SURVEILLANCE AND DIGITAL PRIVACY IN THE TRANSATLANTIC "WAR ON TERROR": THE CASE FOR A GLOBAL PRIVACY REGIME

Valsamis Mitsilegas*

ABSTRACT

This Article examines the impact of the "War on Terror" on the right to privacy by focusing on generalized mass surveillance. It begins by analyzing and comparing the extent and limits of privacy protection in the United States and the European Union and argues that European Union law provides a higher level of constitutional protection of privacy than U.S. law. The Article continues by providing a detailed analysis of the transformation of privacy in the evolution of transatlantic counterterrorism cooperation, examining the challenges that such cooperation poses on the right to privacy in the European Union, providing a typology, and critically evaluating the various transatlantic forms of governance developed to address European privacy concerns. The final part of the Article argues that, in light of the increasingly globalized nature of mass surveillance and the challenges that extraterritorial surveillance pose on human rights and the rule of law, states should work toward the establishment of a global privacy regime. The Article argues that European Union law can provide key benchmarks in this context and goes on to identify four key principles that should underpin the evolution of a global privacy regime.

---

* Professor of European Criminal Law, Director of the Criminal Justice Centre and Head of the Department of Law, Queen Mary University of London. I would like to thank the participants in the Human Rights and the "Forever War" symposium held at Columbia University on December 4, 2015, for their comments on an earlier draft, the editorial board of the *Columbia Human Rights Law Review*, and in particular Brian Yin and Sarah Sloan for their editorial leadership and Niovi Vavoula for her outstanding research assistance in the preparation of this article. Any errors remain my own.

I. INTRODUCTION

One of the key aspects of the "War on Terror" has been the intensification of surveillance. Aided by advances in technology and a growing trend toward the privatization of policing and security, we have now reached a paradigm of surveillance that is both quantitatively (in terms of the volume of personal data accessed by the state) and qualitatively (in terms of how and why such data is processed and analyzed) different from traditional policing models that focus on the detection of criminality. Moreover, this new surveillance paradigm is now globalized. United States security demands transcend borders and have generated mimetic efforts in other parts of the world.

This new paradigm of globalized surveillance poses fundamental challenges to the right to privacy and related rights, in particular the rights to freedom of expression and association. The aim of this Article is to highlight the key aspects of this new surveillance regime and the challenges it poses to the right to privacy. The Article will do so by focusing on the evolution of U.S. surveillance requirements after 9/11 and their subsequent accommodation (or lack thereof) by the European Union. Specifically, Section II of the Article compares the evolution of mass surveillance in the United States with that in the EU, Section III compares the U.S. and European Union constitutional frameworks on the protection of privacy, Section IV analyzes privacy challenges arising from the establishment of avenues for transatlantic counterterrorism cooperation involving mass surveillance, Section V critically evaluates the ways in which these transatlantic initiatives attempt to address privacy concerns within a law enforcement framework, and Section VI examines key ways in which specific privacy initiatives can address human rights shortcomings of mass surveillance. In this context, the Article focuses on three main privacy avenues: (1) the establishment of a level playing field of bilateral privacy between the United States and the EU; (2) the role of extraterritoriality in protecting privacy; and (3) the possibility of the globalization of privacy standards. This Article also explores the case for the establishment of a global privacy regime, which could meaningfully address the human rights challenges of globalized mass surveillance. Finally, the Article presents four key principles to underpin this global regime.

II. THE TRANSFORMATION OF SURVEILLANCE AND PRIVACY IN THE "WAR ON TERROR" IN THE UNITED STATES AND EUROPE

A key transformation of surveillance after 9/11 involves the emphasis on the future. Rather than focusing on the detection of past acts, law enforcement and security efforts are now geared toward the prevention of future terrorist attacks. This move toward preemptive surveillance[1] has also been combined with a shift toward mass, generalized surveillance of everyday activities. This section sketches out in greater detail the main elements of the new paradigm of surveillance in the "War on Terror" and highlight the challenges it poses for privacy. It thens provides a detailed analysis of the evolution of this new paradigm of surveillance in the United States and the EU. The analysis highlights the challenges of this model to the right to privacy and subsequent legislative, policy, and judicial responses to these challenges.

A. The Transformation of Surveillance in the War on Terror: Looking to the Future, the Surveillance of Everybody, and the Everyday

The reconfiguration of the security landscape in recent years has transformed the relationship between the individual and the state. A catalyst toward this transformation has been the growing link between securitization and preemptive surveillance, as well as the focus of security governance on risk assessment.[2] The preemptive turn in surveillance has been based largely upon the collection, processing, and exchange of personal data, which has in turn been marked by four key characteristics.[3] The first characteristic involves the *nature* of the data in question. Preemptive surveillance focuses increasingly on the collection of personal data generated by ordinary, everyday activities. Key examples include the collection, processing, and transfer of personal data on financial transactions, airline travel, and mobile phone communications. The second characteristic involves the addition

---

1. *See generally* Valsamis Mitsilegas, *The Transformation of Privacy in an Era of Pre-Emptive Surveillance*, 20 TILBURG L. REV. 35 (2015) (discussing the main elements of the system of preemptive surveillance and its effects on the right to privacy).

2. *See* RISK AND THE WAR ON TERROR (Louise Amoore & Marieke de Goede eds., 2008).

3. *See also* Mitsilegas, *The Transformation of Privacy in an Era of Pre-Emptive Surveillance*, *supra* note 1.

of new *actors* of surveillance, with the state increasingly co-opting the private sector in surveillance practices.[4] The third characteristic of preemptive surveillance involves the *scale* of data collection, processing, and transfer, with the focus on monitoring everyday life resulting in generalized and mass surveillance marked by the bulk collection and storage of personal data. The fourth characteristic of preemptive surveillance involves the *purpose* of data collection and processing. Data collection after 9/11 focuses not on data related to the commission of specific, identified criminal offenses, but rather on the use of personal data to predict risk and preempt future activity. This has led to what has been called "the 'disappearance of disappearance'—a process whereby it is increasingly difficult for individuals to maintain their anonymity, or to escape the monitoring of social institutions."[5] State authorities thus have access to a wealth of personal data, enabling practices such as profiling and data mining. The impact of state intervention on the individual is intensified when one considers the potential of combining personal data from different databases, collected for different purposes in order to create a profile of risk or dangerousness. This use of personal data leads to a process whereby individuals embarking on perfectly legitimate everyday activities are constantly being assessed and viewed as potentially dangerous without knowing about or contesting such assessment.[6]

This move toward preemptive surveillance poses fundamental challenges for the rights to private life and data protection, and from a broader perspective, impacts the presumption of innocence and concepts of citizenship and trust between the individual and the state. The monitoring en masse of everyday legitimate activities may create a chilling effect on freedom of expression and association. These challenges become more acute in the light of technological advances and the move toward a world of "big data." Big data has been defined as the reliance on data analytics that can process massive quantities

---

4. This privatization of surveillance constitutes another example of the responsibilization strategy, whereby the private sector is co-opted by the state in the fight against crime. For more on the responsibilization strategy, see David Garland, *The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society*, 36 BRIT. J. CRIMINOLOGY 445, 452–55 (1996).

5. Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOC. 605, 619 (2000).

6. Valsamis Mitsilegas, *The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance*, 8 INT'L POL. SOC. 104, 105 (2014).

of data in the search for information, including unforeseen information, which can potentially generate unexpected insights.[7] It is characterized by two basic features: the possibility of accessing and using large quantities of data; and the use of data processing techniques that allow for the recognition of previously unidentified patterns, which might have a predictive quality.[8] A key feature in the brave new world of big data is an emphasis on what Professor of Sociology David Lyon has characterized a "collect-it-all" mentality, the key idea being that new things can be learned from a very large body of data that cannot be learned from less.[9] As Lyon notes, the use of networked technologies that pick up traces from devices and aggregate fragmented data permits surveillance of more mobile populations.[10] The emphasis on "collect-it-all" includes not only data relating to the content of communications or personal records, but also to metadata, which reveals not content, but, in the case of mobile phone communications, the locations of the communicants.[11] By focusing primarily on the collection of mobile phone communications data, the following subsections examine the challenges for privacy posed by this model of mass surveillance on both sides of the Atlantic.

B. Mass Surveillance in the United States: The NSA Scandal and Beyond

U.S. law now allows for the collection of bulk telephone records directly by the National Security Agency ("NSA") under the telephone records program, which the NSA operates under § 215 of the USA PATRIOT Act (legislation enacted after 9/11).[12] The program is operated under an order issued by the Foreign Intelligence Surveillance Act ("FISA") court—an order that is renewed approximately every ninety days.[13]

---

7. GLORIA GONZÁLEZ FUSTER & AMANDINE SCHERRER, BIG DATA AND SMART DEVICES AND THEIR IMPACT ON PRIVACY 10–11 (2015).

8. *Id.*

9. DAVID LYON, SURVEILLANCE AFTER SNOWDEN 68 (2015).

10. *Id.* at 70.

11. On the uses of metadata, see *id.* at 68–75.

12. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered titles of the U.S.C.).

13. Foreign Intelligence Surveillance Act of 1978 § 103, Pub. L. No. 95-511, 92 Stat. 1788 (1978) (codified in scattered titles of the U.S.C.).

Before this legal authorization, though, President Bush had authorized the collection of such data for counterterrorism purposes without judicial warrants or court orders.[14] According to the U.S. Privacy and Civil Liberties Oversight Board, in October 2001, President Bush authorized the NSA to collect the contents of certain international communications under the Terrorist Surveillance Program ("TSP"), and collect in bulk non-content information, or "metadata," about telephone and Internet communications.[15] According to the Privacy Board:

> The President renewed the authorization for the NSA's activities in early November 2001. Thereafter, the authorization was renewed continuously, with some modifications in the scope of the authorized collection, approximately every thirty to sixty days until 2007. Each presidential authorization included the finding that an extraordinary emergency continued to exist justifying ongoing warrantless surveillance. Key members of Congress and the presiding judge of the Foreign Intelligence Surveillance Court were briefed on the existence of the program. The collection of communications content and bulk metadata under these presidential authorizations became known as the President's Surveillance Program. According to a 2009 report by the inspectors general of several defense and intelligence agencies, over time, "the program became less a temporary response to the September 11 terrorist attacks *and more a permanent surveillance tool*."[16]

The Privacy Board's report indicates that from late 2001 through early 2006, the NSA collected bulk telephone metadata based upon presidential authorizations issued every thirty to forty-five days.[17] Legal authorization for this data collection first came in May

---

14. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, 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 37 (2014), https://www.nsa.gov/civil_liberties/_files/pclob_report_on_telephone_records_program.pdf.

15. *Id.*

16. *Id.* at 37 (emphasis added).

17. According to the Report, data retention practices vary among providers. Telephone service providers currently are required by regulation to maintain records of the calls made by each telephone number only for eighteen months.

2006, when the Foreign Intelligence Surveillance Court ("FISC") first granted an application by the government to conduct the telephone records program under § 215.[18] The records collected involved both communications between individuals in the United States and others abroad, and communications wholly within the United States, including local calls.[19] The data collection thus represents the mass surveillance of U.S. citizens and a blurring of the boundaries of what constitutes foreign information. In June of 2013, the Guardian published an article concerning Edward Snowden's revelations about the program; in response, FISC Judge Claire Eagan issued an opinion in August of 2013 explaining the court's rationale for approving the § 215 telephone records program.[20] This was the first judicial opinion to explain the FISA court's legal reasoning in authorizing the bulk records collection.[21] The Privacy Board explained clearly and in detail the main functions and content of this far-reaching program as follows:

> The program is intended to enable the government to identify communications among known and unknown terrorism suspects, particularly those located inside the United States. When the NSA identifies communications that may be associated with terrorism, it issues intelligence reports to other federal agencies, such as the FBI, that work to prevent terrorist attacks. The FISC order authorizes the NSA to collect nearly all call detail records generated by certain telephone companies in the United States, and specifies detailed rules for the use and retention of these records. Call detail records typically include much of the information that appears on a customer's telephone bill: the date and time of a call, its duration, and the participating telephone numbers. Such information is commonly referred to as a type of "metadata." The records collected by the NSA under this program do not, however, include the content of any telephone conversation. After collecting these

---

However, it has been reported that one provider's database includes calls dating back twenty-six years. *Id.* at 141.

18. *Id.* at 9.

19. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 763 (2014).

20. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 13-109 (FISA Ct. Aug. 29, 2013) (amended memorandum opinion).

21. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 14, at 9.

> telephone records, the NSA stores them in a centralized database. Initially, NSA analysts are permitted to access the Section 215 calling records only through "queries" of the database. A query is a search for a specific number or other selection term within the database. Before any specific number is used as the search target or "seed" for a query, one of twenty-two designated NSA officials must first determine that there is a reasonable, articulable suspicion ("RAS") that the number is associated with terrorism. Once the seed has been RAS-approved, NSA analysts may run queries that will return the calling records for that seed, and permit "contact chaining" to develop a fuller picture of the seed's contacts. Contact chaining enables analysts to retrieve not only the numbers directly in contact with the seed number (the "first hop"), but also numbers in contact with all first hop numbers (the "second hop"), as well as all numbers in contact with all second hop numbers (the "third hop").[22]

The program did not, however, comply with the safeguards laid out in FISA governing the powers of intelligence agencies.[23] FISA includes four such safeguards: first, any information obtained should be linked to a specific person or entity already identified prior to the collection of the data; second, probable cause must exist that the target was a foreign power or an agent thereof; third, only certain types of information could be obtained; and fourth, the FISC should provide oversight.[24] The metadata program does not comply with any of these safeguards. According to the Privacy and Civil Liberties Oversight Board, the telephone records acquired under the program have no connection to any specific FBI investigation at the time the government obtains them.[25] Instead, they are collected for future use, in the event that such a connection does arise. The records are also collected in bulk; accordingly, they are not "relevant" to any FBI investigation, unless

---

22. *Id.* at 8–9.

23. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783; 124 Cong. Rec. 35,389 (codified at 50 U.S.C. 1801 (1978)).

24. Donohue, *supra* note 19, at 766–67. These protective clauses and the adoption of FISA as such were prompted by revelations of secret domestic NSA surveillance programs. Therefore, FISA was enacted in order to prevent precisely the types of broad surveillance and create a strictly defined framework for the collection of foreign intelligence. *See id.* at 767–82.

25. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 14, at 57.

that word is drastically redefined.[26] In addition, the program requires the companies to provide the government with calling records on a daily basis.[27] This approach is inconsistent with FISA, which limits the collection of this information. Finally, the statute permits the FBI, not the NSA, to obtain data for use in investigations.[28] The program allows the acquisition of data on an ongoing basis of individuals who are presumed innocent and against whom there is no individualized suspicion.[29] It has also been noted that oversight is delegated to the executive; thus the FISC does not perform its most basic action to protect U.S. citizens.[30]

The U.S. government has relied on *Smith v. Maryland* to defend the constitutionality of the NSA programs.[31] Apart from relying on the so-called "third party doctrine,"[32] according to the U.S. government, the only point when an individual has a reasonable expectation of privacy is not at the moment of the acquisition of data, but when it has been subjected to queries.[33] However, the NSA metadata program differs in multiple respects from the one found in the facts of *Smith v. Maryland*: it involves the bulk collection of data, places individuals under surveillance who are not suspects of any wrongdoing, and requires the ongoing character of surveillance and the compulsory character of transferring the data. These differences, along with the significant evolutions in technology since the judgment was delivered, render the direct application of the *Smith* judgment to the NSA metadata program rather doubtful.[34] The U.S. government also argues that, even if there were a cognizable search for the purposes of the Fourth Amendment, the collection of telephone metadata is

---

26. *Id*.
27. *Id*.
28. *Id.* at 57–58.
29. Donohue, *supra* note 19, at 843–48.
30. According to the order, NSA officials were required to determine whether sufficient evidence exists to place individuals or entities under surveillance—an obligation that was systematically violated. *Id.* at 807–08.
31. ADMINISTRATION WHITE PAPER, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 19 (August 2013).
32. According to the "third party doctrine," a person does not have a legitimate expectation of privacy in information they voluntarily disclose to third parties. *See* United States v. Miller, 425 U.S. 435, 443 (1976).
33. Donohue, *supra* note 19, at 864.
34. *Id*. at 869–71.

nevertheless reasonable.[35] However, this argument disregards the intrusive character of the program,[36] as evidenced not only by the volumes of data available to the NSA, but also by the structured nature of metadata that enables aggregation fairly easily.[37]

In the wake of the Snowden disclosures in 2013, legislative reforms to surveillance practices were considered necessary in order to restore public trust.[38] Indeed, a few months later in October 2013, the USA FREEDOM Bill (formally known as Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act) was introduced, aimed at imposing limitations to surveillance conducted for national security purposes.[39] In June 2015, after seven renewals,[40] the metadata program was left to sunset and was then replaced by a targeted surveillance program prescribed by the USA FREEDOM Act.[41] The Act bans bulk collection and instead allows the government to obtain phone records only if it can demonstrate to the FISA court a reasonable, articulable suspicion that its search term is linked to a foreign terrorist organization.[42] The Act also contains provisions that enhance transparency and accountability about surveillance activities. In particular, while in the past the FISC published almost none of its decisions, the bill requires declassification of the court's opinions containing important legal interpretations, or at least a summary in

35. Defendant's Memorandum of Law in Opposition to Plaintiff's Motion for a Preliminary Injunction at 25, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) No. 13-cv-3994 ("Any intrusion on privacy is minimal [ ] because only telephony metadata are collected.").

