-charges-us-eu-safe-harbor; and orders referenced in www.ftc.gov/news-events/press-releases/2015/05/ftc-approves-final-orders-us-eu-safe-harbor-cases.

58. *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE 'INFORMATION ECONOMY' 343 (Jane I. Winn ed., 2006); WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 15, 21 (2012) (discussing guarantees above and beyond notice and choice entailed by the rights of "Respect for Context" and "Focused Collection"), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

"compatible" with the original purposes of data collection and the difficulty of navigating electronic disclosures to opt out of those uses and third-party transfers that are "incompatible." Furthermore, consumers are generally unable to choose among vendors based on their privacy practices because of the absence of significant differences in vendor policies. Overall, therefore, as a mode of policy coordination and regulatory cooperation in the context of a globalized data economy and multiple legal jurisdictions, Safe Harbor has proven quite successful. As a device for protecting consumer privacy, however, it has been less effective. Policy thinking has evolved considerably since the Safe Harbor agreement was negotiated over a decade ago and therefore it might very well be necessary to change the principles contained in Safe Harbor to assure adequate safeguards for privacy.

The Safe Harbor agreement has recently been undone for reasons quite different from the consumer privacy concerns that originally motivated the agreement.[59] As revealed by Snowden, U.S. Internet companies afford national security agencies extensive access to the personal information of their clients. However, the Safe Harbor agreement and the accompanying Commission adequacy decision are almost entirely focused on market actors and the privacy safeguards that apply when they handle consumer data. The legal instruments have virtually nothing to say on the law that applies when the U.S. government seeks access to consumer data and whether that law is adequate from the perspective of EU law. As a result, as will be discussed at greater length later in this article, the Court of Justice of the European Union (CJEU) has found that Safe Harbor can no longer be used as a legal basis for data transfers from the EU to the U.S.

2. Regulation of Government Actors: PNR and SWIFT

Shortly after 9/11, the EU and the United States became mired in a separate set of privacy conflicts—U.S. government access to EU airline passenger data and EU financial transactions data.[60] This set of regulatory conflicts, unlike Safe Harbor, involved the public sector, specifically government agencies with responsibilities in the field of national security and criminal law. Many of the same regulatory differences that triggered the earlier dispute over the private sector were on display in this second round—the different definitions of permissible personal data processing and the absence, in the United States, of an independent enforcement agency—but were somewhat more surprising given the relatively robust nature of public sector regulation in the United States. As compared to the private sector, there is comprehensive statutory regulation of government actors—namely, the Privacy Act—and there exists a constitutional right to privacy against intrusive government surveillance. As already discussed, however, U.S. constitutional law is largely silent on the right to data privacy and the guarantees of U.S. statutory law are limited in the area of national security and law

59. *See infra* text accompanying notes 180–82.

60. *See generally European versus American Liberty*, *supra* note 34, at 668–74.

enforcement, a trend that has been exacerbated by the post-9/11 political climate.

To understand the contours of this second round of regulatory conflict, it is necessary to first address the jurisdictional issue of how the regulation of police and national security agencies in the United States came to be part of the EU agenda. There are two parts to the answer. First, privacy regulation of the government and the market is interrelated, given that the government is a major user of personal information collected by private entities. Under the EU Directive and Safe Harbor, firms may disclose information to public actors, including law enforcement and national security agencies, if required to do so by law.[61] In the case of European governments, which are subject to a fundamental right to personal data protection and to omnibus data-protection laws, the government's collection of personal data must be based on a clear and precise legal authority and must respect the proportionality principle. When a non-European state requests such information from firms operating within its jurisdiction, and the request is not in line with the guarantees of European data-protection law, then the privacy safeguards for the data in the foreign jurisdiction might not be considered "adequate" In such a case, the data transfer is unlawful under Article 25 of the Directive and European authorities are empowered to take action to either block such transfers or to negotiate agreements that establish the appropriate safeguards in the foreign jurisdiction. The second explanation for the public-sector dimension to the U.S.–EU regulatory dispute is more straightforward: the powers of the EU have progressively expanded to include police, justice, and immigration.[62] After the most recent round of treaty amendments contained in the Lisbon Treaty, these areas are squarely within the jurisdiction of the EU institutions.[63]

In response to 9/11, the U.S. government embarked on an aggressive campaign to collect, pool, and analyze data with possible national security implications, and one of the casualties of this campaign has been a series of transatlantic disputes over the personal data of European citizens. The first involved the passenger name records (PNR) collected by airlines. After 9/11, the U.S. authorities began requiring that all airline carriers submit the PNR data for flights to, from, or through the United States. Given the breadth of the U.S. program—the amount of information involved, the extensive sharing among government agencies, and the unclear privacy safeguards—a number of European air carriers approached the European Commission for guidance on how to satisfy their EU Directive obligation to safeguard the privacy of data transferred to third countries.[64] The significant regulatory differences between the EU and the United States—this time in the public domain—triggered lengthy negotiations over an agreement that would satisfy both security and privacy concerns. The two sides finally reached a deal in 2004.[65] There have been three successive PNR agreements: The original 2004

61. *See* EP and Council Directive 95/46, *supra* note 19, art. 7(c); *Safe Harbor*, *supra* note 55, Annex 1.
62. *See* PAUL CRAIG & GRAINNE DE BURCA, EU LAW: TEXT, CASES, AND MATERIALS 923–56 (5th ed. 2011).
63. *See id.* at 24–28.
64. *Transgovernmental Networks*, *supra* note 20, at 862.
65. *Id.* at 864–65.

agreement; its 2007 replacement; and the agreement currently in force, from 2012.[66]

Especially on the European side, the adequacy of the privacy safeguards afforded by the PNR agreements has been and continues to be contested by a number of institutional actors, including the European Parliament, the European Data Protection Supervisor, and the Article 29 Working Party.[67] Compared to Safe Harbor, this dispute has festered longer. At least part of this acrimony can be attributed to post-9/11 politics and the fairly intransigent stance of successive U.S. administrations on security-related matters.

The terms of cooperation set down under the current EU–U.S. PNR agreement cover the familiar privacy categories of transparency, individual access and correction, security, enforcement, and proportionality (which includes purpose, amount of data collected, sensitive data, retention of data, and data sharing).[68] Before turning to proportionality and enforcement—the two major points of transatlantic difference reviewed earlier in this article and the source of most of the conflict in the PNR negotiations—it is worthwhile mentioning individual access and correction, since it raises issues that have also become prominent in the NSA surveillance controversy. European policymakers have long been perplexed by the exclusion of non-U.S. persons, that is, persons who are not U.S. citizens or legal permanent residents, from coverage under the Privacy Act of 1974. As will be explained below, this differential treatment of U.S. and EU persons has since come to the fore in the context of NSA surveillance because it also marks privacy guarantees in the national security domain. The exclusion of non-U.S. persons from the Privacy Act is important for the access and correction principle because it prevents Europeans from exercising access rights under that legislation.

66. Commission Decision 2004/535, 2004 O.J. (L 235) 11; Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), 2007 O.J. (L 204) 18; Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, 2012 O.J. (L 215) 5 [hereinafter 2012 Agreement].

67. *See, e.g.*, Article 29 Working Party, *Opinion 5/2007 on the Follow-up Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security Concluded in July 2007* (Aug. 17, 2007), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp138_en.pdf; *Letter from Article 29 Working Party to Member of the LIBE Committee of the European Parliament, Brussels*, Ref. Ares (2012)15841-06/01/2012; European Data Protection Supervisor, *Opinion on the Proposal for a Council Decision on the Conclusion of the Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security*, 2012/C 35/03 (Sept. 2, 2012).

68. 2012 Agreement, *supra* note 66. For a general description of the operation of the program, see *Report from the Commission to the European Parliament and the Council on the Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Records to the United States Department of Homeland Security Accompanying the Report from the Commission to the European Parliament and to the Council on the Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Records to the United States Department of Homeland Security*, COM (2013) 844 final (Nov. 27, 2013).

The EU–U.S. agreement, therefore, specifies that the Freedom of Information Act is to be used to obtain the information contained in the PNR held by the Department of Homeland Security (DHS).