36. Donohue, *supra* note 19, at 871.

37. *See Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 5 (2013) (written testimony of Edward W. Felten).

38. *See* Patrick Leahy & Jim Senserbrenner, *The Case for NSA Reform*, POLITICO (Oct. 29, 2013), http://www.politico.com/story/2013/10/leahy-sensenbrenner-nsa-reform-098953.

39. For the text of the Bill, see S. Con. Res. 1599, 113th Cong. (2013).

40. It has been pointed out that the reason why Congress renewed the authorizations was because most members of Congress were unaware of the extent of surveillance the NSA was performing. *See* ACLU v. Clapper, 785 F.3d 787, 820 (2d Cir. 2015).

41. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015).

42. *Id.* §§ 103, 201, 501.

cases when declassification is not possible.[43] Moreover, private companies are given increased ways to report to the public information about the number of FISA orders and national security letters they receive.[44] Importantly, the government is equally obliged to report on the number of times it uses certain surveillance powers annually.[45] Regrettably, Congress dropped a requirement from an earlier draft of the legislation requiring the government to disclose information on the number of U.S. citizens about whom it collects information.[46]

Although the Act represents the first major surveillance reform since the 1970s, it does not completely curtail mass surveillance, much to privacy advocates' disappointment. Other secret programs, such as the one operated against non-EU citizens' communications, are left untouched.[47] In addition, the Act may not necessarily signify the end of bulk collection of phone records; this will depend on the interpretation of many of its provisions by the FISC.[48] The broad definition of "selector terms"—terms that the NSA uses to define the scope of its data requests to phone companies—has raised concerns that the Act will still allow the NSA to collect vast amounts of information.[49]

To these concerns one can add the ambivalence demonstrated by U.S. courts thus far about placing limits on mass surveillance. In

---

43. *Id.* § 402.

44. *Id.* § 603.

45. *Id.* § 602.

46. Sabrina Siddiqui, *Congress Passes NSA Surveillance Reform in Vindication for Snowden*, THE GUARDIAN (June 3, 2015), http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden. Other provisions that were dropped in the final text include the introduction of a special advocate to argue the public's interest in the FISC, and the removal of a requirement that a judge considering a challenge to a gag order must treat government claims that disclosure would harm national security as conclusive. *See US: Modest Steps by Congress on NSA Reform*, HUMAN RIGHTS WATCH (May 8, 2014), https://www.hrw.org/news/2014/05/08/us-modest-step-congress-nsa-reform.

47. HUMAN RIGHTS WATCH, *supra* note 46.

48. Jennifer Granick, *NSA's Creative Interpretations of Law Subvert Congress and the Rule of Law*, FORBES (Dec. 16, 2013), http://www.forbes.com/sites/jennifergranick/2013/12/16/a-common-law-coup-detat-how-nsas-creative-interpretations-of-law-subvert-the-rule-of-law/.

49. Andrea Peterson, *NSA Reform Bill Passes House, Despite Loss of Support From Privacy Advocates*, WASH. POST (May 22, 2014), https://washingtonpost.com/news/the-switch/wp/2014/05/22/nsa-reform-bill-passes-house-despite-loss-of-support-from-privacy-advocates/.

December 2013, a federal judge ruled that the NSA program was most likely unconstitutional, but issued no order, allowing the Court of Appeals for the District of Columbia to review his decision.[50] In August 2015, this court held that the plaintiff had failed to meet the heightened burden of proof regarding standing required for preliminary injunctions, thus sending the case back to the district court.[51] More recently, and despite the scheduled expiration of the program, the same judge confirmed his views and insisted that the constitutional issues were too important to be left unanswered.[52] However, in another case, a federal judge in New York found the program legal.[53] The Second Circuit eventually ruled that the program was not based on a legitimate interpretation of the PATRIOT Act, but it avoided ruling on the various constitutionality issues.[54]

C. Mass Surveillance in the European Union: The Data Retention Directive Saga

Data retention and transfer systems have been established and developed in parallel in the EU and the United States. In the EU, calls for the imposition of data retention obligations grew after the Madrid bombings in 2004. In its follow-up Declaration on Combating Terrorism, issued on March 25, 2004, the EU heads of state instructed the Council of the European Union to examine proposals for establishing rules on the retention of communications traffic data by service providers.[55] The London 7/7 bombings then led to the re-prioritization of the adoption of data retention rules,[56] and the Prime Minister of the United Kingdom, the President of the EU at the time,

50. Klayman v. Obama, 957 F.Supp. 2d 1, 10 (D.D.C. 2013).
51. Obama v. Klayman, 800 F.3d 559, 564 (D.C. Cir. 2015).
52. Klayman v. Obama, 2015 WL 6873127 (D.D.C. 2015).
53. ACLU v. Clapper, 959 F.Supp.2d 724 (S.D.N.Y. 2013).
54. ACLU, 785 F.3d 787, 818–827 (2d Cir. 2015).
55. Presidency Conclusions, Brussels European Council (Mar. 25–26, 2004).
56. Press Release, Council of the European Union Justice and Home Affairs Council, Council Declaration on the EU Response to the London Bombings, ¶ 4 (July 13, 2005), http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/85703.pdf.

subsequently prioritized and expedited negotiations.[57] The Directive was formally adopted in early 2006.[58]

The Data Retention Directive aimed to harmonize member states' data retention provisions, "in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member state in its national law."[59] The Directive applied to traffic and location data on both legal entities and natural persons, but not to the content of electronic communications.[60] Telecommunications providers were placed under an obligation to retain data.[61] Data would be retained for periods "no less than six months and not more than two years from the date of the communication."[62] Moreover, the retention period could be extended by member states "facing particular circumstances that warrant an extension."[63] Access to retained data was limited "only to the competent national authorities in specific cases and in accordance with national law."[64] However, the Directive did not define what constitutes a competent authority, leaving the designation of such authorities to member states. Access to personal data was governed by national law, in accordance with necessity and proportionality and subject to EU and international law (in particular the European Convention on Human Rights ("ECHR")).[65] Specific provisions on data protection[66] (including a provision on the designation of supervisory authorities by member states[67]) and remedies[68] were also included in the Directive. However, these provisions were specific and limited, and

---

57. Chris Jones, *Background to the EU Data Retention Directive*, EU LAW ANALYSIS (Apr. 7, 2014), http://eulawanalysis.blogspot.co.uk/2014/04/background-to-eu-data-retention.html.

58. Directive 2006/24/EC, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54 [hereinafter Data Retention Directive].

59. *Id.* art. 1(1).

60. *Id.* art. 1(2).

61. *Id.* art. 3(1).

62. *Id.* art. 6.

63. *Id.* art. 12(1).

64. *Id.* art. 4.

65. *Id.*

66. *Id.* art. 7–9.

67. *Id.* art. 9.

68. *Id.* art. 13.

their substance, particularly with regard to judicial remedies,[69] was again left for member states to define.[70]

The adoption and implementation of the data retention Directive have proven to be thorny tasks. Dissenting member states have challenged the legality of the adoption of the Directive, though the Court of Justice has upheld the Directive's legality.[71] However, the court's decision has not stopped considerable litigation before national courts[72] and the Court of Justice from going forward. Courts in Europe have had to grapple with the considerable challenges posed by the paradigm of generalized preemptive surveillance, established in the data retention Directive, to privacy and data protection.

Prior to examining the case law of European courts in relation to data retention, it is important to highlight a ruling of the European Court of Human Rights on different aspects of surveillance. In the case of *S. and Marper v. United Kingdom*, the European Court of Human Rights examined the compatibility with the ECHR of the systemic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or whose criminal proceedings have been discontinued in the U.K.[73] The court found that such blanket and indiscriminate retention of data was disproportionate to the stated purpose of combatting crime and thus noncompliant with Article 8 of the Convention.[74] The ruling is important in rejecting the *retention* of DNA data per se: according to the Court, the mere retention and storing of personal data by public authorities, however obtained, has a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data.[75] It is also important in highlighting the broader impact of retention on the affected individuals and, in particular, the risk of stigmatization stemming from the fact that persons in the position of the applicants,

---

69. *Id.* art. 13(1).

70. For further analysis on the negotiations and the content of the Directive, see VALSAMIS MITSILEGAS, EU CRIMINAL LAW 235 (2009).

71. Case C-301/06, Ir. v. European Parliament and Council, 2009 E.C.R. I-00593.

72. For an overview, see Theodore Konstadinides, *Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem*, 36 EUR. L. REV. 722, 722–36 (2011).

73. S. and Marper v. U.K., App. No. 30562/04 and 30566/04, Eur. Ct. H.R. (2008).

74. *Id*.

75. *Id*. ¶ 121.

who have not been convicted of any offense and are entitled to the presumption of innocence, are treated in the same way as convicted persons.[76]

In terms of data retention specifically, a number of constitutional courts in Europe have found domestic data retention legislation implementing the EU data retention Directive to be unconstitutional.[77] A common theme in these opinions is the emphasis on the adverse impact of breaches of privacy on the relationship between the individual and the state more broadly. According to the German Constitutional Court:

> Precautionary storage without cause of all telecommunications traffic data . . . is such a serious encroachment *inter alia* because it can create a sense of being permanently monitored . . . The individual does not know which state authority knows what about him or her, but knows that the authorities may know a great deal about him or her, including highly personal matters.[78]

The Romanian Constitutional Court, on the other hand, has noted that data retention involves all individuals, regardless of whether they have committed criminal offenses or whether they are the subject of a criminal investigation. This is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes. According to the Romanian Court, continuous data retention generates legitimate suspicions about the state's respect for its citizens' privacy and about the perpetration of abuses by the state.[79]

In all of these rulings, courts have criticized the extension of state power by ruling against the retention of personal data, regardless of any subsequent processing of the data. Courts have addressed the erosion of citizenship and trust such retention involves and highlighted the importance of privacy as underpinning the exercise of other

---

76. *Id*. ¶ 122.

77. *See* Mitsilegas, *The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance*, *supra* note 6.

78. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVERFGE] 125, 260–385 (Ger.), ¶ 214.

79. Curtea Constituţională a României [CCR] [Romanian Constitutional Court] Oct. 8, 2009, MONITORUL OFFICIAL AL ROMANIEI, Decision no. 1258.

fundamental rights.[80] By focusing on the individual and adopting a holistic approach to protection, the judiciary has begun to develop privacy into a meaningful constitutional safeguard against preemptive surveillance.

In addition to these powerful rulings from national constitutional courts in Europe, the Court of Justice ("CJEU") has also made a decisive move toward using privacy to limit preemptive surveillance. In its landmark ruling in the case of *Digital Rights Ireland*,[81] the Court of Justice annulled the data retention Directive on the grounds that the EU legislature had failed to comply with the principle of proportionality in the EU Charter of Fundamental Rights (hereinafter the Charter). The court developed its ruling in six main steps. The first step was to focus on proportionality and to emphasize the importance of the principle by reference to CJEU case law,[82] but also by reference to the European Court of Human Rights' jurisprudence in *S. and Marper*.[83] The second step was to view data protection as a means of protecting privacy and the right to respect for private life enshrined in Article 7 of the Charter.[84] The third and key step was the focus on the generalized and unlimited collection of personal data under the Directive. According to the court, the Directive required the retention of all traffic data concerning fixed telephony,

---

80. Mitsilegas, *The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance*, *supra* note 6, at 107.

81. Joined Cases C-293/12 and C-594/12, Digital Rights Ir. Ltd. v. Ir., 2014 E.C.R. 238.

82. According to the settled case law of the court, the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives. *See* Case C-343/09 Afton Chemical, 2010 E.C.R. I-7078; Volker und Markus Schecke and Eifert, 2010 E.C.R. I-11149–50; Cases C-581/10 and C-629/10 Nelson and Others, 2012 ECLI:EU:C:2012:657, 71; Case C-283/11 Sky Österreich, 2013 ECLI:EU:C:2013:28, 9; and Case C-101/12 Schaible v. Land Baden-Württemburg, EU:C:2013:661, 6–9.

83. With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference. By analogy, as regards Article 8 of the ECHR, see S. and Marper, *supra* note 73, at ¶ 47.

84. Case C-293/12, Digital Rights Ir. Ltd. v. Minister for Cmmc'ns, Marine and Nat. Res. and others, 2014 E.C.R. 238.

mobile telephony, Internet access, Internet e-mail, and Internet telephony. It therefore applied to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives.[85] Furthermore, the Directive covered all subscribers and registered users. It therefore required interference with the fundamental rights of practically the entire European population.[86] The court further noted that the Directive affected all persons using electronic communications services, even persons for whom there was no evidence suggesting that their conduct might have a link—even an indirect or remote one—with serious crime.[87] Neither did the Directive require any relationship between the data retained and a threat to public security. In particular, the data retained was not required to be (i) related to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) related to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection, or prosecution of serious offenses.[88] The fourth step that the court took was to focus on the absence of meaningful limits on access to personal data in the Directive[89] and on the fact that no prior authorization by a judicial or independent administrative authority is required.[90] The fifth step was to highlight the shortcomings

---

85. *Id.* ¶ 57.
86. *Id.* ¶ 56
87. *Id.* ¶ 58.
88. *Id.* ¶ 59.
89. *Id*. ¶ 61. Article 4 of the Directive, which governs the access of those authorities to the data retained, does not expressly provide that access and subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offenses or of conducting criminal prosecutions relating thereto; it merely provides that each member state is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.
90. *Id.* ¶ 62. Access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on member states designed to establish such limits.

in the Directive's provisions on the length of data retention.[91] The sixth step for the court, which is of great importance in light of moves toward data transfer to third countries and the globalization of surveillance, was to highlight the absence of safeguards on data security and protection and the lack of geographical limits to data retention. The court pointed out that the Directive did not require the data in question to be retained within the EU, and therefore did not comply with the requirement that an independent authority of compliance maintain control of the data. Such 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.[92]

The implications of the ruling of the Court of Justice in *Digital Rights Ireland* for the reconfiguration of the relationship between preemptive surveillance and privacy cannot be underestimated. Although the court did accept that the retention of telecommunications data pursued a legitimate aim,[93] it clearly found the system of mass, blanket surveillance set out by the Directive disproportionate and in breach of the rights to private life and data protection as enshrined in the Charter. The court's findings on the creation by the Directive of a system of generalized and unlimited surveillance based on the blanket retention of telecommunications data are particularly instructive in this context, and have been echoed on the other side of the Atlantic by the Privacy and Civil Liberties Oversight Board findings on the U.S. NSA program.[94] By stressing the establishment of a system of generalized preemptive surveillance by the data retention Directive, the Court of Justice also reflected to a great extent the case law of national constitutional courts. Although the court did not answer the question of the validity of the Directive in light of Article 11 of the Charter (enshrining the right to freedom of expression), it is highly

---

91. Council Directive 2006/24, art. 6, 2006 O.J. (L105) 54. The Directive requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of the Directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. Furthermore, that period is set at between a minimum of six months and a maximum of twenty-four months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary. *Id.* ¶¶ 63–64.

92. Case C-293/12, Dig. Rights Ir. Ltd. v. Minister for Cmmc'ns, Marine and Nat. Res. and others, 2014 E.C.R. 238, ¶ 68.

93. *Id*. ¶¶ 41–44.

94. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 14.

likely that similar questions will continue to reach the court in the context of EU measures on preemptive surveillance. The court's ruling has significant implications not only in questioning the constitutionality of data retention frameworks, but also in questioning the compatibility with the Charter of the surveillance systems established and legitimized by the transatlantic Passenger Name Records ("PNR") and Terrorism Finance Tracking Program ("TFTP") Agreements as well as the proposals for internal EU PNR and TFTP instruments. The court's findings with regard to the establishment of a system of generalized and unlimited surveillance with weak provisions governing access and length of retention of data are also applicable in the context of the PNR and TFTP Agreements. Transfer of personal data to the U.S. under the respective agreements would not be compatible with the Charter following *Digital Rights Ireland* in view of the weak data protection and privacy safeguards provided by the Agreements and by U.S. law, and the system of massive, generalized surveillance and the bulk transfer of everyday personal data to U.S. authorities that the Agreements entail.

III. COMPARING THE CONSTITUTIONAL PROTECTION OF PRIVACY IN THE EUROPEAN UNION AND THE UNITED STATES: WHY EUROPEAN UNION LAW PROVIDES A HIGHER LEVEL OF PROTECTION

The examination of constitutional responses to mass surveillance in the EU and the United States has demonstrated that EU law provides a higher level of protection of privacy than the United States legal framework in four main respects. First of all, EU law provides a higher level of protection *ratione personae,* i.e., in answering the question of who has privacy rights. The two key human rights instruments that form the backbone of EU constitutional law in the field—the European Convention on Human Rights and the EU Charter of Fundamental Rights—extend the right to privacy (and, in the case of the Charter, the right to data protection), to *everyone*, without limiting protection to citizens of EU member states.[95] This approach to privacy is important as it creates equality and a level playing field in the protection of privacy between citizens and aliens, and also helps to address gaps in protection arising in particular from extraterritorial

95. Eur. Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Nov. 4, 1950, art. 8, Europ. T.S. No. 5, 213 U.N.T.S. 221; Charter of Fundamental Rights of the European Union Articles 7 and 8, 2012 O.J. (C 326), 397 [hereinafter EU Charter of Fundamental Rights].

surveillance practices that states may employ. The second area where EU law provides a higher level of privacy protection involves the *substance* and *content* of the right to privacy. The ruling of the Court of Justice in *Digital Rights Ireland* discussed in this section demonstrates clearly that mass, generalized surveillance is unlawful under EU law. In reaching this conclusion, the court has adopted a three-step test for assessing human rights compliance adopted by the European Court of Human Rights in Strasbourg: the court assessed in turn interference of mass surveillance with the right to privacy, its necessity in a democratic society, and its proportionality to the aim pursued (including asking whether the aim pursued by governments can be achieved by less intrusive means than those adopted).[96] Mass surveillance falls down on the proportionality hurdle. Proportionality in this context provides a stronger privacy safeguard than the Fourth Amendment reasonableness test, whose limits have been pointed out and criticized widely in academic literature.[97] The establishment of privacy-specific constitutional rights (Article 8 of the ECHR and Articles 7 and 8 of the Charter, for example) further contributes to the achievement of a high level of substantive privacy protection in EU law. The third area where EU law provides a higher level of protection involves the provision of remedies and avenues for judicial redress to individuals whose privacy rights have been affected. EU law has made it possible for individuals who claim to be potentially affected by mass surveillance to be provided with a remedy before national courts and before the Court of Justice of the EU. The case of *Schrems*, where a Facebook subscriber was concerned about the potential access to his personal data by U.S. security services, is illustrative in this instance.[98] An extensive approach to standing has also been endorsed by the

---

96. The principle of proportionality is also enshrined in Article 52(1) of the EU Charter of Fundamental Rights. Under Article 52(1), subject to the principle of proportionality, limitations on the exercise of the rights and freedoms recognized by the Charter may be made only if they are necessary and genuinely meet objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others. For an analysis, see PAUL CRAIG, EU ADMIN. LAW ch. 19 (2d ed. 2012).

97. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK. THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007); Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381 (2008); Cynthia Lee, *Reasonableness With Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133 (2012).

98. Case C-362/14, Maximilian Schrems v. Data Prot. Comm'r (Sept. 23, 2015), http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1268424.

European Court of Human Rights. In its recent ruling in *Zakharov*,[99] the court stressed the need to ensure that the secrecy of surveillance measures does not result in the measures being effectively unchallengeable and outside the supervision of the national judicial authorities and of the court:

> [T]he Court accepts that an applicant can claim to be the victim of a violation occasioned by the *mere existence* of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies . . . where the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, *widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified*. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, *thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8*. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto*, is justified. In such cases *the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him.* By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or

99. Roman Zakharov v. Russ., App. No. 47143/06, Eur. Ct. H.R. (2015).

> of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.[100]

In *Zakharov,* the European Court of Human Rights provided a meaningful route toward upholding the right to an effective remedy with regard to privacy violations resulting from state surveillance.[101] It has allowed standing where applicants can evoke the mere existence of secret surveillance measures, with individuals not needing to demonstrate the existence of any risk that surveillance measures were applied to them if national systems do not provide an effective remedy for individuals to challenge such surveillance. The court has thus expressly linked the extension of standing rules with the existence of effective remedies at the national level.

The approach of the European Court of Human Rights is in stark contrast to the U.S. Supreme Court ruling in *Clapper v. Amnesty International*.[102] In *Clapper*, the Supreme Court found that the respondents, who challenged the Foreign Intelligence Surveillance Act, had no standing because they had no injury.[103] According to the Court, the respondents' claim that their communications with foreign contacts would be intercepted at some point in the future was highly speculative.[104] The ruling of the Supreme Court in *Clapper* limits standing considerably in cases of mass surveillance. Accordingly, *Clapper* also constitutes a barrier to the constitutional protection of privacy in the United States.

The enjoyment of the right to an effective remedy is closely linked to the fourth area where EU law provides a higher level of constitutional protection of privacy compared to U.S. law, namely the area of independent privacy supervision. Independent supervision with regard to data protection law is firmly enshrined in EU constitutional law after Lisbon in both the Treaty on the Functioning

---

100. *Id.* ¶ 171 (emphasis added).

101. The right to an effective remedy is also enshrined in Article 47 of the EU Charter of Fundamental Rights. EU Charter of Fundamental Rights, *supra* note 95, art. 47.

102. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

103. *Id*. at 1155.

104. *Id.* at 1143, 1150.

of the European Union ("TFEU")[105] and in the EU Charter of Fundamental Rights.[106] Further, independent supervision is an EU constitutional requirement, which features prominently in transatlantic negotiations on the establishment of a level playing field of protection. By comparison, the United States is seen as not providing an equivalent level of independent supervision.[107] Independent supervision has a dual role. It is essential to ensure rigorous and independent scrutiny of the compliance of member states with EU constitutional and secondary legislation on data protection. However, it is also an avenue—via the powers of independent authorities to investigate individual complaints concerning breaches of data protection law—for the provision of an effective remedy for individuals whose privacy rights have been adversely affected.[108]

This dual role of independent supervisory authorities in ensuring a meaningful and high level of protection has been confirmed in the ruling of the Court of Justice of the EU in *Schrems*.[109] There, the court emphasized the powers of independent authorities to review the substance of individual complaints, even in the existence of a general decision presuming that the level of data protection in a third country (in that case in the United States) is "adequate," with the court linking such review with upholding the rule of law in the EU.[110] At the same time, the very existence of an independent authority at the national level has effectively provided the complainant with standing and an effective remedy at the national and at the EU level: Mr. Schrems complained about the potential misuse of his Facebook personal data in the United States to the Irish independent supervisory authority, the Data Protection Commissioner.[111] Upon rejection of his claim by the Commissioner, he brought an action challenging the

105. Article 16(2) of the TFEU states that compliance with EU data protection rules must be subject to the control of independent authorities. Treaty on the Functioning of the European Union art. 16(2), Oct. 26, 2012, 2012 O.J. (C 326) 47.

106. Article 8 of the Charter on the right to protection of personal data requires compliance with its rules to be subject to control by an independent. EU Charter of Fundamental Rights, *supra* note 95, art. 8.

107. *See infra* discussion of the "Umbrella Agreement" in Part V.a.

108. *See* Hielke Hijmans, *The Role of Independent Supervision in Upholding Privacy in the Age of Surveillance*, OPEN DEMOCRACY (Feb. 8, 2016), https://www.opendemocracy.net/digitaliberties/hielke-hijmans/role-independent-supervision-upholding-privacy-age-surveillance.

109. Schrems, *supra* note 98.

110. *Id.* ¶ 38–66.

111. *Id.* ¶ 25.

Commissioner's decision before the Irish High Court, which then decided to send the question in the form of a preliminary reference to the Court of Justice of the European Union,[112] thus giving rise to the seminal ruling in *Schrems*. The existence of an independent authority at the national level, where individuals can lodge complaints regarding potential breaches of their rights, has thus in this case proven essential to giving a voice to these individuals and providing remedies at both the national and EU level. The action of an individual citizen in *Schrems*, lodging a general claim before an independent authority (a claim which, under the reasoning of the U.S. Supreme Court in *Clapper* would most likely be considered "speculative"[113]), has resulted in a ruling by the Court of Justice of the European union which, as will be seen below, has established a very high benchmark for the protection of privacy at the EU and transatlantic level.

IV. MASS SURVEILLANCE IN TRANSATLANTIC COUNTER-TERRORISM COOPERATION

The human rights challenges posed by the post-9/11 paradigm of mass surveillance exist on a global scale due to a series of cooperative counter-terrorism arrangements between the United States and the EU involving the transfer of personal data to U.S. authorities. This section will analyze three types of counter-terrorism cooperation: cooperation following data transfer requirements imposed unilaterally by U.S. legislation (for example, PNR Agreements); cooperation following unilateral secret executive U.S. action (for example, TFTP Agreements); and cooperation following a direct request by the U.S. to a private company for access to personal data located in servers in Europe. This section will highlight the extent of surveillance these arrangements entail, while the next section will highlight ways in which security arrangements themselves have attempted to address privacy concerns caused by the surveillance systems these arrangements authorize.

112. *Id.* ¶ 25.
113. Clapper, *supra* note 102, at 1143, 1150.

A. The Challenge of Complying with U.S. Post-9/11 Law: The EU-U.S. PNR Agreements

One of the key strands of U.S. counter-terrorism policy post-9/11 has been the requirement that airlines collect detailed personal data from their passengers in advance of travel in order for such data to be available to the Department of Homeland Security.[114] This strategy was adopted after 9/11, which demonstrated to the United States the increasing mobility and destructive potential of modern terrorism and the interdependence between U.S. responses and the global transport infrastructure.[115] This focus on interdependence was reaffirmed by then U.S. Secretary of Homeland Security Tom Ridge, who noted that, "as the world community has become more connected through the globalization of technology, transportation, commerce and communication, the benefits of these advances enjoyed by each of us are available to terrorists as well."[116] To prevent potentially dangerous mobility to the United States on a global scale, the U.S. Congress passed legislation in November 2001 requiring air carriers operating flights to, from, or through the United States to provide U.S. customs with electronic access to data contained in their automatic reservation and departure control systems.[117] This data, known as Passenger Name Records ("PNR"), constitutes a record of each passenger's travel requirements and contains all the information necessary to enable reservations to be processed and controlled by the booking and participating airlines.[118] Transfer of such information to the U.S. authorities before departure has been a key element of the U.S. border security strategy focusing on identification and prevention.[119] PNR data can include a wide range of details, from the passenger's name and address to his email address, credit card details, and on-flight

---

114. Aviation and Transportation Security Act, Pub. L. 107-71, 15 Stat. 597 (codified in scattered sections of 5 U.S.C.; 26 U.S.C.; 31 U.S.C.; 42 U.S.C.; 49 U.S.C.)

115. OFFICE FOR HOMELAND SECURITY, NATIONAL STRATEGY FOR HOMELAND SECURITY 21 (2002).

116. Secretary Tom Ridge, Remarks at the London School of Economics (Jan. 14, 2005), http://www.lse.ac.uk/publicEvents/pdf/20050114-RidgeTom.pdf.

117. *See, e.g.*, 49 U.S.C. § 44909(c)(3) (describing reporting requirements for passenger name records); 19 C.F.R. § 122.49(b) (describing reporting requirements for cargo overages).

118. Richard Rasmussen, *Is International Travel Per Se Suspicion of Terrorism? The Dispute Between the United States and European Union Over Passenger Name Record Data Transfers*, 26 WIS. INT'L L.J. 551, 553–54 (2009).

119. *Id.*

dietary requirements.[120] The transfer of PNR data was deemed to be key to the operation of the U.S. Automated Targeting System ("ATS"), which uses a wide range of databases, including law enforcement and FBI databases "to assess and identify . . . travellers that may pose a greater risk of terrorist or criminal activity and therefore should be subject to further scrutiny or examination."[121]

The imposition of these duties to air carriers has placed them in an uncomfortable position with regard to EU law. Compliance with U.S. requirements to collect and transfer passenger data on such a large scale could result in carriers acting in breach of EU data protection law. In an attempt to reconcile these competing requirements, the European Commission embarked on negotiations with U.S. authorities to create a transatlantic agreement enabling the collection and transfer of PNR records to the United States in accordance with EU law.[122] The proposed agreement was criticized heavily by expert data protection bodies in the EU as well as by the European Parliament because it arguably fell short of respecting EU fundamental rights.[123] Nevertheless, on the basis of a decision by the commission confirming the adequacy of U.S. data protection standards,[124] a transatlantic agreement on the transfer of PNR data to the U.S. Bureau of Customs and Border Protection was signed in 2004. In the agreement, the Council evoked the urgency caused by the uncertainty for carriers and passengers.[125]

The legality of the agreement was subsequently litigated before the Court of Justice of the EU, with the European Parliament bringing an action for annulment of the agreement on the grounds that it violated the principle of proportionality and infringed the fundamental rights of privacy and data protection. In what can be

---

120. *Id.*

121. DEP'T OF HOMELAND SECURITY, PRIVACY OFFICE, A REPORT CONCERNING PASSENGER NAME RECORD INFORMATION DERIVED FROM FLIGHTS BETWEEN THE U.S. AND THE EUROPEAN UNION 38 (2008). For further analysis, see Valsamis Mitsilegas, *Immigration Control in an Era of Globalisation: Deflecting Foreigners, Weakening Citizens, Strengthening the State*, 19 IND. J. GLOBAL LEGAL STUD. 3 (2012).

122. European Commission, European Commission/U.S. Customs Talks on PNR Transmission Brussels, Joint Statement (2003).

123. For further details, *see* Valsamis Mitsilegas, *Contrôle des étrangers, des passagers, des citoyens: Surveillance et anti-terrorisme*, 58 CULTURES ET CONFLITS 155 (2005).

124. Comm'n Decision 2004/535/EC, 2004 O.J. (L235) 11, 15–22.

125. Council Decision 2004/496/EC, 2004 O.J. (L183) 83.

characterized as a pyrrhic victory for the European Parliament, the court annulled the measure but did not examine the substance of the Parliament's fundamental rights noncompliance allegations.[126]

After the 2004 agreement was annulled, a new EU-U.S. PNR agreement was established in 2007.[127] However, this new agreement has done little to address concerns about its compatibility with EU law.[128] Indeed, the European Parliament, which, after the Lisbon Treaty, was required to approve the agreement, expressed serious concerns about the compatibility of the agreement with EU privacy and data protection law.[129] In fact, the Parliament postponed a vote on the agreement so that it could explore options for PNR arrangements that were in line with EU law and that addressed its concerns about PNR.[130] The Parliament also stressed the need for independent review, judicial oversight, and democratic control in any new agreement, and it called for a series of data protection safeguards (purpose limitation, necessity, proportionality, redress) and for provisions on reciprocity.[131]

In response to Parliament's calls, the European Commission published a global PNR strategy.[132] In November 2010, the European Parliament welcomed the Commission's PNR strategy and endorsed the opening of new PNR negotiations with the United States.[133]

---

126. Joint Cases C-317-04 and C-318/04, Eur. Parliament v. Council, 2006 O.J. (C178) 1. The Parliament was supported by the European Data Protection Supervisor, while the Council was supported by the Commission and the U.K.

127. For details, see Valsamis Mitsilegas, *The External Dimension of EU Action in Criminal Matters*, 12 EUR. FOREIGN AFF. REV. 457 (2007).

128. 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), U.S.–EU, Aug. 4, 2007, O.J. (L204) [hereinafter 2007 PNR Agreement], 18. *See also* Council Decision Approving the Signing of the Agreement on the Basis of Articles 24 and 38 TEU, at 16.

129. European Parliament Resolution of 5 May 2010 on the Launch of Negotiations for Passenger Name Record (PNR) Agreements with the United States, Australia and Canada, EUR. PARL. DOC. P7_TA (2010) 0144.

130. *Id*. at Point 4. The European Parliament also postponed the voting for a similar EU-Australia PNR Agreement.

131. *Id*. at Points 6, 9.

132. Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) Data to Third Countries, COM (2010) 492 final (Sep. 21, 2010).