Returning to proportionality and enforcement, the purposes of PNR data processing are limited mostly to preventing and prosecuting terrorist offenses and transnational crimes punishable by imprisonment of three years or more. Nineteen types of PNR data can be requested, and the transmission from the air carrier to DHS occurs via a "push" system, meaning that the carrier transmits the required data into DHS's database.[69] The "push" system is designed to reduce the risk that irrelevant data will be collected, which can occur when DHS is authorized to extract the PNR directly from the carrier's reservation system through what is known as a "pull" system.[70] Sensitive data—in the PNR context, often religious affiliation revealed by meal preferences—can only be used under exceptional circumstances and are generally deleted after thirty days. PNR data are retained for fifteen years—five years in an "active" database and ten years in a "dormant" database—after which time they are anonymized; if data are used for a specific case or investigation they may be retained as long as necessary.[71] Sharing this data with other domestic government agencies is allowed only for the counterterrorism and law enforcement purposes authorized by the agreement and even then, only "in support of those cases under examination or investigation."[72] Presumably, therefore, sharing does not occur in bulk, but rather only with reference to specific individuals or events being investigated. As for enforcement and oversight, the DHS Privacy Office is tasked with primary responsibility, but the agreement also mentions other "Department Privacy Officers," the DHS Office of Inspector General, the Government Accountability Office, and the United States Congress.[73]

In 2006, the second major dispute over privacy regulation of government actors emerged, this time over access to and use of financial data. Since 9/11, the United States Treasury Department, under a program known as the Terrorist Finance Tracking Program (TFTP), had been collecting vast quantities of financial data on bank transfers and other types of operations from the Belgian private entity the Society for Worldwide Interbank Financial Telecommunications (SWIFT).[74] SWIFT is the largest financial telecommunications network in the world and is the system used to execute and record most interbank transactions. Although it is established in Belgium, it had two operational servers, one in the Netherlands and a mirror server in the United States. Because of its presence in the United States, SWIFT was subject to the administrative subpoena power of the

69. *Id.* at 14.

70. *See, e.g.*, Article 29 Working Party, *Opinion 7/2010 on European Commission's Communication on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries*, at 6 (Nov. 12, 2010), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp178_en.pdf.

71. 2012 Agreement, *supra* note 66, at 8 (art. 8).

72. *Id.* at 10 (art. 16).

73. *Id.* at 10 (art. 14).

74. For an account of the initial stages of the TFTP dispute, see *European versus American Liberty*, *supra* note 34, at 672–74.

Department of Treasury, which is authorized to request financial information for counterterrorism purposes. But because SWIFT is established in Belgium and the vast majority of the data in the U.S. mirror server originated in the EU, SWIFT was also clearly subject to European privacy law and the duty under that law to ensure that privacy would be respected upon the transfer of that data to third countries. In fact, from the beginning, SWIFT knew that it was running the risk of violating European privacy law. Because it was prohibited under the terms of the administrative subpoena from disclosing the data transfers, SWIFT requested and received a "comfort letter" from the Department of Treasury in which the Department pledged to support SWIFT in the event that it was later sued by foreign governments or third parties.

When the TFTP was revealed in 2006, the European Parliament and European data-protection authorities strongly condemned the U.S. government for secretly and indiscriminately collecting the private financial records of millions of Europeans. Both the Belgian data-protection authority and the Article 29 Working Party found that SWIFT had violated European privacy law.[75] The European Commission and the U.S. Department of Treasury subsequently entered into discussions to assuage European privacy concerns. The result was a number of Treasury representations laying out the scope of the privacy guarantees built into the TFTP and an agreement allowing an "eminent European person" appointed by the Commission to conduct periodic reviews to ensure that Treasury had complied with its representations.[76] Although this oversight system did indeed result in two largely favorable reports to the Commission by the French magistrate Jean-Louis Bruguière,[77] it was soon taken over by events: SWIFT announced in 2007 that it planned to establish a new operating center in Switzerland by 2009 so that intra-European bank messages could be stored exclusively in Europe.[78] It therefore became urgent for the U.S. government to reach a deal with the EU to assure continued access to European financial transaction data once those data were

75. Belgian Data Protection Commission, Opinion No. 37/2006 of 27 Sept. 2006 on the Transfer of Personal Data by the CSLF SWIFT by Virtue of UST (OFAC) Subpoenas, at 26–27, http://www.steptoe.com/assets/attachments/2644.pdf; Article 29 Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (Nov. 22, 2006), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf.

76. Notice: Publication of U.S./EU Exchange of Letters and Terrorist Finance Tracking Program Representations of the United States Department of the Treasury, 72 Fed. Reg. 60054-02 (Oct. 23, 2007).

77. *Commission Report on the Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program* (Mar. 13, 2011), http://ec.europa.eu/dgs/home-affairs/news/intro/docs/commission-report-on-the-joint-review-of-the-tftp.pdf; *Report on the Second Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program* (Dec. 14, 2012) [hereinafter *Report on Implementation of Agreement*], http://ec.europa.eu/dgs/home-affairs/pdf/20121214_joint_review_report_tftp_en.pdf.

78. Andre R. Jaglom, *Internet Distribution, E-Commerce and Other Computer Related Issues: Current Developments in Liability On-Line, Business Methods Patents and Software Distribution, Licensing and Copyright Protection Questions*, SW041 ALI-CLE 687, 668–69 (2015).

physically removed from the United States and were therefore no longer subject to the U.S. administrative subpoena power. The first agreement, signed in 2009, was voted down by the European Parliament largely in reaction to what was perceived as a move by the Council and Commission to circumvent the Parliament's new powers in the areas of police and judicial cooperation and external relations after the entry into force of the Lisbon Treaty.[79] The second EU–U.S. agreement (TFTP II), signed and ratified in summer 2010, is the agreement currently in force.[80]

Similar to the PNR agreement, the privacy guarantees in TFTP II can be grouped into transparency; individual access and correction; security; enforcement; and proportionality, which includes purpose, amount of data collected, sensitive data, retention of data, and data sharing. The procedure outlined under the agreement requires that the Treasury issue requests for data—generally categories of data—that are "necessary" for purposes of prevention, investigation, detection or prosecution of terrorism or terrorist financing and that are "tailored as narrowly as possible to minimise the amount of data requested."[81] Such requests are issued to SWIFT and to Europol, which must review the request for compliance with proportionality before SWIFT can release the data.[82] Once the Treasury receives the data, it may only conduct individualized searches—not data mining—and only when it suspects that the subject in question has a "nexus to terrorism or its financing."[83] Although the agreement recognizes a category of "sensitive data," it anticipates that the financial transaction data will rarely, if ever, implicate sensitive data; most likely for this reason, the agreement does not specify the special precautions that would be taken in the unlikely event that sensitive data were generated.[84] Retention periods differ for "extracted" and "non-extracted" data—non-extracted data are to be deleted after five years, whereas extracted data can be retained for as long as necessary for the specific investigation or prosecution for which they are used.[85] The information extracted in individualized searches may be shared with other law enforcement and national security agencies "for lead purpose only and for the exclusive purpose of the investigation, detection, prevention, or prosecution of terrorism or its financing."[86] Similar to PNR, oversight is entrusted primarily to the Privacy Office, this time in the Treasury Department.

Even more so than the PNR agreement, TFTP II has failed to allay European privacy concerns and has been the object of repeated criticism by

79. European Parliament Press Release, *SWIFT: European Parliament Votes Down Agreement with the US* (Nov. 2, 2010).

80. Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data from the European Union to the United States for the Purposes of the Terrorist Finance Tracking Program, 2010 O.J. (L 195) 5 [hereinafter 2010 Agreement].

81. *Id.* at 8 (art. 4.2.(c)).

82. *Id.* at 8 (art. 4.4).

83. *Id.* at 9 (art. 5.6).

84. *Id.* at 9 (art. 5.7).

85. *Id.* at 9 (art. 6).

86. *Id.* at 9 (art. 7).

parliamentarians and European data-protection authorities.[87] This can be explained by virtue of the sheer volume of personal data entailed and the secretive nature of the program. Whereas passenger name records are relatively discrete data points, linked to a specific person and flight, the requests made under TFTP II are drawn broadly so as to capture possible terrorist financing. Moreover, whereas individuals may experience fairly immediate consequences from PNR—for instance, repeated secondary screening on entry in the United States, which may give rise to the access, correction, and oversight procedures outlined in the agreement—the financial data used in TFTP will generally only trigger visible government action when the individual is apprehended or prosecuted, making those provisions largely theoretical. Finally, transparency is particularly challenging in the TFTP context: the Treasury has argued that the effectiveness of the program would be undermined by the disclosure of the terms used to extract the data or the number of investigations supported by the financial data.[88]

To conclude this discussion, it is important to note one element of transatlantic privacy conflicts in the public sector that sets them off from conflicts involving market regulation. As Henry Farrell and Abe Newman have argued, the U.S.–EU disputes over PNR and TFTP have not only set the EU against the United States but have exposed divisions between institutional actors within the EU.[89] Ministries of Home Affairs, represented on the Council, and representatives of the more conservative political groups in the European Parliament, such as the European People's Party, have generally been more favorable to sharing data with the United States than data-protection authorities and liberal and left-leaning parliamentarians. Moreover, these pro-security actors have used U.S.–EU negotiations over PNR and TFTP to leverage more extensive powers for their own police and intelligence agencies: both PNR and TFTP II include provisions on reciprocity that require the U.S. authorities to share the data generated by the PNR and TFTP programs with their European counterparts.[90] Furthermore, PNR and TFTP II have served as a springboard for similar intra-European data-sharing programs.[91] These transatlantic disputes, therefore, both have exposed the conflicting positions of privacy and security advocates within the EU and have offered an opportunity for pro-security actors to enhance the EU's law

87. *See, e.g.*, *Letter from Article 29 Working Party to Melissa A. Hartmen, Deputy Assistance Secretary, Privacy, Transparency and Records, U.S. Department of the Treasury* (June 7, 2011); Committee on Civil Liberties, Justice and Home Affairs, European Parliament, *Minutes from Meeting of 3 October 2011*, *from 15.00 to 18.30, and 4 October 2011, from 09.00 to 12.30 and from 15.00 to 18.30*, LIBE_PV(2011) 1003_1.

88. *See, e.g.*, *Report on Implementation of Agreement*, *supra* note 77, at 5.

89. *See* Henry Farrell & Abraham Newman, *The New Politics of Interdependence: Cross-National Layering in Trans-Atlantic Regulatory Disputes*, 48 COMP. POL. STUD. 1, 10–15 (2014); Abraham Newman, *Transatlantic Flight Fights: Multi-level Governance, Actor Entrepreneurship and International Anti-terrorism Cooperation*, 18 REV. OF INT'L POL. ECON. 481 (2011).

90. 2012 Agreement, *supra* note 66, at 11 (art. 20); 2010 Agreement, *supra* note 80, at 10 (arts. 10–11).

91. *See, e.g.*, *Proposal for a Directive of the European Parliament and of the Council on the Use of the Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime*, COM (2011) 32 final (Feb. 2, 2011).

enforcement and national security capabilities.

III
NSA SURVEILLANCE

The latest chapter in the history of transatlantic disputes over data privacy began in 2013 with the Edward Snowden leaks of massive NSA surveillance. As with PNR and SWIFT, the EU–U.S. controversy concerns the activities of government agencies responsible for national security, but the immense scale of the NSA programs makes the other two seem fairly inconsequential by comparison. More than the previous episodes, the NSA's activities have exposed rifts not only between the two sides of the Atlantic, but also within Europe, between security agencies and privacy institutions and between the actual practice of state security and the formal legal requirements and fundamental rights that are supposedly applicable against all state actors. As the European public learned from the Snowden leaks, the NSA has been routinely assisted by its counterparts in the United Kingdom, France, and other European countries even though many of the surveillance programs squarely implicate the European right to personal data protection. This part considers the implications of the NSA disclosure both for transatlantic relations and for the future evolution of EU privacy regulation.

A. European Perspectives on the Snowden Leaks

Much is unknown about the programs of mass surveillance carried out by the NSA and its European counterparts in the last decade. Western governments have frequently resorted to the state secrecy doctrine to maintain a veil of ignorance over the general features of intelligence programs.[92] However, as a result of the Snowden leaks and the official and unofficial disclosures that ensued, a series of basic facts have been clarified and can be assumed uncontroversial.[93] Although the leaks concerned a truly spectacular array of surveillance activities, attention has focused on two in particular: One program, conducted under Section 215 of the Patriot Act, which collects the call records of virtually every American;[94] and another, conducted under Section 702 of the Foreign Intelligence Surveillance Act, which is targeted at foreigners and has as a result been the main focus of European

92. Interestingly, whereas the U.S. government has declassified many documents following the Datagate, European governments so far have not taken similar steps.

93. *See* CASPAR BOWDEN, EUR. PARLIAMENT POL'Y DEPT., CITIZENS' RTS. & CONST. AFF., THE U.S. SURVEILLANCE PROGRAMMES AND THEIR IMPACT ON EU CITIZENS' FUNDAMENTAL RIGHTS (2013), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf.

94. *See generally* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014) [hereinafter REPORT ON TELEPHONE RECORDS PROGRAM], https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf. For a detailed analysis, see Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 HARV. J.L. & PUB. POL'Y 757, 770–76 (2014); David S. Kris, *On the Bulk Collection of Tangible Things,* 7 J. NAT'L SEC. L. & POL'Y 209 (2014).

criticism.[95]

Under Section 702, the U.S. government is authorized to target for surveillance "non-US persons," that is, not U.S. citizens or permanent residents, who are "reasonably believed to be located outside the United States," in order "to acquire foreign intelligence information."[96] Unlike traditional foreign intelligence surveillance, the U.S. government need only certify the believed identity and location of the target; it is not required to show probable cause that the person is a lone-wolf terrorist or an agent of a foreign power.[97] The NSA uses Section 702 to engage in two main types of electronic surveillance and bulk data collection. First, with PRISM collection, the government obtains content and metadata from Internet companies related to a "selector," such as an e-mail address.[98] The kind of information varies by provider and can include e-mails, videos, social networking details, and more. Second, with "upstream collection," the government compels the assistance of the providers that control the telecommunications backbone over which communications transmit. Through this device, the government intercepts communications directly, again based on a "selector."[99] Upstream collection, unlike PRISM, can include the content of telephone conversations. In addition to these and similar programs, information has recently surfaced that the NSA, independently or in cooperation with foreign services, mainly the United Kingdom Government Communications Headquarters, has engaged in surveillance of EU institutions, member state embassies, and foreign leaders.[100] One example is the much-discussed interception of Chancellor Merkel's telephone communications.

Civil society actors, journalists, human rights nongovernmental organizations, ordinary citizens, and others were outraged to learn of the scale and nature of the surveillance programs. In contrast, the reaction of European governments was mixed. On one hand, they repeatedly voiced their strong objections to the U.S. authorities, as in the case of the alleged wiretapping of Chancellor Merkel's telephone;[101] on the other hand, they failed to address head-on the leaked information that implicated European intelligence agencies.[102] Indeed, in contrast with the United States, which has openly admitted the existence of the NSA

95. *See generally* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014) [hereinafter REPORT ON SECTION 702 SURVEILLANCE], https://www.pclob.gov/library/702-Report.pdf.

96. 50 U.S.C. § 1881a(a) (2012).

97. BIGNAMI, THE US LEGAL SYSTEM, *supra* note 32, at 25.

98. *See* REPORT ON SECTION 702 SURVEILLANCE, *supra* note 95, at 7.

99. *Id.*

100. *See* Dieter Deiseroth, *Nachrichtendienstliche Überwachung durch US-Stellen in Deutschland – Rechtspolitischer Handlungsbedarf?,* 2013 ZEITSCHRIFT FÜR RECHTSPOLITIK 194; DIDIER BIGO ET AL., NATIONAL PROGRAMS FOR MASS SURVEILLANCE OF PERSONAL DATA IN EU MEMBER STATES AND THEIR COMPATIBILITY WITH EU LAW 7 (2013) [hereinafter NATIONAL PROGRAMS FOR MASS SURVEILLANCE], http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf.