133. Eur. Parliament Resolution of 11 November 2010 on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries, and on the Recommendations from the Commission to the Council to Authorise the Opening of

However, the negotiation of a new transatlantic PNR Agreement was met with skepticism in the United States, with a number of U.S. voices arguing that the provisions of the 2007 agreement should be maintained and that changes were not necessary.[134] The European Commission, on the other hand, justified the need for a new EU-U.S. PNR agreement as follows:

> The data protection laws of the EU do not allow European and other carriers operating flights from the EU to transmit the PNR data of their passengers to third countries which do not ensure an adequate level of protection of personal data without adducing appropriate safeguards. A solution is required that will provide the necessary legal basis for the transfer of PNR data from the EU to the US as a recognition of the necessity and importance of the use of PNR data in the fight against terrorism and other serious transnational crime, whilst avoiding legal uncertainty for air carriers. In addition, this solution should be applied homogenously throughout the European Union in order to ensure a legal certainty for air carriers and respect of individuals' rights to the protection of personal data as well as their physical security.[135]

Despite U.S. resistance, a new EU-U.S. PNR agreement was eventually approved by the European Parliament in early 2012 and took effect on June 1, 2012.[136] The agreement will remain in force for a period of seven years and, unless one of the parties gives notice of its intention not to renew further, it will be renewable for subsequent seven-year periods.[137] Its structure is a significant improvement from a rule of law perspective, as the main provisions and safeguards are set out largely in the text of the EU–U.S. agreement itself, rather than

---

Negotiations between the European Union and Australia, Canada and the United States, EUR. PARL. DOC. P7_TA (2010) 0397.

134. KRISTIN ARCHICK, CONG. RESEARCH SERV., RS22030, U.S.–EU COOPERATION AGAINST TERRORISM (2013).

135. *Proposal for a Council Decision on the Signature of the Agreement between the United States of America and the European Union on the Use and Transfer of PNR to the United States Department of Homeland Security*, at 2, COM (2011) 805 final, Brussels (Nov. 23, 2011).

136. 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, U.S.-E.U., Aug. 8, 2012, O.J. (L215) 5 [hereinafter EU-U.S. PNR Agreement]. On entry into force, see *id.* art. 27(1).

137. *Id.* art. 26(1), 26(2).

in a letter by the United States to the EU, as was the case with the 2007 agreement. The purpose of the agreement—"to ensure security and to protect the life and safety of the public"—is defined rather broadly.[138] This expansive wording may challenge calls for the inclusion of strict purpose limitation safeguards under the agreement. The agreement applies to a wide range of carriers: to carriers operating passenger flights between the EU and the United States[139] as well as to carriers incorporating or storing data in the EU and operating passenger flights to or from the United States.[140] The agreement establishes an obligation for carriers to provide PNR data contained in their reservation systems to the U.S. Department of Homeland Security ("DHS") as required by DHS standards and consistent with the agreement.[141] Data transmission will occur initially ninety-six hours before departure and additionally either in real time or for a fixed number of routine and scheduled transfers as specified by DHS.[142] The agreement defines PNR data by reference to the Guidelines of the International Civil Aviation Organization ("ICAO").[143] As with the previous transatlantic PNR agreements, the actual categories of PNR data to be transferred to DHS are listed in an annex to the agreement. The annex contains nineteen categories of PNR data, including frequent flier information, payment information, travel itinerary, travel status, seat number, general remarks, and historical changes.[144] The agreement thus maintains the paradigm of the privatization of crime control set out in earlier agreements and imposes extensive obligations on carriers to transmit a wide range of everyday personal data to DHS.

The new EU-U.S. PNR Agreement contains a number of safeguards. Addressing longstanding concerns by the European Parliament, the agreement provides that PNR data will be transferred to DHS under the "push" method, and not under the "pull" method, which involved U.S. authorities extracting PNR data from airline

138. *Id.* art. 1(1).
139. *Id*. art. 2(2).
140. *Id*. art. 2(3).
141. *Id.* art. 3.
142. *Id.* art. 15(3). *But see id.* art. 15(5) (describing exceptions).
143. *Id*. art. 2(1).
144. *Id.* at Annex.

databases themselves.[145] Carriers are required to acquire the technical ability to use the "push" method no later than twenty-four months following the entry into force of the agreement.[146] However, the "pull" method is still permitted by the agreement when carriers are unable to respond to DHS requests, or in exceptional circumstances in order to respond to a specific, urgent, and serious threat.[147]

The agreement also contains a purpose limitation provision, allowing the collection, use, and processing of PNR data by U.S. authorities strictly for the purposes of preventing, detecting, investigating, and prosecuting terrorist offenses (defined by EU law), and other transnational crimes that are punishable by a sentence of imprisonment of three years or more.[148] However, these purpose limitation safeguards are substantially watered down: "PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual, or if ordered by a court;"[149] "PNR may be used and processed by DHS to identify persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination;"[150] and "[p]aragraphs 1–3 shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR."[151]

The agreement contains a number of specific data protection provisions, including those on data security,[152] sensitive data,[153] non-discrimination,[154] transparency,[155] access for individuals,[156] and correction and rectification.[157] Of particular significance is the provision on profiling, which states that "[t]he United States will not

145. *Id.* art.15(1). The move toward the push system was already envisaged in the U.S. letter to the EU as part of the 2007 EU-U.S. PNR agreement. 2007 PNR Agreement, *supra* note 128, at Point 8.

146. EU-U.S. PNR Agreement, *supra* note 136, art. 15(4).

147. *Id.* art. 15(5).

148. *Id.* art. 4(1).

149. *Id.* art. 4(2).

150. *Id.* art. 4(3).

151. *Id.* art. 4(4).

152. *Id.* art. 5.

153. *Id.* art. 6.

154. *Id.* art. 9.

155. *Id.* art. 10.

156. *Id.* art. 11.

157. *Id.* art. 12.

make decisions that produce significant adverse actions affecting the legal interests of the individuals based solely on automated processing and use of PNR."[158] The agreement also contains a specific provision on redress, but this provision references U.S. law, and the value that it adds for European citizens is unclear.[159] Similarly, data protection and privacy concerns are not assuaged by the agreement's provisions on data retention because DHS will retain PNR in an active database for up to five years,[160] and, after this active period, it will transfer PNR to a dormant database, where it may remain for up to ten years.[161] After this dormant period expires, any retained data must be made fully anonymous.[162] However, data related to a specific investigation may be retained in an active PNR database until the end of the investigation.[163] Moreover, the agreement allows the onward transfer of PNR data to third countries.[164]

The data protection safeguards provided for in the agreement are further diluted if examined within the framework of the agreement's provisions governing its applicability and the agreement's relationship with other instruments. The preamble to the agreement states that the "[a]greement does not constitute a precedent for any future arrangements between the Parties, or between either of the Parties and any other party, regarding the processing, use, or transfer of PNR or any other form of data, or regarding data protection."[165] This provision was likely intended to address U.S. concerns that the EU-U.S. PNR agreement would influence bilateral agreements between EU member states and the United States on the transfer of PNR data.[166] However, this seems to disregard that member state action in the field must be consistent with EU law and the EU-U.S. PNR agreement, because an international agreement adopted in the fight

158. *Id.* art. 7.
159. *Id*. art. 13.
160. *Id.* art. 8(1).
161. *Id.* art. 8(3).
162. *Id.* art. 8(4).
163. *Id.* art. 8(5).
164. *Id.* art. 17(1) ("The United States may transfer PNR to competent government authorities of third countries only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with those terms.").
165. *Id*. at Preamble.
166. ARCHICK, *supra* note 134, at 18–19.

against crime is part of EU law and international agreement.[167] Moreover, Article 21(2) states that nothing in the EU-U.S. PNR agreement will derogate from existing obligations of the United States and EU member states, including under the EU-U.S. Mutual Legal Assistance Agreement and the related bilateral mutual legal assistance instruments between the United States and EU member states.[168] A similar clause, designed to ensure the transfer of data to the United States under the broad provisions of the transatlantic agreement on mutual legal assistance, appears in the EU-U.S. TFTP agreement.[169] This again disregards the fact that bilateral agreements in the field of freedom, security, and justice should be implemented in conformity with EU law. These provisions raise serious questions about the extent to which individuals should expect a high level of protection under the new transatlantic PNR agreement.

B. Addressing U.S. Executive Action: The EU-U.S. TFTP Agreements

Another instance of U.S. authorities initiating generalized preemptive surveillance after 9/11 was the establishment of the Terrorist Financing Tracking Program ("TFTP"). Under this program, U.S. authorities could issue subpoenas, based on suspicion of involvement in international terrorism, for personal data generated by financial transactions in Europe and held by the Society for Worldwide Interbank Financial Telecommunication ("SWIFT"), a worldwide financial messaging service that facilitates international money transfers.[170] Routine access to SWIFT data by U.S. authorities was revealed in an article in *The New York Times* in 2006, which explained

---

167. For an analysis of the implications of the existence of shared competence in the field of freedom, security, and justice in the context of the EU-U.S. TFTP Agreement, see Marise Cremona, *Justice and Home Affairs in a Globalised World: Ambitions and Reality in the Tale of the EU–US SWIFT Agreement* (Inst. of European Integration Research, Working Paper No. 04/2011, Mar. 2011).

168. EU-U.S. PNR Agreement, *supra* note 136, art. 21(2).

169. Agreement on Mutual Legal Assistance between the E.U. and the U.S., Jul. 19, 2003 O.J. (L 181) 34 [hereinafter Mutual Legal Assistance Agreement]. For an analysis of the Agreement on Mutual Legal Assistance, see Valsamis Mitsilegas, *The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data*, 8 EUR. FOREIGN AFF. REV. 515 (2003).

170. U.S. DEP'T OF THE TREASURY, TERRORIST FINANCING TRACKING PROGRAM: FACT SHEET (Aug. 2, 2010), https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/TFTP%20Fact%20Sheet%20revised%20-%20(8-8-11).pdf.

that the TFTP program was initiated in secret several weeks after 9/11.[171] It was run out of the CIA and overseen by the Treasury Department, and it was a significant departure from typical practice in how the U.S. government acquires Americans' financial records: "[t]reasury officials did not seek individual court-approved warrants or subpoenas to examine specific transactions, [but] instead rel[ied] on broad administrative subpoenas for millions of records from [SWIFT]."[172] The revelation caused alarm in Europe, with both the Article 29 Working Party on data protection and the European Parliament expressing doubts about the compatibility of U.S. access to SWIFT data with European data protection law.[173] In response to these concerns, U.S. authorities explained the legal basis for the collection of SWIFT data under U.S. law,[174] emphasizing the emergency framing of U.S. executive action[175]:

---

171. Eric Lichtblau & James Risen, *Bank Data Is Sifted by U.S. in Secret to Block Terror*, N.Y. TIMES, June 23, 2006, http://www.nytimes.com/2006/23/washington/23intel.html.

172. *Id.* According to *The New York Times*, administration officials asked the *Times* "not to publish this article, saying that disclosure of the Swift program could jeopardize its effectiveness." *Id.*

173. *See Opinion 10/2006 of the Article 29 Data Protection Working Party on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, at 2 (Nov. 22, 2006) (concluding that, given the large scale of U.S. Treasury subpoenas, the continued processing of personal data is not compatible with the original commercial purpose for which the data was collected); European Parliament Resolution on the Interception of Bank Transfer Data from the SWIFT System by the US Secret Services, EUR. PARL. DOC. P6_TA(2006)0317 (2006); European Parliament Resolution on SWIFT, the PNR Agreement and the Transatlantic Dialogue on these Issues, EUR. PARL. DOC. B6-0042/2007 (2007).

174. Processing of EU Originating Personal Data by United States Treasury Department for Counter Terrorism Purposes—'SWIFT'—Terrorist Finance Tracking Program—Representations of the United States Department of the Treasury, 2007 O.J. (C 166) 18 [hereinafter Terrorist Fin. Tracking Program—Representations of the U.S. Dep't of the Treasury].

175. On September 23, 2001, the President of the United States issued Executive Order 13224. Exec. Order No. 13224, 3 C.F.R. § 13224 (2001). In that Order, the President declared a national emergency to deal with the 9/11 terrorist attacks and the continuing and immediate threat of further attacks, and blocked the property of, and prohibited transactions with, persons who commit, threaten to commit, or support terrorism. *Id.* The International Emergency Economic Powers Act of 1977 and the order, as implemented through the Global Terrorism Sanctions Regulations, authorize the Director of the Treasury Department's Office of Foreign Assets Control ("OFAC") to require any person to furnish financial transactions or other data in connection with an economic sanctions-related investigation. *Id.*

> Shortly after the September 11, 2001 attacks, as part of an effort to employ all available means to track terrorists and their networks, the Treasury Department initiated the TFTP. Under the TFTP, the Treasury Department has issued administrative subpoenas for terrorist-related data to the U.S. operations center of [SWIFT] . . . These subpoenas require SWIFT to provide the Treasury Department with certain financial transaction records—which are maintained by SWIFT's U.S. operations center in the ordinary course of its business—to be used exclusively for counterterrorism purposes as specified in the following sections . . . . The financial transaction records provided by SWIFT under compulsion of subpoena may include identifying information about the originator and/or recipient of the transaction, including name, account number, address, national identification number, and other personal data.[176]

The United States also provided the EU with a number of assurances and safeguards.[177] These included the appointment of an EU Eminent Person based in the United States to oversee access by U.S. authorities to SWIFT data.[178] The Eminent Person would verify the protection of EU-originating personal data and, in particular, confirm that processes for deletion of non-extracted data had been carried out.[179] In 2008, French Judge J.-L. Bruguière was appointed as the first EU Eminent Person.[180] Judge Bruguière, assisted by the European Commission, produced two reports, the first in December 2008 and the second in January 2010, "concluding that the U.S. Treasury complie[d] with its data protection undertakings and that the TFTP had been instrumental in preventing terrorist attacks within the

---

These are the legal authorities under which OFAC issues subpoenas to SWIFT for financial data that are related to terrorism investigations. *Id.*

176. Terrorist Fin. Tracking Program—Representations of the U.S. Dep't of the Treasury, *supra* note 174, at 18.

177. *Id*. The representations explained the fundamental principles underlying the TFTP, the legal authority to obtain and use SWIFT data, and included provisions limiting the extraction and use of data to the investigation of terrorism. *Id.*

178. *Id.* at 24–25.

179. *Id.*

180. For background, *see* J. Santos Vara, *The Role of the European Parliament in the Conclusion of the Transatlantic Agreements on the Transfer of Personal Data after Lisbon* (Ctr. for the Law of EU External Relations, Working Paper No. 2, 2013).

EU of the magnitude of the London, Madrid and Bali attacks."[181] The legal force of the U.S. assertions and the extent to which they could address EU constitutional concerns are questionable.

In 2007, SWIFT decided to alter the architecture of its databases to avoid mirroring European databases in U.S. territory.[182] This change in SWIFT architecture meant that U.S. authorities no longer had automatic access to SWIFT data generated in Europe.[183] This development rendered necessary a transatlantic agreement allowing access by U.S. authorities to such data.

The Council signed the first EU-U.S. TFTP agreement on November 30, 2009.[184] The agreement was applied on a provisional basis starting February 1, 2010.[185] However, soon after the Council signed the agreement, the Lisbon Treaty was passed, which requires the European Parliament to consent to agreements covering fields to which the ordinary legislative procedure applies, like the EU-U.S. TFTP agreement.[186] Member states chose to sign the agreement before the entry into force of the Lisbon Treaty, in what can be seen as an attempt to force Parliament into approving an agreement that was crystallized under previous rules that granted Parliament a minimal scrutiny role. The extent to which Parliament was sidelined in the process of scrutinizing the text of the TFTP agreement is highlighted by the fact that the agreement was completely declassified on February 8, 2010—just a few days ahead of the Parliament vote on February

---

181. *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*, at 2 (Feb. 17–18, 2011).

182. *SWIFT Board Approves Messaging Re-Architecture*, SWIFT, Oct. 4, 2007, https://www.swift.com/insights/press-releases/swift-board-approves-messaging-re-architecture.

183. Anthony Amicelle, *The EU's Paradoxical Efforts at Tracking the Financing of Terrorism: From Criticism to Imitation of Dataveillance,* CEPS PAPER IN LIBERTY AND SEC. IN EUR. 5–6 (Aug. 2013), http://aei.pitt.edu/43185/1/LSE_No_56_Dataveillance.pdf ("SWIFT representatives wanted to store European SWIFT messages in mirror servers in both the Netherlands and Switzerland, and no longer in the US operating centre. . . . [O]fficials could no longer request access to interbank messages that circulate in Europe.").

184. Council Decision 2010/16/CFSP/JHA, 2010 O.J. (L 8) 9.

185. *Id*. at 9.

186. *The European Parliament: Powers,* EUR. PARLIAMENT 1–2 (2016), http://www.europarl.europa.eu/ftu/pdf/en/FTU_1.3.2.pdf.