101. *See generally* Sabine Leutheusser-Schnarrenberger, *Europäer sind nicht Bürger zweiter Klasse im Datenschutz,* 2013 MULTIMEDIA UND RECHT 481

102. NATIONAL PROGRAMS FOR MASS SURVEILLANCE, *supra* note 100, at 9–19.

programs and has confirmed their main features, the member states have so far failed to give detailed explanations of their surveillance programs and have maintained the classified status of most of the relevant documents.[103]

The Snowden leaks and the journalistic and parliamentary inquiries that have been conducted to date unequivocally demonstrate that several European intelligence agencies have actively participated in the implementation of the NSA programs and have themselves collected a vast amount of data and information subsequently made available, generally on the basis of reciprocity, to their foreign counterparts.[104] In particular, the United Kingdom has cooperated closely with the NSA, setting up an extremely powerful system of large-scale surveillance.[105] According to some allegations, it seems also that the GCHQ infiltrated the Belgian communication provider Belgacom to collect data on European institutions.[106] Such activities are not to be explained only on the basis of the long-lasting U.K.–U.S. relationship in the field of intelligence—a relationship that is also backed by a substantial financial contribution from the Unites States to GCHQ.[107] Instead, there is sufficient evidence that the agencies of other European countries, such as Germany, France, Sweden, and the Netherlands, have carried out similar mass-surveillance programs. Among such programs are the direct control of communications nodes known as "upstreaming," systematic access to private-sector data, and the use of decryption software.[108]

The scale and technological sophistication of these programs are probably not comparable to the U.S. surveillance programs. There is no doubt, however, that mass surveillance of communications has been carried out by European agencies, and that in most cases a vast amount of personal data—content data and metadata—has been made available to their U.S. counterparts.[109] From a European perspective, therefore, it is necessary to acknowledge that mass surveillance is by no means a solely U.S. issue. It also raises the question, again from a European viewpoint, of the legal basis and legitimacy of both the EU and U.S. surveillance operations, discussed next.

---

103. *Id.*; Stefan Heumann, *Die NSA in aller Munde—und was ist mit dem BND?*, CARTA (Mar. 3, 2011), http://www.carta.info/66295/die-nsa-in-aller-munde-und-was-ist-mit-dem-bnd/; Working Party, *Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes*, at 9 (Dec. 5, 2014) [hereinafter *Working Document*], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf.

104. For a detailed analysis, see NATIONAL PROGRAMS FOR MASS SURVEILLANCE, *supra* note 100, at Annex 1.

105. This program is code-named TEMPORA and consists of the routine interception of submarine cables, with the aim of gaining knowledge of the content of Internet communications. *See id.* at 51.

106. *Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm*, DER SPIEGEL (Sept. 20, 2013), http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

107. Nick Hopkins & Julian Borger, *Exclusive: NSA Pays £100m in Secret Funding for GCHQ*, THE GUARDIAN, (Aug. 1, 2013), http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden; *See* NATIONAL PROGRAMS FOR MASS SURVEILLANCE, *supra* note 100, at 54–55.

108. *Id.* at 19–26.

109. *Working Document*, *supra* note 103, at 9.

B. The Lawfulness of U.S. Surveillance

The Section 702 program has attracted significant criticism in Europe. As discussed earlier in the analysis of PNR and TFTP II, there are several different types of privacy guarantees generally believed to be important under European law: transparency, individual access and correction, accuracy, security, oversight, and proportionality. As in the earlier transatlantic privacy disputes, the European reaction has been partly driven by the argument that these standards have not been met. It is obviously impossible and undesirable to ensure complete transparency, individual access and correction, and oversight in the area of intelligence gathering, but the degree of freedom afforded to surveillance actors under the Section 702 program has been a source of puzzlement.

Consider first the European constitutional requirement of a basis in law for any infringement of the right to personal data protection. Although the current version of the Section 702 program is conducted, unlike earlier versions, pursuant to a congressional law that sets down different substantive and procedural criteria, the type of personal information that may be gathered—foreign intelligence information involving non-U.S. persons located outside of the United States is not clearly defined.[110] As noted in the report of the EU Data Protection Working Party, "foreign intelligence could, on the face of the provision, include information concerning the political activities of individuals or groups, or activities of government agencies, where such activity could be of interest to the United States for its foreign policy."[111] It could also include activities relevant to U.S. economic interests.[112] The U.S. government, questioned on the exact scope of the notion, refused to give a detailed answer on the grounds that this would compromise the efficacy of intelligence activities.[113] Moreover, FISA contains no limitation on the geographical reach of the surveillance, and it therefore could, in principle, cover not only the operations of service providers in the United States, but also data stored in the cloud and data processed by subsidiaries of U.S. companies located in the EU.

Turning to the safeguards afforded by judicial oversight, at first blush they appear substantial when compared with Europe's corresponding judicial safeguards. In many European systems, oversight is conducted by special parliamentary committees or executive bodies, and does not contemplate a role for the courts. By contrast, under FISA, a special court comprised of ordinary

110. For a detailed analysis of the history and content of Section 702, see LIBERTY AND SECURITY, *supra* note 29, at 130.

111. *Report on the Findings by the EU Co-Chairs of the Ad Hoc EU–US Working Group on Data Protection*, at 4 (Nov. 27, 2013) [hereinafter *Report*], http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

112. The President, however, has stated that the collection of foreign commercial information is not authorized for purposes of affording a commercial advantage to U.S. companies. Office of the Press Sec'y, *Presidential Policy Directive—Signals Intelligence Activities*, § 1(c), WHITE HOUSE (Jan. 17, 2014) [hereinafter *PPD-28*], http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

113. *Id.*

judges (the FISA Court) supervises intelligence surveillance. In the context of Section 702, however, the powers of the FISA Court are relatively limited: it only approves the type of foreign intelligence information being collected, the targeting procedures used by the NSA to conclude that surveillance will lead to the acquisition of foreign intelligence information on a non-U.S. person outside of the United States, and the minimization procedures used to prevent the collection and use of information on U.S. persons.[114] In contrast with traditional FISA surveillance, the FISA Court does not review applications for the surveillance of specific individuals.[115] Furthermore, the FISA Court's orders are classified and companies that are required to cooperate with the NSA, under the authority of the orders, are bound to secrecy. As a result, there is no way for data subjects to be informed that their personal data are being collected or processed.[116] Relatedly, individuals have no right to obtain access, rectification, or erasure of data, and the prospect of administrative or judicial redress is virtually nonexistent. The difficulty of obtaining a judicial remedy, absent a criminal prosecution based on unlawfully acquired evidence, was confirmed in *Clapper v. Amnesty International USA*.[117] In that case, the Supreme Court found that the petitioners—human rights lawyers and others who communicated with clients abroad—did not have standing because the claim that their telephone communications were likely to be intercepted was "too speculative."[118]

NSA surveillance has also raised proportionality issues familiar from the previous rounds of transatlantic conflict. One feature of the surveillance programs that has attracted much attention is the lack of protection for metadata.[119] In the context of the Section 215 call records program, the U.S. government has confirmed that the NSA collects call metadata from all major telecommunications companies and maintains a database of all such calls for five years.[120] This is done irrespective of the safeguards formally set forth by the Fourth Amendment—judicial warrant and probable cause—but consistent with the interpretation given by the Supreme Court in the 1970s, according to which there is no "reasonable expectation of privacy" for personal data entrusted to a third party.[121] As explained at the beginning of this article, the EU takes the opposite approach: metadata is considered "personal data" and therefore must be collected and processed according to the general principles of data-protection law. [122] Another anomaly

114. REPORT ON SECTION 702 SURVEILLANCE, *supra* note 95, at 26–27.

115. *See* L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits,* 66 VAND. L. REV. 1343, 1399 (2013).

116. *See Report*, *supra* note 111, at 16; Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability,* 51 STAN. J. INT'L L. 69, 82–84 (2015).

117. 133 S. Ct. 1138 (2013).

118. *See* Neil M. Richards, *The Dangers of Surveillance,* 126 HARV. L. REV. 1934, 1935 (2013).

119. *See generally* Bryce Clayton Newell, *The Massive Metadata Machine: Liberty, Power and Secret Mass Surveillance in the U.S. and Europe,* 9 J. L. & POL'Y FOR INFO. SOC'Y 481 (2014).