11.[187] This perceived attack on Parliament's institutional prerogatives led the European Parliament, notwithstanding sustained high-level pressure from European governments and the U.S. administration,[188] to reject the EU-U.S. TFTP agreement in February 2010, thus depriving U.S. authorities of a legal way to access European SWIFT data.[189] The European Parliament explained that the TFTP agreement "must be considered as a departure from European law and practice in how law enforcement agencies would acquire individuals' financial records for law enforcement activities, namely individual court-approved warrants or subpoenas to examine specific transactions instead of relying on broad administrative subpoenas for millions of records."[190]

The rejection of the first EU-U.S. TFTP agreement did not halt negotiations in the field. Both the U.S. and European governments deemed resuming negotiations a matter of urgency on the grounds that non-access by U.S. authorities to European SWIFT data would represent a major security gap. This is notwithstanding the fact that access to a wide range of financial data (albeit not in bulk form) could already take place under Article 4 of the 2003 EU-U.S. Agreement on Mutual Legal Assistance.[191] Negotiations, this time fully after Lisbon, led to the second EU-U.S. TFTP agreement in the summer of 2012; this agreement is currently in force.[192] The agreement is premised upon the recognition that the TFTP "has been instrumental in identifying and capturing terrorists and their financiers and has generated many leads that have been disseminated for counter terrorism purposes to competent authorities around the world, with particular value for EU

187. Deirdre Curtin, *Official Secrets and the Negotiation of International Agreements: Is the EU Executive Unbound?* 50 COMMON MKT. L. REV. 423, 449 (2013).

188. J. Monar, *Editorial Comment. The Rejection of the EU–US SWIFT Interim Agreement by the European Parliament: A Historic Vote and Its Implications*, 15 EUR. FOREIGN AFF. REV. 143, 145 (2010).

189. EUR. PARL. DOC. A7-0013/2010 (2010).

190. *Id.*

191. Mutual Legal Assistance Agreement, *supra* note 169.

192. Council Decision on the Conclusion 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 2010/412, 2010 O.J. (L 195) 3; 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 TFTP Agreement].

member states."[193] The agreement serves the dual purpose of providing the U.S. Treasury with financial payment messages "for the exclusive purpose of the prevention, investigation, detection or prosecution of terrorism or terrorist financing"[194] and of providing relevant information obtained through the TFTP to law enforcement, public security, or counterterrorism authorities of member states, or Europol or Eurojust (the EU agency dealing with the judicial cooperation in criminal matters), for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. This provision thus serves to address European concerns by including purpose limitations and reciprocity safeguards. However, the agreement allows the provision of SWIFT data to a wide range of authorities,[195] and it allows onward transmission to third countries.[196]

What should not be forgotten is that, as with the previous agreement, the new EU-U.S. TFTP agreement legitimizes under EU law the bulk transfer of everyday financial data, stemming from ordinary financial activities, to U.S. authorities. The legal challenges with regard to the bulk transfer of data were also highlighted by the European Data Protection Supervisor ("EDPS") in his opinion on the draft agreement, in which he emphasized that bulk transfers should be replaced with mechanisms allowing financial transaction data to be filtered in the EU, thereby ensuring that only relevant and necessary data are being sent to U.S. authorities.[197] The European Data Protection Supervisor was of the view that, if such mechanisms could not be found immediately, then the agreement should strictly define a short transitional period after which bulk transfers would no longer be

193. TFTP Agreement, *supra* note 192, at 5.

194. *Id*. art. 1(1)(a).

195. *Id*. art. 3.

196. *Id*. art. 7 (covering onward transfer and providing that such information shall be shared only with law enforcement, public security, or counterterrorism authorities in the United States, member states, or third countries, or with Europol, Eurojust, or other appropriate international bodies).

197. *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the Conclusion 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 Purposes of the Terrorist Finance Tracking Program*, 2010 O.J. (C 355) 10, ¶ 20 [hereinafter *Opinion of the Eur. Data Prot. Supervisor*].

allowed.[198] This provision is not in the final agreement,[199] but the agreement does open the door to the establishment of a European TFTP system.[200]

The EU-U.S. TFTP agreement includes a number of data protection safeguards. In addition to the safeguards included in relation to U.S. requests, the agreement provides safeguards applicable to the processing of provided data, including: purpose limitations, the prohibition of data mining, the prohibition of interconnection of provided data with other databases, the requirement to respect necessity and proportionality in data processing, and the requirement for all searches of provided data to be based upon preexisting information or evidence which demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing.[201] The agreement also includes specific provisions on data retention and deletion, with Article 6(4) stating that all non-extracted data received on or after July 20, 2007 shall be deleted not later than five years from receipt.[202]

The agreement also includes a series of provisions on specific data protection rights, including transparency,[203] the right of access,[204] the right to rectification, erasure or blocking,[205] the maintenance of the accuracy of the information,[206] and a provision of redress.[207] However, these safeguards do not negate the fact that the EU-U.S. TFTP agreement has legitimized and allows for what the Europol Joint

198. *Id.*

199. Terrorist Fin. Tracking Program–Representations of the United States Dep't of the Treasury, *supra* note 174, art. 23(2).

200. *Id.* art. 11.

201. *Id*. art. 5.

202. *Id.* art. 6. However, as noted in the European Commission's report on the second joint review to the agreement, Treasury informed the EU review team that the deletion of data could not be implemented as an ongoing process; instead, Treasury would carry out this deletion only after longer time intervals. *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*, at 10, SWD (2012) 454 final (Oct. 2012) [hereinafter *Second Joint Review of the Implementation of TFTP*].

203. Terrorist Fin. Tracking Program—Representations of the United States Dep't of the Treasury, *supra* note 174, at art. 14.

204. *Id.* art.15.

205. *Id.* art. 16.

206. *Id.* art. 17.

207. *Id.* art. 18.

Supervisory Body has called a "massive, regular data transfer from the EU to the US."[208]

C. The Challenge of U.S. Extraterritorial Surveillance: The Microsoft Saga

The U.S. requirements for access to data held by Microsoft demonstrate the privacy challenges arising from the global reach of U.S. surveillance.[209] A case dealing with this issue is currently pending before U.S. courts.[210] It was initiated in 2013 as U.S. authorities sought access to data related to an email account held by Microsoft. In December 2013, the U.S. government presented an affidavit establishing probable cause to believe that a Microsoft-based email account was being used for narcotics trafficking. The U.S. magistrate judge issued a search warrant pursuant to the 1986 Stored Communications Act ("SCA"),[211] requesting that Microsoft disclose the contents of the email account. Microsoft, however, refused to disclose the requested records on the basis that the U.S. court could not compel Microsoft to do so because the data were stored in a datacenter in Dublin, Ireland. Microsoft then filed a motion to vacate the warrant, which was denied; the judge stressed that the warrant obligated Microsoft to produce the solicited data, regardless of their storage location.[212] The judge found that the request by the government was not a conventional warrant, but rather a "compelled disclosure" or subpoena, and held that it was not an extraterritorial assertion of U.S. law.[213] Microsoft then filed a motion with the district court to quash the

---

208. Europol Joint Supervisory Body, Implementation of the TFTP Agreement: Assessment of the Follow-up of the JSB Recommendations (Third Inspection Report), at 2 (Mar. 18, 2013).

209. *See* Sergio Carrera, Gloria Gonzalez Fuster, Elspeth Guild & Valsamis Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*, CTR. FOR EUR. POLICY STUDIES (July 2015), https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf.

210. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

211. The SCA is part of the Electronic Communications Privacy Act (ECPA), and regulates law enforcement access to content communications when in the possession of a provider of electronic communications service (ECS) or remote computing service (RCS) to the public. Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

212. In re *Warrant*, 15 F. Supp. 3d at 472.

213. *Id*. at 471–72.

warrant issued by the magistrate judge. The district court denied Microsoft's motion and explained that with the SCA, Congress intended for electronic communications providers to produce any information under their control, including information stored abroad.[214]

Microsoft contested the district court decision on two grounds: first, that the records are stored in a datacenter in a foreign country and are not owned by Microsoft, but rather by the email user, and second, that the order entails a conflict of laws and the impermissible exercise of extraterritorial authority.[215] The U.S. government has argued that there is no conflict of laws and that the United States retains the authority to order an entity within its jurisdiction to repatriate records. According to the U.S. government, "the power of compelled disclosure reaches records stored abroad so long as there is personal jurisdiction over the custodian and the custodian has control over the records."[216] From this viewpoint, Microsoft, as a company based in the United States, enjoys "corporate citizenship" to which are attached some responsibilities, including the duty to comply with a disclosure order issued by a U.S. court.[217]

An amicus curiae brief presented by a member of the European Parliament in support of Microsoft argues that the company could be allowed to transfer the data through the procedures established in the Mutual Legal Assistance Treaty (MLAT), but not directly from Microsoft to U.S. authorities.[218]

Ireland also submitted an amicus brief, observing that foreign courts should respect Irish sovereignty,[219] and stating that it "would be pleased to consider, as expeditiously as possible, a request under the treaty [the Criminal Justice (Mutual Assistance) Act], should one be

---

214. *Id.* at 472.

215. Microsoft has been joined by nine amici curiae comprised of two members of the European Parliament, technology and media companies, trade associations and civil society, and representatives from the academic community. *See* Brief for Brennan Center for Justice at NYU School of Law et al. as Amici Curiae Supporting Appellant, Microsoft v. U.S., No. 14-2985 (2d Cir. Dec. 15, 2014); Brief for Ir. as Amicus Curiae Supporting Appellant, Microsoft v. U.S., No. 14-2985 (2d Cir. Dec. 23, 2014).

216. Brief for the U.S. at 9, Microsoft v. U.S., No. 14-2985 (2d Cir. Mar. 9, 2015).

217. *Id.* at 57.

218. Brief for Jan Philipp Albrecht, member of Eur. Parl. as Amicus Curiae Supporting Appellant at 9, Microsoft v. U.S., No. 14-2985 (2d Cir. Dec. 19, 2014).

219. Brief for Ir., *supra* note 215, at 3.

made."[220] Noting a case where the Supreme Court of Ireland held that it was lawful for Irish taxation authorities to order an Irish bank to produce records of accounts held by its customers,[221] the brief explains that only "*in the absence of alternative means*" shall an Irish court order the production of records from an Irish entity on foreign soil.[222]

An amicus brief presented by Digital Rights Ireland Limited ("DRI"), Liberty, and the Open Rights Group, underlines that the EU MLAT must be regarded as "self-executing" in U.S. law, and thus affects previous U.S. law without requiring any further legislation.[223] Stressing the mandatory need to follow the MLAT provisions, the brief notes that "[a]dopting the U.S. position would allow the U.S. government to unilaterally substitute U.S. court compulsion for the balancing process represented by the MLAT information request procedures."[224]

The U.S. government, however, argues that using MLAT would not be effective, as the data could quickly be moved to a different country, and because mutual legal assistance procedures are lengthy and do not result in a prompt disclosure of records.[225] The validity of this argument is contested in the DRI and others' amici briefs, which argue that mutual legal assistance between the United States and Ireland functions efficiently and which stress that "European law does not block the disclosure of information to foreign law enforcement authorities so long as there are sufficient protections of individual rights within the mechanism for such disclosure."[226]

Any transfer of personal data must occur only if it is in compliance with EU law. A key legal instrument in this context is the EU-U.S. Agreement on Mutual Legal Assistance ("MLA"), which was signed, together with a parallel transatlantic agreement on extradition, in 2003.[227] The agreement imposes a series of obligations

---

220. *Id.* at 4. For the text of the Act, *see* Criminal Justice (Mutual Assistance) Act 2008 (Act No. 7/2008) (Ir.).

221. Walsh v. Nat'l Irish Bank, [2013] IESC 4 (Ir.).

222. Brief for Ir., *supra* note 215, at 6.

223. Brief for Digital Rights Ir. Ltd. et al. as Amici Curiae Supporting Appellant at 18–20, Microsoft v. U.S., No. 14-2985 (2d Cir. Dec. 15, 2014).

224. *Id*. at 25.

225. Brief for the U.S., *supra* note 216, at 51–52.

226. Brief for Digital Rights Ir. Ltd. et al., *supra* note 223, at 13.

227. Agreement on Extradition between the E.U. and the U.S., Jul. 19, 2003 O.J. (L 181) 27; Mutual Legal Assistance Agreement, *supra* note 169; *see also* Council Decision Concerning the Signature of the Agreements between the E.U.

upon EU member states stemming from EU law. While the agreement supplements bilateral agreements, these do not operate in isolation from EU law. The EU law dimension is visible throughout the MLA agreement: member states will coordinate within the European Council;[228] it will "ensure that the provisions of this Agreement are applied in relation to bilateral mutual legal assistance treaties between the Member States and the United States of America";[229] it will "ensure that the provisions of this Agreement are applied in the absence of a bilateral mutual legal assistance treaty";[230] and it will ensure that the parties to the Agreement consult, as necessary, "to enable the most effective use to be made of this Agreement."[231] In addition, the non-derogation clause of Article 13 states:

> [T]his Agreement is without prejudice to the invocation by the requested State of grounds for refusal of assistance available pursuant to a bilateral mutual legal assistance treaty, or, in the absence of a treaty, its applicable legal principles, including where execution of the request would prejudice its sovereignty, security, public order, or other essential interests.[232]

The agreement should be interpreted consistently with the requirements of EU constitutional and human rights law, including, in particular, the provisions of the EU Charter of Fundamental Rights. The agreement itself contains a specific provision on data protection, Article 9, which aims to facilitate the exchange of data between the United States and the EU to the broadest extent possible, despite their differences in privacy protection.[233] The purpose announced in the

---

and the U.S. on Extradition and Mutual Legal Assistance in Criminal Matters, 2003/516 2003 O.J. (L 181) 25 (EC).

228. Council Decision Concerning the Signature of the Agreements, *supra* note 227, art. 2(2).

229. Mutual Legal Assistance Agreement, *supra* note 169, art. 3(1).

230. *Id.* art. 3(3)(a).

231. *Id.* art. 11.

232. *Id.* art. 13.

233. *Id.* art. 9. Article 9(1) states:

> The requesting State may use any evidence or information obtained from the requested State: (a) for the purpose of criminal investigations and proceedings; (b) for preventing an immediate and serious threat to its public security; (c) in its non-criminal judicial or administrative proceedings directly related to investigations or proceedings: (i) set forth in subparagraph (a); or (ii) for which mutual legal assistance was rendered under

agreement is so broad that it is doubtful that it meets the fundamental EU data protection principle of purpose limitation.[234] Data protection is weakened further by Article 9(4), which allows a state to apply the use limitation provision of the applicable bilateral mutual legal assistance treaty in lieu of Article 9 of the agreement, where doing so will result in less restriction on the use of information.[235] Article 9(2) further weakens the already limited data protection framework: while its first part (Article 9(2)(a)) allows states to request additional safeguards in order to comply with a request, its second part (9(2)(b)) posits that the requested state may not impose the legal standards of the requesting state for processing personal data as a condition under subparagraph (a) for providing evidence or information.[236] This is an attempt to ensure that concerns with regard to U.S. data protection law will not constitute a barrier to cooperation under the Mutual Legal Assistance Agreement.[237]

It is questionable whether these provisions are compatible with EU law. They raise major concerns, especially in light of recent

---

> Article 8; (d) for any other purpose, if the information or evidence has been made public within the framework of proceedings for which they were transmitted, or in any of the situations described in subparagraphs (a), (b) and (c); and (e) for any other purpose, only with the prior consent of the requested State.

234. According to Article 1 of the MLA Agreement, its stated purpose is "to provide for enhancements to cooperation and mutual legal assistance." *Id.* art. 1.

235. *Id.* art. 9(4).

236. *Id.* art. 9(2).

237. In order to ensure that full cooperation takes place notwithstanding these concerns, the explanatory note to the agreement states:

> Article 9(2)(b) is meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases . . . . A broad, categorical, or systematic application of data protection principles by the requested State to refuse cooperation is therefore precluded. Thus, the fact the requesting and requested States have different systems of protecting the privacy of data (such as that the requesting State does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting State uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), may as such not be imposed as additional conditions under Article 9(2a).

Id.

revelations of breaches of privacy by the NSA.[238] The Treaty on the Functioning of the European Union ("TFEU") emphasizes that everyone has the right to the protection of personal data concerning them and calls for the adoption of further EU data protection rules, compliance with which must be subject to the control of independent authorities.[239] The EU–U.S. MLA Agreement is at odds with the Lisbon requirement for an independent data protection supervisory authority. As the ECHR makes clear, data protection is central to the Charter. In particular, Article 7 of the Charter establishes the right to respect for private and family life, while Article 8 establishes a specific right to personal data protection.[240] According to Article 8(2), such data must be processed for *specified* purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.[241] The EU–U.S. MLA Agreement also falls afoul of the ECHR because the agreement does not specify the purpose of the data collected. To avoid breaching any right to privacy, member states should only implement the MLA Agreement in conformity with the ECHR, including judicial decisions, like *Digital Rights Ireland*, interpreting the ECHR's import for data collection.