120. *See Report*, *supra* note 111, at 11; REPORT ON TELEPHONE RECORDS PROGRAM, *supra* note 94, at 25; Kris, *supra*, note 94, at 221. The program was amended by Congress in June 2015, but the retention period was not modified.

121. *See European versus American Liberty*, *supra* note 34, at 624.

122. *See* Malone v. U.K., 7 Eur. Ct. H.R. 14 (1984); *see also* Case C-293/12, Digital Rights Ireland Ltd. v.

with respect to European law is how privacy principles are applied to bulk collection. The U.S. intelligence community takes the position that the acquisition of personal data does not amount, in and of itself, to "processing"; data are processed only at the moment when they are analyzed by a human being.[123] In other words, the default position in U.S. national security law is that privacy concerns arise only when the information is accessed by a human being. This view stands in contrast with European law, under which the right to personal data-protection is triggered at the moment of collection, and facilitates more extensive bulk collection than is contemplated under European law.

In addition to these well-known transatlantic differences, the Snowden leaks have introduced a new bone of contention in transatlantic privacy relations—the dramatic difference in U.S. law between the treatment of citizens and non-citizens. Even more than PNR and TFTP, the NSA programs have brought into sharp focus the two-track scheme that runs throughout U.S. privacy law and that results in relatively few guarantees for EU citizens.[124] This is particularly apparent under Section 702.[125] The surveillance authorized under Section 702 is directed at foreign citizens who are not legal residents and who are believed to be located outside the United States.[126] A corollary of this basic mission is that most of the limitations contained in Section 702 seek to protect U.S. persons from being swept up in foreign intelligence surveillance.[127] The targeting and minimization procedures subject to the approval of the FISA Court are aimed at protecting the privacy of U.S. persons, not foreign citizens. This two-track scheme also marks U.S. constitutional law. All government surveillance must respect the privacy guarantees contained in the Fourth Amendment, but the Supreme Court has held that the Fourth Amendment does not apply to nonresident aliens located abroad.[128] In other words, most of the EU citizens implicated by NSA surveillance

Minister for Communc's, Marine and Natural Res., 2014 E.C.R (2014).

123. *See Report*, *supra* note 111, at 9.

124. *See generally* BIGNAMI, THE US LEGAL SYSTEM, *supra* note 32, at 36.

125. S*ee* Konrad Lachmayer & Normann Witzleb, *The Challenge to Privacy From Ever-Increasing State Surveillance: A Comparative Perspective,* 37 U.N.S.W. L.J. 748, 764 (2014); LIBERTY AND SECURITY, *supra* note 29.

126. *See* LIBERTY AND SECURITY, *supra* note 29, at 135.

127. *See* Christopher Kuner, *Foreign Nationals and Privacy Protection: A Comparative Transatlantic Analysis*, *in* DATA PROTECTION ANNO 2014: HOW TO RESTORE TRUST?: CONTRIBUTIONS IN HONOUR OF PETER HUSTINX, EUROPEAN DATA PROTECTION SUPERVISOR (2004–2014) 213 (Hielke Hijmans & Herke Kranenborg eds., 2014).

128. According to the U.S. Supreme Court decision in United States v. Verdugo-Urquidez, 494 U.S. 259, 265–68 (1990), the Fourth Amendment does not guarantee rights for non-U.S. persons outside the United States. Rather, the Fourth Amendment protects the rights of "the people," that is, "a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community." Applying this model, several scholars have argued that the Fourth Amendment is not implicated by the mass-surveillance of foreign communications carried out by the NSA. *See* John Yoo, *The Legality of National Security Agency's Bulk Data Surveillance Programs*, 37 HARV. J. L. & PUB. POL'Y 901, 919 (2014); Judith Rauhofer & Caspar Bowden, *Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud* 23–25 (Univ. of Edinburgh Sch. of Law, Research Paper Series No. 2013/28), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2283175 (referencing the personal data of foreigners stored by U.S. based cloud computing providers).

have no privacy rights under the U.S. Constitution.

To be fair, many, if not most, countries operate with surveillance laws that afford heightened privacy protections to their own citizens. For example, German law authorizes its intelligence services to carry out surveillance only on telecommunications connections that are not regularly used by German citizens, thereby treating non-Germans less favorably.[129] What is more exceptional is the denial of any human rights protection for foreigners. Many constitutions and international treaties—including Article 17 of the International Covenant on Civil and Political Rights (ICCPR), to which the United States is party—protect privacy as a human right vested in all persons.[130] Thus the constitutional jurisprudence of countries like Germany does not draw a categorical difference between the rights afforded to citizens and foreigners. A number of European commentators have argued that because the United States permits the virtually unrestricted surveillance of the communications of foreigners located outside of its territory, it violates its human rights obligations under the ICCPR.[131]

The extraterritorial application of human rights treaties is a controversial issue and it is not easy to predict how it will be resolved in the field of mass surveillance.[132] On this scope issue, however, as on the substance of privacy rights, there are significant differences between the United States and Europe. The United States has traditionally argued that under the ICCPR states are only responsible for human rights violations on their own territory, not extraterritorially.[133] By contrast, the European approach is somewhat more flexible. The European Convention of Human Rights, which is framed in different terms than the ICCPR, has been applied by the ECtHR and the Commission of Human Rights in cases of extraterritorial violations of human rights.[134] To avoid irrational or unfeasible results, the ECtHR has limited the obligation of the member states to respect the rights guaranteed by the Convention to two main situations: First, the spatial model, which is the de facto effective control over an area;[135] and second, the personal jurisdiction model, or the exercise of authority and control over an

129. Kuner, *supra* note 127, at 13.

130. *See* G.A. Res. 68/167 (Jan. 21, 2014); High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Rep. of the Office of the U.N. High Commissioner for Human Rights*, at 6, U.N. Doc. A/HRC/27/37 (June 30, 2014).

131. *See* Wolfgang Ewer & Tobias Thienel, *Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals,* 2014 NJW 30, 32; Markus Kotzur, *Datenschutz als Menschenrecht?*, 2013 ZEITSCHRIFT FÜR RECHTSPOLITIK 216, 218; see also Ilina Georgieva, *The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR,* 31 *Utrecht J. Int'l & Europ. L.* 104, 124 (2015).

132. On the general issue of extraterritorial application of human rights treaties, see MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES AND POLICY 7–9 (2011).

133. Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT. L.J. 81, 102–08 (2015); *see also* Beth Van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change*, 90 INT'L L. STUD. 20, 22–34 (2014).

134. *See generally* Milanovic, *supra* note 133; THEORY AND PRACTICE OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS § 1.4.3.M (Pieter Van Dijk et al. eds., 2006).

135. Loizidou v. Turkey, App. No. 15318/89, 310 Eur. Ct. H.R. (ser. A) (1995).

individual.[136] If such jurisdictional criteria are satisfied, then a state in question may be answerable even for extraterritorial violations.

The ECtHR's approach to extraterritoriality has been developed mainly regarding cases concerning the infringement of the right to life, liberty, and personal integrity.[137] Applying it to interferences with privacy is a difficult task, largely because such interferences are typically incorporeal and do not require the exercise of physical powers over the person. To gain traction over the issue, it is useful to distinguish, following a suggestion by Marko Milanovic, among three different factual scenarios: (1) The surveillance is carried out on the state's own territory and the target is located inside the national borders; (2) the surveillance is carried out, or the resulting data are processed, on the state's own territory but the target is located abroad;[138] and (3) the person is located abroad and the interference with privacy takes place outside the state's own territory. Under the ECtHR's spatial model of jurisdiction, one could argue that both the first and second scenarios justify the application of the Convention.[139]

The third situation is more problematic because it is not covered by the spatial model, and even under the personal model, it is not clear whether the interception of communications or the bulk collection of metadata would qualify as an exercise of "authority or control" over an individual. Milanovic has recently argued that the right to privacy under the ECHR should be applied extraterritorially in this third situation as well, noting that it would be irrational to treat differently factual situations that involve the same set of substantive problems.[140] The interferences with privacy under the Section 702 program, however, do not appear to trigger this more complex scenario but rather seem to fall under the second scenario, given that both PRISM collection and upstream collection take place on U.S. territory.[141] One could argue, therefore, that if personal data of European citizens are collected and processed by the NSA without complying with the procedural and substantive requirements of Article 17 of the ICCPR, the overall situation would be highly asymmetrical: American citizens would be protected by Article 8 of the European Convention of Human Rights (with respect to surveillance carried out by European intelligence and police authorities), whereas Europeans would not enjoy similar guarantees vis-à-vis surveillance by U.S. authorities.