In light of the above analysis, the approach by Microsoft is noteworthy. The company asked a federal appeals court in September 2015 to block the U.S. government from forcing the company to hand over a customer's emails stored on a server in Ireland, warning that the precedent would create a "global free-for-all" that eviscerates personal privacy.[242] Since then, Microsoft announced that it would allow foreign customers to hold data in European facilities under the control of Deutsche Telekom, a German telecommunications group.[243] "The legal and technical arrangement is intended to put the data of European government and business customers, along with millions of citizens, completely out of reach from U.S. authorities."[244] It is an

238. *See Mitsilegas*, *The Transformation of Privacy in an Era of Pre-Emptive Surveillance*, *supra* note 1.

239. Treaty on the Functioning of the European Union, *supra* note 105, art. 16.

240. EU Charter of Fundamental Rights, *supra* note 95, art. 7, 8.

241. *Id.* art. 8(2).

242. *Microsoft Challenges Warrant for Emails Stored in Ireland*, N.Y. TIMES, Sept. 10, 2015, http://www.nytimes.com/2015/09/10/technology/microsoft-challenges-warrant-for-emails-stored-in-ireland.html.

243. *Microsoft Unveils New Data Plan to Tackle US Internet Spying*, IRISH TIMES, Nov. 12, 2015, http://www.irishtimes.com/business/technology/microsoft-unveils-new-data-plan-to-tackle-us-internet-spying-1.2426877.

244. *Id*.

attempt by Microsoft to ensure maximum legal certainty by firmly and unambiguously placing the location of personal data under EU law.

V. ADDRESSING PRIVACY CONCERNS WITHIN THE TRANSATLANTIC SECURITY COOPERATION FRAMEWORK

Negotiations about transatlantic counterterrorism cooperation (and in particular the EU-U.S. PNR and TFTP Agreements) have been fraught with controversy stemming from concerns in Europe regarding the adverse effect that these agreements would have on the right to privacy. To address these concerns, the agreements themselves have introduced a number of safeguards, most notably safeguards related to oversight and review. In addition, the agreements have included elements of mutual recognition and attempts to internalize and globalize the U.S. security model. This section will analyze and critically evaluate each of these efforts in turn.

A. Addressing Privacy Concerns through Governance: The Establishment of Oversight and Review Mechanisms[245]

1. Oversight

Both the TFTP and the PNR agreements include oversight mechanisms.[246] To address concerns regarding the extensive scope of transfer of financial data to U.S. authorities, a key innovation in the EU-U.S. TFTP agreement has been to embed EU mechanisms of oversight into the operational aspects of the transfer of SWIFT data to the United States. Establishing EU operational oversight mechanisms was central to the negotiating position of the European Parliament for the second TFTP agreement.[247] The agreement does provide for operational oversight, though not by a judicial authority, as the European Parliament wanted, but by Europol.[248] According to Article 4(4) of the agreement, upon receipt of a request for data transfer,

245. This section expands and updates the analysis in Mitsilegas, *Transatlantic Counter-terrorism Cooperation and European Values: The Elusive Quest for Coherence*, *in* A TRANSATLANTIC COMMUNITY OF LAW 289 (D. Curtin & E. Fahey eds., 2014).

246. TFTP Agreement, *supra* note 192, art. 4; EU-U.S. PNR Agreement, *supra* note 132, art. 14.

247. EUR. PARL. DOC. (B7-0243) 10 (2010).

248. TFTP Agreement, *supra* note 192, art. 1(b).

Europol will verify whether the request complies with the requirements of Article 4(2), which requires requests by U.S. authorities to identify as clearly as possible the data necessary for counterterrorism purposes, to substantiate clearly the necessity of the data, and to be tailored as narrowly as possible in order to minimize the amount of data requested.[249] According to Article 4(5), once Europol has confirmed that the request complies with the requirements of 4(2), the request will have binding legal effect within the EU as well as in the United States, and the Designated Provider (SWIFT as indicated in the annex to the agreement) is thereby authorized and required to provide the data to the U.S. Treasury Department.[250] Europol thus acts as a gatekeeper, whose approval is essential in order to authorize the transfer of SWIFT data to the United States. This represents a significant move from private oversight of the transfer of private personal data to the state to public oversight by a European body.[251]

Conferring these oversight powers upon Europol constitutes a change to its traditional role and represents an extension of Europol's powers.[252] In addition to concerns about the enhancement of Europol's powers, there are also efficiency and human rights concerns associated with Europol's role under the agreement. Europol is a law enforcement body with a clear security mandate.[253] The TFTP agreement has thus entrusted the scrutiny of U.S. security services to their EU security/law enforcement counterparts. This choice has given rise to allegations that Europol is unduly favorable toward requests from U.S. authorities, and that this has led to inadequate and ineffective oversight. The fact that Europol has not rejected a single U.S. request supports these allegations.[254]

---

249. *Id.* art. 4(4).

250. *Id.* art. 4(5).

251. Anthony Amicelle, *The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the 'SWIFT Affair'* 20 (Centre de Recherches Internationales, SciencesPo, Res. Questions No. 36, May 2011).

252. *See* Council Decision of 6 April 2009 Establishing the European Police Office (2009/371/JHA), art. 5, 2009 O.J. (L 121) 37, 39 [hereinafter Europol Decision]; *see also* Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and Repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final, March 27, 2013 (EC).

253. Europol Decision, *supra* note 252, art. 3.

254. Nikolaj Nielsen, *EU Hands Personal Data to US Authorities on Daily Basis*, EU OBSERVER, June 22, 2012, https://euobserver.com/justice/116719.

Concerns about Europol are exacerbated after reading Europol's report to the European Parliament on its role under Article 4.[255] In its report, Europol adopts a rather flexible approach with regard to the purpose limitation and specificity requirements of the agreement: according to Europol, identifying a nexus to terrorism in specific cases is a requirement under other provisions in the agreement "*and forms no part of the request as submitted by the US Department of the Treasury to the Designated provider under Article 4*."[256] Moreover, the report notes:

> Due to the specific construction of the TFTP Agreement the US authorities must demonstrate a concrete nexus to terrorism in individual cases only in the context of the individual searches under 5(5) of the TFTP Agreement, once the received data are used for concrete search and/or analysis activities etc. Consequently Article 4(2) of the TFTP Agreement does not prohibit that the requests received by Europol exhibit a certain level of abstraction.[257]

These assertions by Europol are contrary to the very architecture of the agreement, to the purpose of the safeguards inserted therein, and to the wording of Article 4(2). In particular, Article 4(2) requires U.S. requests to "identify as clearly as possible the data . . . that are necessary for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing."[258] Requests must also "be tailored as narrowly as possible in order to minimise the amount of data requested."[259]

The willingness of Europol to accommodate broad requests from U.S. security services conforms to the theory of the socialization of transnational security professionals as developed by Professor Didier Bigo. According to Bigo, the transnationalization of bureaucracies has created a socialization and a set of differentiated

---

255. *See generally Europol Activities in Relation to the TFTP Agreement: Information Note to the European Parliament*, EUROPOL 1 (Apr. 8, 2011), http://www.statewatch.org/news/2012/jun/eu-usa-tftp-europol-2012.pdf (describing Europol's activities under the TFTP agreement between August 2010 and April 2011).

256. *Id.* at 4 (emphasis added).

257. *Id.* at 7.

258. TFTP Agreement, *supra* note 192, art. 4(2)(a).

259. *Id.* art. 4(2)(c).

professional interests that take priority over national solidarities.[260] This reasoning can apply by analogy to EU solidarities: Europol demonstrates greater solidarity with their U.S. security counterparts rather than with the interests of EU citizens, parliamentarians, and data protection/privacy professionals.

In addition to the operational oversight entrusted to Europol when U.S. requests are received, the EU-U.S. TFTP agreement provides for a second level of operational oversight in the United States. The agreement requires oversight of the data protection and purpose limitation safeguards set out in the agreement "by independent overseers, including by a person appointed by the European Commission, subject to him having appropriate security clearances by the US."[261] According to Article 12(1), such oversight includes "the authority to review in real time and retrospectively all searches made of the Provided Data . . . and, as appropriate, to request additional justification of the terrorism nexus."[262] "In particular, independent overseers . . . have the authority to block any or all searches that appear to be in breach of Article 5 [of the agreement]," which establishes a series of safeguards for the processing of data.[263] Article 12(2) of the agreement further provides that "[t]he Inspector General of the U.S. Treasury Department will ensure that the independent oversight described in paragraph 1 is undertaken pursuant to applicable audit standards."[264] This provision can be seen as an attempt to address EU calls for the establishment of a system of independent data protection supervision in the United States, which would reflect the system established under EU law.[265] It is doubtful that the Treasury audit mentioned in Article 12 is equivalent to independent data protection supervision. However, it constitutes an attempt—together with the innovative mechanism of locating an EU-appointed official in the United States with specific powers of operational oversight—to enhance oversight and meet EU requirements.

---

260. *See* Didier Bigo, *Globalized (in)Security: The Field and the Ban-opticon*, *in* TERROR, INSECURITY AND LIBERTY: ILLIBERAL PRACTICES OF LIBERAL REGIMES AFTER 9/11 10 (Didier Bigo & Anastassia Tsoukala eds., 2008).

261. TFTP Agreement, *supra* note 192, art. 12(1).

262. *Id.*

263. *Id.* art. 12(1), 5.

264. *Id.* art. 12(2).

265. *See Op. of the Eur. Data Prot. Supervisor*, *supra* note 197, at ¶ 36.

Unlike the EU-U.S. TFTP agreement, which includes provisions on operational oversight by EU authorities, the agreement on PNR entrusts such oversight exclusively to U.S. authorities. According to Article 14(1), compliance with the privacy safeguards in the agreement is "subject to independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer, who . . . have the power to refer violations of law related to this Agreement for prosecution or disciplinary action, when appropriate."[266] In addition to this specific oversight mechanism, Article 14(2) provides for independent review and oversight by one or more of the following: DHS Office of Inspector General, the Government Accountability Office, and the U.S. Congress.[267] These oversight mechanisms are more related to transparency than to operational controls: according to Article 14(2), "[s]uch oversight may be manifested in the findings and recommendations of public reports, public hearings, and analyses."[268]

2. Regular Monitoring and Review

Another mechanism to ensure that the safeguards set out in the PNR and TFTP agreements are met is the joint review of these agreements on a regular basis. Under the TFTP agreement, both the EU and the United States monitor the effectiveness of the safeguards, controls, and reciprocity provisions set out in the agreement.[269] Article 13(2) sets out in greater detail the areas to be covered by the review, including:

> (a) the number of financial payment messages accessed, (b) the number of occasions on [sic] which leads have been shared with Member States, third countries, Europol, and Eurojust, (c) the implementation and effectiveness of this Agreement, including the suitability of the mechanism for the transfer of information, (d) cases in which the information has been used for the prevention, investigation, detection, or prosecution of terrorism or its financing, and (e) compliance with the data protection obligations specified in this Agreement.[270]

---

266. EU-U.S. PNR Agreement, *supra* note 136, art. 14(1).
267. *Id*. art. 14(2).
268. *Id*.
269. TFTP Agreement, *supra* note 192, art. 13(2).
270. *Id*.

The review includes both a representative and a random sample of searches and a proportionality assessment.[271] "For the purposes of the review, the European Union shall be represented by the European Commission, and the United States by the U.S. Treasury."[272] Each party's delegation may include experts in security, data protection, and the law, but only the EU delegation must include two data protection authorities, one of which must be from a member state where a designated provider, like SWIFT, is located.[273] "Following the review, the European Commission will present a report to the European Parliament and the Council on the functioning of this [TFTP] Agreement . . . ."[274]

The joint review envisaged by the TFTP agreement is an important transparency tool and brings into the public domain a variety of information on the detailed functioning of the agreement. The Commission Report on the first joint review made a number of recommendations for improvement, including: (1) the need to further substantiate the added value of the TFTP program (in particular via the collection and analysis of more feedback in order to provide more verifiable insights into the actual added value of the TFTP); (2) the collection of more statistical information that would be made public; and (3) the provision of as much information as possible about the requests provided to Europol.[275]

The second joint review has proven to be more controversial. In it, the Commission chose to report on parallel scrutiny efforts conducted by Europol's Joint Supervisory Body on Data Protection ("JSB") TFTP agreement.[276] The JSB has produced a number of critical reports highlighting gaps in data protection and Europol's scrutiny role, including the fact that Europol approved requests even when they lacked specificity, as well as gaps in transparency and scrutiny

---

271. *Id*.
272. *Id.* art. 13(3).
273. *Id*.
274. *Id.* art. 13(2).
275. *Commission Report on the Joint Review Report 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*, SEC (2011) 438 final (Feb. 17–18, 2011).
276. *Second Joint Review of the Implementation of TFTP*, *supra* note 202.

resulting from the persistent informality in the practices of Europol.[277] The JSB has also highlighted the secrecy surrounding aspects of the scrutiny of the TFTP Agreement, noting that, "due to Europol's classification of most TFTP-related information as EU SECRET, the JSB's final report is classified as EU SECRET."[278] In its third report, the JSB welcomed progress made after its two prior inspections, but sustained its focus on the practices of Europol and highlighted the continuation of the transfer of personal data in bulk.[279]

The Commission Report on the second joint review criticized, instead of applauding, the additional layer of data protection scrutiny provided by the Europol JSB, noting that "parallel or uncoordinated initiatives or inquiries should be avoided because they undermine the Article 13 review process and have caused considerable workload of the Treasury in particular."[280] This comment can be seen as a response to the U.S. government's concerns over the perceived interference and increased transparency that scrutiny by the Europol JSB may entail.[281] The text of the Commission Report on the joint review reveals an alignment of the Commission's interests not with other EU bodies and actors, but with the U.S. government, in a striking example of security socialization.

---

277. Europol Joint Supervisory Body, *Report on the Inspection of Europol's Implementation of the TFTP Agreement*, Report No. JSB/Ins. 11-07 (Mar. 4, 2011) (noting that Europol admitted that information provided orally, of which there is no record, plays a role in its verification of each request).

278. Europol Joint Supervisory Body, Europol JSB Inspects for the Second Year the Implementation of the TFTP Agreement, INFORMACIJSKI POOBLAŠČENEC (Mar. 22, 2012), https://www.ip-rs.si/en/news/europol-jsb-inspects-for-the-second-year-the-implementation-of-the-tftp-agreement-1086/.

279. Europol Joint Supervisory Body, Implementation of the TFTP Agreement: Assessment of the Follow-Up of the JSB Recommendations, EUROPEAN PARLIAMENT (Mar. 18, 2013), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/jsb_inspection_rep2013/JSB_inspection_rep2013EN.pdf.

280. *Second Joint Review of the Implementation of TFTP*, *supra* note 202, at 15–16.

281. *Id*. at 16 ("During the review, as on previous occasions, the Treasury expressed serious concerns and legal doubts about how the JSB has carried out TFTP-related inspections and communicated on those inspections. This relates in particular to the JSB's decision from mid-October 2012 to grant access to its classified second inspection report to members of the European Parliament's LIBE committee without Europol's and the Treasury's prior consultation and consent, which is considered a clear violation of applicable secrecy rules and a breach of mutual trust.").

The Commission's willingness to uphold security interests and to justify the securitized function of Europol as an overseer of the agreement can also be found in the second joint review. According to the review, Europol has established an intensive dialogue with their Treasury counterparts, which has become an integral monitoring element, in addition to the formal regular reviews under Article 13.[282] It is striking that Europol's perceived data protection role is here applauded at the same time as the work of the data protection scrutineer *par excellence*, the Europol JSB, is being criticized.

The security focus of the Commission is also visible in its evaluation of the performance of Europol under Article 4. While the review accepts that in no cases did verification by Europol lead to a rejection of a U.S. request,[283] the Commission Report stresses and justifies the operational considerations underpinning Europol's role under the agreement. According to the Commission:

> Europol explained to the review teams that it carries out its verification task under Article 4 based on an *operational* assessment of the validity of the US request . . . The fact that the verification task under Article 4 has been given to Europol, i.e. to a law enforcement and not to a data protection body, shows that, ultimately, the verification criteria set out in Article 4 have to be assessed in the light of operational considerations and security needs. This is particularly true for the difficult question whether the US requests are "*as narrowly tailored as possible*" . . . .[284]

These comments by the Commission create concern about the extent to which scrutiny by Europol under Article 4 can operate as an effective safeguard and meaningful control of U.S. requests for financial data under the TFTP agreement. The second joint review remains essentially uncritical as regards the oversight approach adopted by Europol. According to the Commission, the review teams felt that "it is not for them (not for any other monitoring body) to replace Europol's final decision by their own less informed judgement."[285] Here, the emphasis is placed again on security, with the reviewers exhibiting undue deference to Europol's operational considerations placed within a securitized framework and

---

282. *Id*.
283. *Id.* at 6.
284. *Id*. at 7.
285. *Id*.

demonstrating a confluence between EU and U.S. law enforcement interests. Securitization is here linked with depoliticization, with the review team in essence negating the review task entrusted to it by the TFTP agreement. This depoliticization is accepted explicitly in the Commission's report, noting that the second review was based on the understanding that *it was not its task to provide a political judgment of the agreement*, this being considered outside the scope and mandate under Article 13.[286] At the same time, the review of the agreement was accompanied by great efforts to accommodate U.S. concerns with regard to maintaining secrecy[287] and limiting the amount of information provided during the review[288] while producing a report that would be acceptable to the Treasury.[289]

The preamble to the new EU-U.S. PNR agreement recognizes the importance of the joint review mechanism to the development of a transatlantic PNR legal framework.[290] The agreement provides for a joint review one year after its entry into force and at regular intervals thereafter for a period of four years (which resulted in joint reviews in 2005 and 2010).[291] The European Commission represents the EU, and DHS represents the United States. The teams may include appropriate experts on data protection and law enforcement.[292] The EU will scrutinize in particular the onward transfer of PNR data by the United States to third countries.[293] As with the TFTP agreement review

---

286. *Id*. at 4.

287. *Id*. at 3.

288. *Id*. at 5–6 (stating that "as during the first review, the US side did not disclose concrete figures on data volumes" and "assessing the added value of the TFTP and communicating clearly and openly about the implementation of the programme and the Agreement can only be done in so far as this does not jeopardise the on-going value and integrity of the programme. The Treasury has on many occasions expressed its concern to ensure that no sensitive or classified details of the programme should become public as this could harm the effectiveness of the programme.").

289. *See id*. at 4 ("Finally, it should be clarified that this report was prepared by, and reflects the views of the EU review team, based on the work of the joint review and other work independently conducted on the EU side. However the modalities for the second review and the procedure for the issuance of this report *were agreed with the Treasury,* including an opportunity for the latter to conduct a prior check of this report for the purpose of identifying any classified or sensitive information that could not be disclosed in public.").

290. EU-U.S. PNR Agreement, *supra* note 136.

291. *Id*. art. 23(1).

292. *Id*. art. 23(2).

293. *Id*.

mechanism, the joint review provides welcome transparency about the implementation of the agreement.

Joint review does not necessarily lead to joint reporting, however. In 2010, the Commission produced a report, but emphasized that it was not a joint report of the EU and U.S. teams.[294] The Commission Report provided insights on the use of PNR data by the DHS, stating that PNR provides the DHS with the opportunity to perform risk assessments on the basis of scenario-centered targeting rules in order to identify the "unknown" potential high risk individuals.[295] It also raised concerns regarding the broad use of PNR data and, in particular, the matching of PNR against immigration and customs databases.[296] The Commission's report confirms the challenges that the transfer of PNR data to DHS poses for the protection of privacy and personal data, as well as for the relationship between the individual and the state.

B. Addressing Concerns via Adequacy and Mutual Recognition

A key and tested technique in attempting to address concerns over the limitations of the U.S. data protection framework has been for the EU to declare that U.S. standards on privacy and data protection are adequate. Article 8 of the EU-U.S. TFTP agreement states that, subject to ongoing compliance with the commitments to privacy and protection of personal data set out in the agreement, the U.S. Treasury Department is deemed to ensure an adequate level of data protection for the purposes of the agreement.[297] This declaration is a demonstration of trust toward U.S. authorities and must be read together with the preambular provision stressing the parties' "common values governing privacy."[298] It serves to legitimize the transfer of

---

294. Eur. Comm'n, *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 PNR data by Air Carriers to the United States Department of Homeland Security*, 8506/10 (Apr. 15, 2010) [hereinafter *2010 Comm'n Report on the Implementation of PNR*].

295. *Id*. at 4.

296. *Id*. at 9.

297. TFTP Agreement, *supra* note 192, art. 8.

298. *Id*. at Preamble of the Agreement, recital 8. *See also id*. at recital 10 (noting the rigorous controls and safeguards utilized by the U.S. Treasury Department for the handling, use, and dissemination of financial payment messaging data pursuant to the TFTP).

personal data to the United States, but whether the U.S. system provides an adequate level of data protection and privacy standards remains an open question.

To support the assertion of adequacy, the EU-U.S. TFTP agreement includes a number of data protection safeguards. In addition to the safeguards included in relation to U.S. requests, the agreement provides safeguards applicable to the processing of provided data, including purpose limitation, the prohibition of data mining, the prohibition of interconnection of provided data with other databases, the requirement to respect necessity and proportionality in data processing, and the requirement for all searches of provided data to be based upon preexisting information or evidence that demonstrates a reason to believe that the subject of the search has a nexus to terrorism or its financing.[299] The agreement also includes specific provisions on data retention and deletion, with Article 6(4) stating that all non-extracted data received on or after July 20, 2007 shall be deleted not later than five years from receipt.[300] However, as has been noted in the Commission's report on the second joint review to the agreement, the Treasury Department informed the EU review team that the deletion of data could not be implemented as an ongoing process on a rolling basis, but would instead be carried out after longer time intervals.[301] The agreement also includes a series of provisions on specific data protection rights, including transparency,[302] the right of access,[303] the right to rectification, erasure, or blocking,[304] the maintenance of the accuracy of the information,[305] and a provision of redress.[306]

The EU-U.S. PNR agreement contains a number of specific data protection provisions, including provisions on data security,[307] sensitive data,[308] nondiscrimination,[309] transparency,[310] access for

299. *Id*. art. 5.
300. *Id*. art. 6.
301. *Second Joint Review of the Implementation of TFTP*, *supra* note 202, at 10.
302. TFTP Agreement, *supra* note 192, art. 14.
303. *Id.* art. 15.
304. *Id*. art. 16.
305. *Id*. art. 17.
306. *Id*. art. 18.
307. EU-U.S. PNR Agreement, *supra* note 136, art. 5.
308. *Id*. art. 6.
309. *Id.* art. 9.
310. *Id*. art. 10.

individuals,[311] and correction and rectification.[312] Of particular significance is the provision on profiling, according to which the United States may not make decisions based solely on automated processing and use of PNR that produce significant adverse actions affecting the legal interests of the individuals.[313] The agreement also provides a specific provision on redress,[314] but this provision has limited effects.[315]

In addition to these specific data protection standards, the PNR agreement attempts to ensure mutual recognition, first by stating that the agreement complies with fundamental rights, and then by describing the U.S. data protection framework as adequate.[316] According to Article 19 of the EU-U.S. PNR agreement, for the purposes of the agreement and its implementation, DHS will be deemed to provide, within the meaning of relevant EU data protection law, an adequate level of protection for PNR processing and use.[317] This declaration of adequacy is designed to reassure carriers obliged to provide data to the U.S. and creates a presumption of compliance with EU law. According to Article 19, carriers that provide PNR to DHS in compliance with the agreement will be deemed to have complied with the applicable legal requirements of the EU related to the transfer of such data from the EU to the U.S.[318] In addition to the declaration of adequacy, the agreement also operates on the basis of presumptions of equivalence in order to allow the onward transfer of PNR data after their transmission to DHS. Article 16 of the agreement on domestic sharing and safeguards states that receiving authorities will afford to PNR "*equivalent or comparable*" safeguards as set out in this Agreement.[319] Article 17(2) states that, apart from emergency circumstances, any transfer of data will occur pursuant to express understandings that incorporate data privacy protections *comparable* to those applied to PNR by DHS.[320] The data protection safeguards of the EU-U.S. PNR agreement itself, rather than the EU internal

311. *Id*. art. 11
312. *Id.* art. 12.
313. *Id*. art. 7.
314. *Id.* art. 13.
315. Elaine Fahey, *Law and Governance as Checks and Balances in Transatlantic Security: Rights, Redress, and Remedies in EU-US Passenger Name Records and the Terrorist Finance Tracking Program*, 32 Y.B. OF EUR. L. 1, 1 (2013).
316. *See, e.g.*, EU-US PNR Agreement, *supra* note 136, art. 19.
317. *Id*.
318. *Id*.
319. *Id.* art. 16(1)(c) (emphasis added).
320. *Id*. art. 17(2).

privacy- and data-protection safeguards, thus form the benchmark of assessment of comparability or equivalence. The presumption of comparability of data protection extends to both other U.S. authorities and third countries, and the assessment of comparability—especially in relation to third countries—is entrusted to the United States.[321]

In *Schrems*, the Court of Justice recently addressed the relationship between mutual recognition, mutual trust, and the protection of fundamental rights in the context of transatlantic cooperation.[322] It found that the level of protection of personal data provided by the United States was inadequate for the purposes of the EU-U.S. safe harbor agreement.[323] The Court of Justice began by providing a definition of the meaning of adequacy in EU law and by identifying the means of its assessment. The court looked at the wording of Article 25(6) of Directive 95/46 on data protection, which provides for the adoption by the European Commission of adequacy decisions concerning the transfer of personal data to third countries.[324] The court stressed that Article 25(6) requires that a third country "*ensures*" an adequate level of protection by its domestic law or its international commitments, adding that the adequacy of the protection ensured by the third country is assessed "for the protection of the private lives and basic freedoms and rights of individuals."[325] The court thus expressly linked Article 25(6) with obligations stemming from the EU Charter of Fundamental Rights: Article 25(6) implements the express obligation in the Charter to protect personal data, and it is intended to ensure that the high level of protection continues where personal data is transferred to a third country.[326] The court recognized that adequacy does not require a third country to ensure a level of protection identical to that guaranteed in the EU legal order.[327] However, the term "adequate level of protection" must be understood as requiring the third country to ensure a level of protection of fundamental rights and freedoms *essentially equivalent* to that guaranteed within the EU.[328] The court explained that, if there were

---

321. *Id*. *See also id*. art. 17(1) (requiring consistency with the terms of the agreement).
322. Schrems, *supra* note 98.
323. *Id.* ¶¶79–98.
324. *Id.* ¶ 68.
325. *Id*. ¶ 70 (emphasis added).
326. *Id.* ¶¶ 72–73.
327. *Id.*
328. *Id.* (emphasis added).

no such requirement, the objective of ensuring a high level of data protection would be disregarded, and this high level of data protection could easily be circumvented by transfers of personal data from the EU to third countries for processing in those countries.[329] The court thus introduced a high threshold of protection of fundamental rights in third countries: not only must third countries ensure a high level of data protection when they receive personal data from the EU, but they must also provide a level of protection which, while not identical, is essentially equivalent to the level of data protection which is guaranteed by EU law.

This finding is extremely important, not only because it confirms the responsibilities of third countries to ensure a high level of protection, but also because it requires data protection to be effective in practice. This approach places a number of duties on the European Commission when assessing adequacy. The Commission is obliged to assess both *the content* of the applicable rules in the third country resulting from its domestic law or international commitments *and the practice* designed to ensure compliance with those rules.[330] Moreover, it is incumbent upon the Commission, after it has adopted an adequacy decision pursuant to Article 25(6), to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified.[331] Such a check is also required when evidence gives rise to a doubt in that regard.[332] The court's conceptualization of adequacy has thus led to the requirement of the introduction of a rigorous and periodical adequacy assessment by the European Commission, an assessment that must focus on whether a level of data protection essentially equivalent to the one provided by the EU is ensured by third countries.

On the basis of these general principles, the court went on to assess the validity of the specific adequacy decision by the European Commission. The court annulled the decision, which had found the level of protection in the U.S. adequate, because the U.S. did not adequately protect the fundamental rights of persons whose personal data was or could be transferred from the European Union to the United States.[333] The court based its ruling largely on the case of

329. *Id*.
330. *Id.* ¶¶ 74–75 (emphasis added).
331. *Id*. ¶ 76.
332. *Id*.
333. *Id.* ¶¶ 87–91.

Digital Rights Ireland[334] and reiterated that legislation permitting public authorities to have access on a generalized basis to the content of electronic communications compromises the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.[335] In this manner, the Court of Justice stressed that generalized, mass, and unlimited surveillance is contrary to privacy and data protection. The court's findings are thus equally applicable to other instances of generalized surveillance, including surveillance permitted under the EU-U.S. PNR and TFTP agreements, both of which involve generalized, indiscriminate surveillance.

C. Addressing Privacy Concerns by Replicating the U.S. Paradigm of Mass Surveillance: From Internalization to Globalization

1. Internalization

A key element in both the TFTP and PNR systems of cooperation between the EU and the United States is the possibility of the EU's internalization of the U.S. system. The European Parliament has suggested the establishment of a TFTP system to facilitate the extraction of the relevant personal data in the EU under a European system.[336] It may also be seen as an effort to minimize European reliance on U.S. intelligence.[337] Article 11 of the agreement states that the Commission will study the possible introduction of an equivalent EU system allowing for a more targeted transfer of data.[338] The agreement also provides that, if the EU decides to establish an EU system, the United States will cooperate and provide assistance and advice to contribute to the effective establishment of such a system.[339] The Commission's report on the second joint review of the agreement indicates that there will continue to be close cooperation and

334. C-293/12 and C-594/12, Digital Rights Ir. Ltd. v. Minister for Commc'ns, Marine and Natural Res. *et al*, 2015 E.C.J. 127.

335. Schrems, *supra* note 98, at ¶ 94.

336. Resolution on the Launch of Negotiations for Passenger Name Record (PNR) Agreements With the United States, Australia and Canada, EUR. PARL. DOC. B7-0244/2010 (2010).

337. Ariadna Ripoll Servent & Alex MacKenzie, *The European Parliament as a 'Norm Taker'? EU–US Relations after the SWIFT Agreement*, 17 EUR. FOREIGN AFF. REV. 71, 83 (2012).

338. TFTP Agreement, *supra* note 192, art. 11(1).

339. *Id.* art. 11(2).

consultation with the United States on this issue,[340] and states explicitly that the functioning of reciprocity under the agreement is an essential factor in assessing the necessity of a possible establishment of an equivalent EU system.[341] In this manner, the EU TFTP system is essentially an alternative if the U.S. authorities do not cooperate sufficiently with the EU under the EU-U.S. TFTP agreement. This is a departure from the European Parliament's rationale for the establishment of an EU system, according to whom the aims of such a system would be to contribute to the fight against terrorism and its financing and to limit the amount of personal data transferred to third countries.[342] The effect of establishing an EU TFTP system will be to import within the EU and legitimize a highly invasive program of executive action, and thus to normalize an emergency security response without questioning the necessity of the mass transfer of everyday financial data to state authorities.

As with the TFTP Agreement, the EU-U.S. PNR agreement envisages the establishment of an EU PNR system. The agreement states that, if and when an EU PNR system is adopted, the parties will consult to determine whether the agreement would need to be adjusted accordingly to ensure full reciprocity. Such consultations would in particular examine whether any future EU PNR system would apply less stringent data protection safeguards than those provided for in the agreement, and whether the agreement should therefore be amended.[343]

The European Commission released a proposed EU PNR system in 2007.[344] The Commission explained that the proposal was a result of the "policy learning" from, inter alia, the existing EU PNR agreements with the United States and Canada.[345] The Commission justified the establishment of a European system of PNR transfer as necessary for law enforcement purposes. It proposed a system that was

---

340. *Second Joint Review of the Implementation of TFTP*, *supra* note 202, at 14. *See also* TFTP Agreement, *supra* note 192, art. 11(3).

341. TFTP Agreement, *supra* note 192, art. 11(3).

342. *Communication from the Commission to the European Parliament and the Council: A European Terrorist Finance Tracking System: Available Options*, COM (2011) 429 final (Jul. 13, 2011).

343. EU-U.S. PNR Agreement, *supra* note 136, art. 20(2).

344. *Commission Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes*, COM (2007) 654 final (Nov. 6, 2007).

345. *Id.* at 2.

very similar to the U.S. PNR system, at least regarding the categories of transferred data[346] and the emphasis on risk assessment.[347] As with the U.S. system, the proposed PNR system carries with it the risk that it would lead to the profiling of individuals.[348] The adoption of the PNR directive faces a rocky road; it was rejected by the Civil Liberties Committee of the European Parliament in the spring of 2013.[349] However, the draft directive constitutes a prime example of the internalization of the U.S. security model by the EU, leading to the lowering of internal EU privacy and data protection standards.[350] The terrorist events in Paris in November 2015 have strengthened calls for the establishment of an internal EU PNR system to address the issue of so-called "foreign fighters," with President Obama praising the benefits of PNR in a recent joint press conference with President Hollande of France.[351] However, the internalization of the U.S. PNR model by the EU will cause challenges to both the right to privacy and to the fundamental EU law principle of free movement. It will internalize in the EU a paradigm of indiscriminate mass surveillance of every individual who exercises movement and mobility in Europe.