In addition to the discriminatory application of privacy rights, another novel

136. Al-Skeini v. United Kingdom, App. No. 55721/07, 53 Eur. Ct. H.R. 18, para. 137 (2011). The Court stated:

> It is clear that, whenever the State through its agents exercises control and authority over an individual, and thus jurisdiction, the State is under an obligation under Article 1 to secure to that individual the rights and freedoms under Section 1 of the Convention that are relevant to the situation of that individual. In this sense, therefore, the Convention rights can be 'divided and tailored.'

Id.

137. *See generally* Milanovic, *supra* note 133, at 37–48.

138. For a similar case, see Weber v. Germany, App. No. 54934/00, 2006-XI Eur. Ct. H.R. 1173 (2006).

139. *See* Milanovic, *supra* note 133, at 60.

140. *Id.* at 60–61.

141. *See generally* BOWDEN, *supra* note 93, at 13–24.

element of the current transatlantic dispute involves the methods that have been used by the NSA to gather intelligence on Europeans. The first part of this article described two official channels through which the U.S. government can obtain personal data on Europeans—pursuant to the PNR agreement and to the TFTP II agreement. There also exists the Mutual Legal Assistance Agreement between the EU and United States, which makes it possible, under certain conditions, to gather and exchange data for the prevention and investigation of criminal activities, including international terrorism.[142] In the eyes of some European commentators, the U.S. authorities have deliberately circumvented these official channels by collecting data directly from private service providers, an action they claim might even amount to a violation of international law.

C. The Lawfulness of European Surveillance

As mentioned above, according to initial reports, it appears that some of the largest European intelligence agencies, including those of England, France, and Germany, have actively cooperated with the NSA and have collected and probably exchanged large amounts of personal data on European citizens, including many who have never been the object of a counterterrorism or criminal investigation.[143] This has revealed the rift, discussed earlier in the context of PNR and TFTP II, between different European actors. Although data-protection authorities and certain liberal political parties have championed privacy rights,[144] they have always met with powerful resistance from the forces of law and order, and in particular, the national security establishment. The allegations of mass data collection and processing by European intelligence services also raise the question of whether a gap exists between the law on the books and the actual operation of state activities: Have the principles of European data-protection law been violated? Various complaints have already been lodged both before national and supranational courts,[145] but even at this early stage it is possible to clarify some general points.

At the outset, it should be noted that the legal framework governing the various intelligence programs is highly fragmented. As a policy area, national security falls outside the competences of the EU and is reserved for the member states.[146] The

142. *See Letter from EU Vice-President Viviane Reding to U.S. Attorney General Eric Holder*, at 2 (June 10, 2013), http://edri.org/files/holder.pdf.

143. For a detailed overview, see generally NATIONAL PROGRAMS FOR MASS SURVEILLANCE*, supra* note 100.

144. *See, e.g.*, *Working Document*, *supra* note 103; Article 29 Working Party, *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes* (Apr. 10 2014) [hereinafter *Opinion 04*], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.

145. The ECtHR has affirmed the admissibility of the case Big Brother Watch v. U.K., App. No. 58170/13 (2013); *see also* Liberty v. Secretary of State for the Foreign and Commonwealth Office, UKIPTrib 13_77-H (2015) (declaring the regime that governs the sharing between Britain and the United States of electronic communications intercepted in bulk was unlawful for breach of Art. 8 ECtHR prior to the disclosures made during the court proceedings). Also particularly relevant is the recent decision of the CJEU, Grand Chamber, is Case 362/14, Schrems v. Data Protection Commissioner (2015), discussed below.

146. Treaty on European Union Art. 4(2), Oct. 26, 2012, 2012 O.J. (C 326); *see also Opinion 04*, *supra* note 144, at 6–7.

laws regulating the powers, internal organization, and responsibilities of intelligence and security agencies, as well as oversight mechanisms, tend to vary significantly among different European countries.[147]

Notwithstanding this diversity, a number of general principles can be derived from the European constitutional framework and from the harmonized European law of data protection. Because the European Convention on Human Rights governs all the activities of European states, including national security surveillance, the jurisprudence of the ECtHR is the most clearly applicable body of law. As explained earlier, the right to privacy under Article 8 of the Convention is triggered whenever public or private bodies gather information that can be associated with a person. For processing to be lawful, there must be a basis in law, a clearly defined purpose set down in that law, and proportionality. The Court has adapted these general requirements to the specific context of surveillance by national intelligence services in what, by now, constitutes a fairly substantial line of jurisprudence.

First, in the 1978 case of *Klass and Others v. Germany*,[148] the Court held that any person whose communications are likely being monitored under a secret intelligence program, even if it cannot be shown that he or she was actually a victim of surveillance, has standing to sue.[149] In other words, an application is considered admissible even in the absence of concrete evidence of harm. As the Court observed in *Weber and Saravia v. Germany*:

> [T]he mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services, and thereby amounts to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.[150]

This relatively permissive test for obtaining standing contrasts with the United States Supreme Court's position, affirmed in *Clapper*, that the mere threat of surveillance does not establish standing.[151]

Once the Court finds that the surveillance in question amounts to an interference with the right to privacy under Article 8, it examines whether the interference is *provided for by the law* and is *necessary in a democratic society* to

147. *See* DIRECTORATE GEN. FOR INTERNAL POLICIES, PARLIAMENTARY OVERSIGHT OF SECURITY AND INTELLIGENCE AGENCIES IN THE EUROPEAN UNION (2011). A complete legal analysis, therefore, would require proceeding jurisdiction by jurisdiction, something which would exceed the scope of this article.

148. Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R. (1978).

149. *Id.* §§ 34–38 (laying down the principle according to which "an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him. The relevant conditions are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures").

150. Weber v. Germany, App. No. 54934/00, Eur. Ct. H.R. § 78 (2006) [hereinafter Weber Decision] (emphasis added).

151. 133 S. Ct. 1138 (2013).

achieve the aims mentioned in Article 8 (2) of the Convention.[152] Roughly speaking, "provided for by law" maps onto the legal basis and purpose requirements discussed in the first part of this article, whereas "necessary in a democratic society" tracks this article's proportionality analysis.

In the context of intelligence operations, the Court has repeatedly stated that the "law" authorizing secret surveillance programs must "be *accessible* to the person concerned, who must, moreover, be able to *foresee its consequences* for him, and *compatible with the rule of law*."[153] To understand the Court's jurisprudence, it is useful to reproduce in full the following passage on foreseeability, applicable both to the interception of individual communications and to mass electronic surveillance programs:

> [F]oreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly . . . [h]owever, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident . . . [i]t is therefore essential to have *clear, detailed rules* on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated . . . . *The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures . . . . [T]he law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference*. In its case-law on secret measures of surveillance, the Court has developed the following *minimum safeguards that should be set out* in statute law in order to avoid abuses of power: *the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed*.[154]

Applying this jurisprudence on the "law" required to authorize the interference with the privacy right, the ECtHR held against the United Kingdom in *Liberty v. The United Kingdom*.[155] The Strasbourg Court found that the 1985 Act authorizing the interception of communications passing between the United Kingdom and an external receiver violated Article 8 for the following three reasons: (1) There was no limit on the type of external communications that could be included in a warrant; (2) the Act allowed the State authorities broad discretion on the question of which communications, out of the total volume of those physically captured, would be read or listened to; and(3) the procedures to be followed in selecting specific communications for examination, sharing, storing, and destroying were not set out in a manner accessible to the public.[156] A similar conclusion was reached in the subsequent case of *Iordachi v. Moldova*.[157]

Moving to the second part of the inquiry—whether the interference is

152. Weber Decision, *supra* note 150, at § 80.
153. *Id.* at § 84.
154. *Id.* §§ 93–95 (emphasis added)
155. Liberty v. U.K., App. No. 58243/00, Eur. Ct. H.R. §§ 64–70 (2008).
156. *Id.* §§ 64–69.
157. Iordachi v. Moldova, App. No. 25198/02, Eur. Ct. H.R. (2009).

necessary in a democratic society—the Strasbourg Court has repeatedly affirmed that secret surveillance measures, although seriously interfering with the right to respect of private life, may be considered admissible insofar as they are aimed at protecting national security.[158] The member states, however, are not allowed unlimited discretion in designing such programs: "in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it," governments are required to put in place "adequate and effective guarantees against abuse."[159] With this requirement, the Court imposes a classic proportionality test, which must take into consideration "all the circumstances of the case, such as the nature, scope and duration of the possible measures; the grounds required for ordering them; the authorities competent to authorize, carry out and supervise them; and the kind of remedy provided by the national law."[160]

To illustrate the application of these principles, in the case of *Weber and Others v. Germany,* the ECtHR came to the conclusion that the German program that permitted the wiretapping of international telephone calls for purposes of counterterrorism, the so-called G-10 Act, as modified by the Fight against Crime Act of 28 October 1994,[161] satisfied both of Article 8's requirements of "law" and being "necessary in a democratic society." The law defined in a clear and precise manner the offenses that could give rise to an interception order, the duration of the interception, the categories of persons likely to be intercepted, the maximum duration of monitoring measures, the procedure to be followed for examining and using the data, and the circumstances in which recordings could be erased or tapes destroyed.[162]

An analysis of TEMPORA, one of the most intrusive and sophisticated of the national security programs revealed by Snowden, sheds light on how these principles might be applied to mass surveillance. There are two primary components to the program. First, it appears that the GCHQ has been allowed to access, in secret and without controls, the personal data pertaining to U.K. citizens gathered by the NSA under the Section 702 program.[163] If this is confirmed, then such an activity would amount to a circumvention of the Regulation of Investigatory Powers Act 2000, which requires the government to adopt specified safeguards when intercepting communications of individuals located in the United Kingdom. Without a detailed and accessible legal basis, and in the absence of any

158. Weber Decision, *supra* note 150, § 106; *see also* Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R. § 49 (1978).

159. Weber Decision, *supra* note 150, at § 106.

160. *Id.*

161. Act of 13 August 1968 on Restrictions on the Secrecy of Mail, Post and Telecommunications (*Gesetz_zur Beschränkung des_Brief-, Post- und_Fernmeldegeheimnisses*), as modified by the Fight against Crime Act of 28 October 1994 (*Verbrechensbekämpfungsgesetz*). *See* Matthias Bäcker, *Das G 10 und die Kompetenzordnung,* 2011 DÖV 840.

162. Weber Decision, *supra* note 150, at § 92.

163. NATIONAL PROGRAMS FOR MASS SURVEILLANCE, *supra* note 100, at 53, 55.

"adequate and effective guarantee against abuse,"[164] it is difficult to see how such an interference with private life could be considered legitimate by the Strasbourg Court. Second, it has been reported that the GCHQ has intercepted more than 200 fiber optic cables landing in the United Kingdom, storing and extracting data related to "external communications" of primarily non-U.K. citizens. The intercepted communications include both the content and metadata of telephone calls and internet traffic, such as e-mails, Facebook entries, and Google searches. Although authorized under certificated warrants issued pursuant to section 8(4) of the Regulation of Investigatory Powers Act 2000, this surveillance seems to be disproportionate insofar as the bulk interception of communications on a continuous and indiscriminate basis comprises blanket surveillance of thousands and possibly of millions of people.[165] Additionally, U.S. officials have allegedly been granted extensive access to this data, again in the absence of a clear and transparent legal basis.[166]

Will the European courts rule against the mass surveillance programs carried out by several national agencies, allegedly in collaboration with the NSA? Although it is hard to tell at the moment, some indications suggest that they might. In 2013, the ECtHR, following a preliminary examination of its admissibility, decided to give priority, under rule 41, to the application lodged by *Big Brother Watch and Others* (a coalition of nongovernmental organizations engaged with the protection of privacy and other civil liberties) against the United Kingdom.[167] The applicants have complained that the TEMPORA program, analyzed above, has no adequate basis in domestic law and is not proportionate under Article 8 of the Convention.[168]

The Court of Justice of the European Union has also recently taken a more categorical approach to privacy. Since the Snowden revelations, the Court has decided three important data-protection cases: *Digital Rights Ireland v. Minister of Communications Ireland and others*,[169] *Google Spain v. Agencia Española de Protección de Datos and Mario Costeja González*,[170] and *Schrems v. Data Protection Commissioner*.[171] All bear witness to the Court's hardening stance on the right to personal data protection.The judgments also demonstrate considerable attention

164. Weber Decision, *supra* note 150, at § 106.

165. TEMPORA was challenged before the United Kingdom Investigatory Powers Tribunal. The Tribunal held in favor of one of the claimants (an Egyptian nongovernmental organization), on the basis of a breach of Article 8 of the ECHR, in light of the exceedingly long time of retention of the intercepted data. *See* Liberty v. Secretary of State for the Foreign and Commonwealth Office, UKIPTrib 13_77-H (2015) As regards the other claimants, the Tribunal held that the sharing of information between the U.S. and Britain in the frame of the PRISM and TEMPORA programs was in breach of Art. 8 ECHR, because the domestic law was not sufficiently transparent and accessible to the public, prior to the disclosures made during the court proceedings. *Id.*

166. NATIONAL PROGRAMS FOR MASS SURVEILLANCE, *supra* note 100, at 55.

167. Big Brother Watch v. U.K., App. No. 58170/13, Eur. Ct. H.R. (2013).

168. The complaint is available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/bbw_org_ep_ck_v_uk_/bbw_org_ep_ck_v_uk_en.pdf.

169. Case C-293/12, Digital Rights Ireland Ltd. v. Minister for Communic's, Marine and Natural Res., 2014 E.C.R (2014).

170. Case-131/12 (2014) (not yet reported).

171. Case-362/14 (2015) (not yet reported).

to the extraterritorial dimension of the policy problem and the challenges of safeguarding the right in the face of market and government surveillance that occurs within other jurisidictions, particularly the United States. And lurking in the background, or in the case of *Schrems,* squarely on the face of the judgment, is the deeply troubling policy problem that has been brought to the fore by the Snowden revelations: How can privacy be protected in the face of unprecedented advances in digital technologies, the growing concentration of power and personal data in the hands of market actors, and the seemingly unlimited appetite for that data among law enforcement, national security, and other government actors?[172]

On April 8, 2014, in *Digital Rights Ireland v. Minister of Communications Ireland and others*, the CJEU found that Directive 2006/24/EC was invalid.[173] The so-called Data Retention Directive required electronic communication providers to collect and retain all traffic and location data of all their clients concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony for a period between six months and two years. These metadata were to be made available "for the purpose of the investigation, detection and prosecution of serious crime."[174] The CJEU found the Directive incompatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, which respectively enshrine the right to privacy and the right to personal data protection.

In *Digital Rights Ireland*, the CJEU reasoned that the interference with privacy was particularly serious because of the huge quantity and type of data involved, together with the fact that the data were retained and subsequently used without any knowledge of the data subject. In the view of the CJEU, the data-retention requirement was "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[175] In the judgment, the CJEU acknowledged that the objectives of the Directive were of the utmost importance, being related to the fight against organized crime and terrorism[176] but found that the interference with privacy was not proportionate to the legitimate aims being pursued. To reach this conclusion, the Court assigned particular relevance to the following elements: (1) The data retention program applied to all persons without limitations, and 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;" (2) the program covered all data, irrespective of any relationship between such data and a threat to public security; (3) the Directive set down no substantive and procedural conditions to regulate access to and use of the data by the competent national authorities; (4) such access was not made dependent "on a prior review carried

172. On the underlying social and technological context and its transformation, see Fred H. Cate et al., *Systematic Government Access to Private-Sector Data,* 2 INT'L DATA PRIVACY L. 195 (2012); Richards, *supra* note 118, at 1936–41.

173. Digital Rights Ireland Ltd., *supra* note 168.

174. *Id.* at § 16.

175. *Id.* at § 37.

176. *Id.* at § 51.

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;" and (5) the retention period was fixed in general terms, between six months and two years, without a distinction being made among the different types of data and without employing criteria designed to guarantee that the retention period be limited to what was strictly necessary in light of the aims pursued.[177]

The CJEU also pointed to another flaw in the Data Retention Directive: it did not prohibit the retention of the metadata outside of 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, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.[178]

The danger alluded to—transferring data to less privacy-protective jurisdictions—could be very well be interpreted as a specific reference to NSA surveillance.

Only one month after *Digital Rights Ireland*, the CJEU handed down its judgment in *Google Spain*. There the CJEU found Google liable for violating the so-called right-to-be-forgotten in the EU Data Protection Directive.[179] That right is linked to the right of individual access and correction, discussed earlier in this article, and requires that firms like Google expunge from their computer systems personal information that fails to comply with data-protection standards such as accuracy and proportionality. In a critical part of the judgment, the Court found in favor of broad territorial application of the EU Directive to ensure that European data-protection rights could not be circumvented by processing personal data outside the EU.[180] Even though Google argued that the EU Directive was not applicable because all the data processing connected with its search engine occurred in the the United States, the CJEU found that a corporate presence in the EU for purposes of selling advertising space was enough to bring Google within the territorial scope of the Directive.

The last in this trilogy of data-protection cases is *Schrems v. Data Protection Commissioner*. In the wake of the NSA scandal, an Austrian citizen and subscriber of Facebook, Maximilian Schrems, lodged a complaint before the Irish Data Protection Commissioner. He claimed that Facebook Ireland systematically transferred the data of its European customers to Facebook USA's servers in the United States, where they were stored. Facebook was a participant in the Safe Harbor program and therefore, as explained earlier in this article, was entitled to a finding of adequacy for purposes of satisfying the requirements of the EU Data Protection Directive on data transfers to third countries. Schrems, however, relied on the Snowden revelations of Facebook's involvement in the PRISM program (which allows the NSA access to the data of EU citizens held by Internet

177. *Id.* at §§ 51–68.

178. *Id.* at § 68.

179. Case-131/12, Google Spain SL v. Agencia Española de Protección de Datos (2014) (not yet reported).

180. *Id.* § 54.

companies) to argue that the transfers violated the substantive and procedural guarantees of the Directive and the European Charter of Fundamental Rights (Articles 7 and 8). When the Data Protection Commissioner refused to take action, Schrems challenged the Commissioner's decision in Irish court, which in turn referred the issue to the CJEU.

The CJEU held in favor of Schrems, against Safe Harbor. Although the judgment touches on a number of issues, the most important one for purposes of this article is the question of whether adherence to the Safe Harbor principles guarantees the adequacy of data protection for European data transferred to the United States. The Court's answer was a resounding "No." The Court faulted the Safe Harbor agreement and the accompanying Commission decision on adequacy for including a broad exception for U.S. government access to personal data based on "national security, public interest, or law enforcement requirements" or based on "statute, government regulation, or case-law."[181] In assessing adequacy, the Commission had focused exclusively on the private sector and had failed to assess whether the legal standards applicable to government actors were comparable to those under EU data-protection law.[182]

After pointing out these flaws in the Commission's decision, the Court set down the criteria that would have to be satisfied for the United States to be considered an adequate jurisdiction. These criteria are grounded on the legal basis and purpose, as well as proportionality, requirements that have been central to this area of constitutional law since the early 1970s and that have already been discussed in the context of the German Constitutional Court and the ECtHR. The Court found that indiscriminate access to electronic data, in particular the content of communications, would violate the essence of the right to privacy. Any law serving as the basis for a interference with the right to privacy would have to include "objective criterion . . . to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference."[183] In addition, the right of access, correction, and in some cases, erasure, would have to be enforceable through the courts.[184] Since the Commission made no such findings, the Court held that the Safe Harbor adequacy determination was invalid.

IV
CONCLUSION

The revelations of NSA surveillance are but the last, albeit perhaps the most dramatic, episode in transatlantic privacy regulation. Whatever one might think of the NSA programs, they have undoubtedly had repercussions for privacy and transatlantic relations more broadly speaking. In July 2013, the European Parliament passed a Resolution calling for an official investigation into the NSA

181. *Id.* §§ 84–87
182. *Id.* §§ 88–90.
183. *Id.* § 93.
184. *Id.* § 95.

programs and instructed its Parliamentary Committee on Civil Liberties, Justice, and Home Affairs to conduct an in-depth inquiry into the matter.[185] After six months of intense activity, on January 8, 2014, the Rapporteur Claude Moraes published a Draft Report that called for a Parliament Resolution condemning the programs of indiscriminate surveillance of citizens and proposing a complex package of reforms aimed at improving privacy safeguards.[186] The Report, approved by the European Parliament on March 12, 2014, demonstrates the climate of distrust created by the NSA programs. This climate has compromised some of the arduous efforts of the past decades to overcome regulatory differences and create a harmonized privacy scheme to facilitate transatlantic trade and to improve cooperation on security and law enforcement. The Parliament Report called for immediate suspension of Safe Harbor and, as discussed above, a year later, the Court of Justice invalidated the Commission decision granting "adequate" data-protection status to those U.S. firms that subscribe to the Safe Harbor principles. Even earlier, in October 2013, the Parliament passed a resolution advocating suspension of TFTP II.

There have also been consequences for transatlantic trade relations more broadly speaking. The 2014 Parliament Report called for the suspension of the negotiations for a Transatlantic Trade and Investment Partnership Agreement until the conclusion of negotiations on a transatlantic "Umbrella Agreement" setting down data-protection guarantees for personal information exchanged for law enforcement purposes.[187] Although Transatlantic Trade and Investment Partnership Agreement negotiations have gone forward, there is currently a significant push to also conclude the Umbrella Agreement, without which it is unlikely that the European Parliament will ratify any trade deal at all. One of the biggest hurdles to finalizing and ratifying the Umbrella Agreement is the double standard for U.S. citizens and EU citizens in U.S. law, a double standard that has been particularly evident in the operation of the Section 702 program.

It would be misleading to portray the European reaction to the Snowden leaks as unequivocally hostile. The member states and their governments, individually and through the Council of Ministers, have been fairly silent. Moreover, there have been numerous attempts by interior ministers and their supporters to enhance EU-wide surveillance in the interest of fighting the threat of extremism and terrorism. For instance, the President of the European Council, Donald Tusk, has recently urged the European Parliament to pass a longstanding proposal for an EU

185. Resolution of 4 July 2013 on the US National Security Agency Surveillance Program, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Privacy, 2013/2682 (RSP) (2013), http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2013-0322&language=EN.

186. All the relevant documents are collected in LIBE COMMITTEE INQUIRY, ELECTRONIC MASS SURVEILLANCE OF EU CITIZENS: PROTECTING FUNDAMENTAL RIGHTS IN A DIGITAL AGE (2013–2014), http://www.europarl.europa.eu/document/activities/cont/201410/20141016ATT91322/20141016ATT91322EN.pdf.

187. *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* (Jan. 8, 2014), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-526.085+02+DOC+PDF+V0//EN&language=EN.

PNR that would mimic the system in place in the United States.[188] What can be said, however, is that the vigorous transatlantic debate on privacy can contribute to protecting both sides from complacency. There is no doubt that personal data processing can produce, both in the market and the surveillance contexts, significant benefits. There is also no question that robust privacy guarantees are necessary and the transatlantic debate has had a positive impact on privacy. As with many policy issues, the debate on privacy is somewhat lopsided and the regulatory actors most directly impacted can sometimes use the ebb and flow of public attention to avoid institutional reform.[189] As public outrage over the Snowden affair fades and government and corporate actors seek to strategically delay—and perhaps avoid—legal change, the existence of a symbolic set of fundamental rights and a vocal set of watchdogs in Europe can help sustain attention to the policy problem and keep privacy reform on the public agenda.

188. Donald Tusk, President of the European Council, Address to the European Parliament, Strasbourg (Jan. 13, 2015).

189. For the theory of how salience cycles can be used strategically by institutional actors to delay or prevent change, see GIOVANNI CAPOCCIA, WHEN DO INSTITUTIONS BITE? HISTORICAL INSTITUTIONALISM AND THE POLITICS OF INSTITUTIONAL CHANGE (2012) (unpublished typescript) (on file with the University of Oxford).