---

346. Requested data includes all forms of payment information, including billing address, travel status of passenger (including confirmations), check-in status, no show or go show information, seat number and other seat information, number and other names of travelers on PNR, and "general remarks." *Id.* at 25.

347. *See* Mitsilegas, *Immigration Control in an Era of Globalisation: Deflecting Foreigners, Weakening Citizens, Strengthening the State*, *supra* note 121.

348. *See Op. of the Eur. Data Prot. Supervisor on the Proposal for a Directive of the Eur. Parliament and of the Council on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation, and Prosecution of Terrorist Offences and Serious Crime*, 2011 O.J. (C 181) 24.

349. Press Release, European Parliament, Civil Liberties Committee Rejects EU Passenger Name Record Proposal (Apr. 24, 2013), http://www.europarl.europa.eu/news/en/news-room/20130422IPR07523/Civil-Liberties-Committee-rejects-EU-Passenger-Name-Record-proposal.

350. For more on internalization, see J. Argomaniz, *When the EU Is the "Norm-Taker": The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms*, 31 J. OF EUR. INTEGRATION 119 (2009).

351. President Obama mentioned the need for better intelligence and for sharing passenger name records. Remarks by President Obama and President Hollande of France in Joint Press Conference (Nov. 24, 2015), http://www.whitehouse.gov/the-press-office/2015/11/24/remarks-president-obama-and-president-hollande-france-joint-press.

2. Globalization

The internalization of U.S. paradigms of surveillance is coupled, at least in the case of PNR, with parallel calls for their globalization. In addition to calling for the establishment of an EU PNR system,[352] the European Commission has also called for the development of a global regime for the collection and transfer of PNR data. In its Communication on a Global Approach to Transfers of PNR Data to Third Countries, the Commission called upon the EU to consider initiating discussions with international partners that use PNR data and those that are considering using such data in order to explore the possibility of dealing with PNR transfers on a multilateral level.[353] To justify this move toward multilateralism, the Commission stated:

> As more and more countries in the world use PNR data, the issues arising from such use affect the international community. Even though the bilateral approach which has been adopted by the EU was the most appropriate one under the circumstances and seems to be the most appropriate one for the near future, it risks ceasing to be appropriate if many more countries become involved with PNR. The EU should therefore examine the possibility of setting standards for the transmission and use of PNR data on an international level. The Guidelines on PNR access that have been developed by ICAO in 2004 offer a solid basis for the harmonisation [sic] of the modalities of transmissions of PNR data. However, these guidelines are not binding and they deal insufficiently with data protection issues. They are therefore not sufficient in themselves, but should rather be used for guidance, especially on matters affecting the carriers.[354]

---

352. In addition to the EU PNR agreement, the EU has also concluded an agreement with Australia. *See* Agreement between the European Union and Australia on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the Australian Customs and Border Protection Service, EU-Austl., July 14, 2012, O.J. (L 186) 4. An agreement with Canada has been referred to the Court of Justice by the European Parliament for preliminary check. Opinion 1/15 on Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (pending).

353. *Communication on the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries*, COM (2010) 492 final (Sep. 21, 2010).

354. *Id*. at 10.

The EU is emerging as a global actor aiming to shape global, multilateral standards on PNR transfers. However, in doing so, it legitimizes and accepts the U.S. focus on the generalized surveillance of mobility. This signifies a move from U.S. unilateral emergency action to the internalization of such action in EU law, and then to the development of global standards regulating the transfer of PNR data.

VI. ESTABLISHING A GLOBAL PRIVACY LEVEL PLAYING FIELD: FROM TRANSNATIONAL TO EXTRATERRITORIAL TO GLOBAL PRIVACY STANDARDS

This article has thus far highlighted both the challenges that the post-9/11 paradigm of preemptive, mass surveillance pose to the protection of the right to privacy, as well as the limits of the current legislative responses in the field of security to address these challenges in a meaningful way. The way forward therefore requires a shift in focus from regulatory accommodations of privacy within security measures to the development of concrete norms of privacy, ultimately resulting in the development of a global privacy regime. This section will examine the development of a privacy regime from three perspectives: (1) transatlantic cooperation; (2) extraterritorial jurisdiction and extraterritorial application of human rights norms; and (3) the globalization of privacy protection.

A. Establishing a Transatlantic Privacy Level Playing Field

In 2009, a transatlantic agreement on a series of common data protection principles was reached.[355] This agreement marked the first step toward the establishment of a transatlantic level playing field on privacy. Along with reference to a series of specific data protection standards, the parties aimed to reach a broad understanding of equivalence of data protection taken "as a whole," and not an understanding that is based upon the scrutiny of specific (singular) examples.[356] It is unlikely, though, that such a broad approach to

355. Joint Statement, US Mission to the EU, U.S.–EU Reach Agreement on Common Data Prot. Principles (Oct. 28, 2009), http://useu.usmission.gov/useu_dataagreement_102809.html.

356. *Id.* ("On equivalent and reciprocal application of data privacy law, the European Union and the United States should use best efforts to ensure respect for the requirements, taken as a whole as opposed to singular examples, that each asks the other to observe.").

equivalence will suffice to ensure compliance with EU data protection and privacy standards. What is key to this approach, however, is the focus on mutual recognition of the data protection systems of the EU and the United States based upon the presumption that the systems do in fact offer an acceptable level of protection. However, this presumption has been challenged, most recently by the Court of Justice in the case of *Schrems.*

A step forward, especially in light of *Schrems,* would be the move toward harmonization of privacy standards on a transatlantic level to accompany mutual recognition and underlying presumptions of adequacy. The EU has followed this approach in its harmonization of basic criminal law across member states.[357]

The next step in the transatlantic privacy dialogue would be the creation of a transatlantic agreement on privacy. In 2009, the European Commission adopted a mandate for the negotiation of an EU-U.S. agreement on privacy, which would require a number of data protection safeguards to apply in transatlantic agreements authorizing the transfer of personal data.[358] Negotiations toward a transatlantic privacy agreement in the field started in 2010.[359] According to a joint statement on the negotiation of the agreement by former European Commission Vice-President Viviane Reding and U.S. Attorney General Eric Holder, such an agreement will allow for even closer transatlantic cooperation in the fight against crime and terrorism through the mutual recognition of a high level of protection afforded equally to citizens of both the United States and the EU, and will thus facilitate subsequent agreements concerning the sharing of personal data.[360]

---

357. For a detailed analysis, see VALSAMIS MITSILEGAS, EU CRIMINAL LAW AFTER LISBON: RIGHTS, TRUST AND THE TRANSFORMATION OF JUSTICE IN EUROPE (2016).

358. Press Release, Eur. Commission, European Commission Seeks High Privacy Standards in EU-US Data Protection Agreement (May 26, 2010), http://europa.eu/rapid/press-release_IP-10-609_en.htm?locale=en.

359. ARCHICK, *supra* note 134, at 6 (providing an overview of the contested issues in negotiations).

360. Press Release, European Commission, Joint Statement on the Negotiation of a EU-US Data Privacy and Protection Agreement by European Commission Vice-President Viviane Reding and U.S. Attorney General Eric Holder (June 6, 2012), http://europa.eu/rapid/press-release_MEMO-12-474_en.htm.

The text of the transatlantic privacy agreement, otherwise known as the "Umbrella" agreement, has recently been finalized.[361] Negotiations finished on September 8, 2015 after four years of discussions, and the text is currently awaiting approval from the European Parliament.[362] The agreement sets out data protection standards for the transatlantic exchange of personal information in relation to the prevention, detection, or prosecution of criminal offenses, including terrorism, with a view to ensuring "a high level of protection of personal information," while enhancing cooperation between the United States and the EU and its member states.[363] The agreement "establishes the framework for the protection of personal information *when transferred* between the U.S., on the one hand, and the EU or its member states, on the other."[364] It covers both transfers that take place between criminal law enforcement authorities and transfers that take place pursuant to an agreement between the parties, including agreements providing that private companies may transfer data to a law enforcement authority of the other party.[365] It contains a number of data protection safeguards, including a

361. Although the text of the agreement has been finalized since September 2015, EU and U.S. officials did not disclose its content. The Electronic Privacy Information Center sued the Department of Justice to obtain the agreement. *See* Complaint for Injunctive Relief, Electronic Privacy Info. Ctr. v. U.S. Dep't of Justice, No. 1:15-cv-01955 (D.D.C. Apr. 11, 2015); *see also* Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf [hereinafter Umbrella Agreement].

362. On December 3, 2010, the Council adopted a decision authorizing the Commission to enter into negotiations with the United States for the completion of an agreement on the protection of personal data when transferred and processed for law enforcement purposes. *See Proposal for a Council Recommendation to Authorise the Opening of Negotiations for an Agreement Between the European Union and the United States of America on Protection of Personal Data When Transferred and Processed for the Purpose of Preventing, Investigating, Detecting or Prosecuting Criminal Offences, Including Terrorism, in the Framework of Police Cooperation and Judicial Cooperation in Criminal Matters*, *Annex*, COM (2010) 252 PO/2010/3091. For an overview of the negotiations, see EU–US Data Protection Negotiations Non-Paper on Negotiations During 2011, 5999/12 (Feb. 3, 2012); *see also* EUR. UNION COMM'N SERVS., COMMISSION SERVICES NON-PAPER ON STATE OF PLAY OF NEGOTIATIONS ON EU–US DATA PROTECTION "UMBRELLA AGREEMENT," 8761/14 (2014) [hereinafter NEGOTIATIONS ON EU–US DATA PROT. AGREEMENT].

363. Umbrella Agreement, *supra* note 361, art. 1(1).

364. *Id.* art. 1(2) (emphasis added).

365. *Id*. art. 3.

prohibition of the transfer of data to third parties without the consent of the relevant EU body,[366] and a provision mandating that limitations on retention of the transferred data be established.[367] As with the transatlantic data transfer agreements, it also includes a provision on joint review.[368]

Perhaps one of the most important safeguards introduced by the agreement is the fact that all EU citizens will be entitled to seek the enforcement of their privacy rights before U.S. courts.[369] This was contentious issue for years, with the United States traditionally refusing to grant judicial redress and insisting on administrative redress only.[370] Because the agreement allows individuals who are not U.S. citizens to seek judicial redress in U.S. courts, Congress must pass a Judicial Redress Act to effectuate the agreement (effectively opening U.S. courts to certain non-citizens for the limited purposes set forth in the agreement).[371] The bill successfully passed the House of Representatives on October 20, 2015.[372]

However, there are still elements in the agreement that do not comply with EU law. For example, the preamble to the agreement maintains the existing status quo, with the exception of the issue of judicial redress and the presumption of adequacy in the transatlantic counterterrorism cooperation agreements.[373] This provision of the

---

366. *Id*. art. 7(1).

367. *Id*. art. 12. The Commission claims that these provisions go beyond what is found in most existing agreements. *See* NEGOTIATIONS ON EU–US DATA PROT. AGREEMENT, *supra* note 362, at 6 (requiring that the parties "provide for specific and appropriate retention periods").

368. Umbrella Agreement, *supra* note 361, art. 23.

369. *Id.* art. 19.

370. Peter Schaar, *Leaky Umbrella* EUR. ACAD. FOR FREEDOM OF INFO. AND DATA PROT. (Sep. 18, 2015), http://www.eaid-berlin.de/?p=779.

371. The Judicial Redress Act of 2015, H.R. 1428, 114th Cong. (2015).

372. Peter Sayer, *Judicial Redress Act Heads for Senate, Making New Safe Harbor Agreement More Likely*, PCWORLD (Oct. 21, 2015), http://www.pcworld.com/article/2995935/judicial-redress-act-heads-for-senate-making-new-safe-harbor-agreement-more-likely.html. However, the vote in Congress has been delayed. Lisa Brownlee, *EU-US Safe Harbor: Judicial Redress Act Vote Delayed*, FORBES (Jan. 20, 2016), http://www.forbes.com/sites/lisabrownlee/2016/01/20/eu-us-safe-harbor-judicial-redress-act-vote-delayed/.

373. Umbrella Agreement, *supra* note 361, ¶ 4 ("Recognizing that certain existing agreements between the Parties concerning the processing of personal information establish that those agreements provide an adequate level of data protection within the scope of those agreements, the Parties affirm that this Agreement should not be construed to alter, condition, or otherwise derogate from

agreement thus disregards the rulings of the Court of Justice in *Digital Rights Ireland*[374] and *Schrems*.[375] Those rulings cast serious doubts on the compatibility of the EU-U.S. PNR and TFTP agreements with EU law and—in the case of *Schrems*—demolish the presumption of adequacy enshrined in various transatlantic agreements. The Umbrella Agreement also disregards *Schrems*, stating that "the processing of personal information by the United States, or the European Union and its member states, will be *deemed to comply* with their respective data protection legislation."[376] This presumption of compliance is concerning; instead, it should be rebuttable, and the legality of each transfer and its compliance with human rights should be established on a case-by-case basis.[377] The agreement allows the further sharing of the transferred data with "other authorities," including "authorities of constituent territorial entities of the Parties not covered by this Agreement."[378] Furthermore, provided that certain conditions are met (such as consent of the competent source authority), the agreement provides for downstream transfers of the data to third parties not bound by the agreement.[379]

Even in the two areas where the United States has made systemic concessions to meet EU demands—on the issues of independent supervision and judicial redress—EU law requirements have not been fully met. With regard to independent supervision, the agreement includes an article on "effective oversight," which requires that parties:

> have in place public authorities that: (a) exercise independent oversight functions and powers, including review, investigation, and intervention; (b) have the power to act upon complaints made by individuals

---

those agreements; noting however, that the obligations established by Article 19 of this Agreement on judicial redress would apply with respect to all transfers that fall within the scope of this Agreement, and that this is without prejudice to any future review or modification of such agreements pursuant to their terms.").

374. Digital Rights Ir. Ltd., *supra* note 81.

375. Schrems, *supra* note 98.

376. *Id*. art. 5(3) (emphasis added).

377. Although Article 6 states that the transferring authority may impose additional conditions in a specific case, the agreement then weakens this safeguard by adding that such conditions will "not include generic data protection conditions, that is, conditions imposed that are unrelated to the specific facts of the case." *Id*. art. 6.

378. *Id*. art. 6(2), 14(1)–(2), 20(1)(b).

379. *Id*. art. 7, 20(1)(d).

> relating to the implementation of the Agreement; and (c) have the power to refer violations of the Agreement for prosecution or disciplinary action where appropriate.[380]

However, the United States has stated that it intends to meet this requirement "cumulatively," which does not meet the independent supervision requirements of EU law, including the Charter of Fundamental Rights.[381] Furthermore, regarding judicial redress, the agreement emphasizes that the availability of judicial redress is subject to any requirements that administrative redress first be exhausted.[382] EU citizens thus appear to be in a worse position than U.S. citizens in this context, because they will not be able to choose the means of redress, but rather will be required to follow a separate procedure.[383] Moreover, judicial redress is only available to address violations of the agreement, not to challenge the lawfulness of data processing as a whole.[384] Finally, and most importantly, judicial redress is applicable only to citizens of the parties to the agreement.[385] This approach runs counter to the human rights approach enshrined in the European Convention on Human Rights and in EU law, whereby human rights are applicable to everyone—the agreement instead perpetuates an exclusionary model of human rights protection based on citizenship.

---

380. *Id*. art. 21(1).

381. *See* Schaar, *supra* note 370. According to Article 21(3), "[t]he United States will provide for oversight under this Article cumulatively through more than one authority, which may include, inter alia, inspectors general, chief privacy officers, government accountability offices, privacy and civil liberties oversight boards, and other applicable executive and legislative privacy or civil liberties review bodies." Umbrella Agreement, *supra* note 361, art. 21(3).

382. Umbrella Agreement, *supra* note 361, art. 19.

383. EPIC has argued in favor of the change in the meaning of the term "individual" under the U.S. Privacy Act to ensure equality. *See* Letter from EPIC to Chairman Goodlatte and Representative John Conyers, Jr., U.S. House of Representatives Comm. on the Judiciary (Sept. 16, 2015), https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.

384. *See* Francesca Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, EUR. PARLIAMENT 13–14 (May 2015), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf (identifying the three circumstances under which an EU citizen could sue for judicial redress under the Privacy Act, which do not include a cause of action for challenging the lawfulness of data processing as a whole).

385. Umbrella Agreement, *supra* note 361, art. 19.

The agreement can thus be viewed from two different perspectives: from a pessimistic perspective, the protection offered by the agreement remains limited and, in many respects, provides standards that are different—and at times non-compliant—with EU law. From an optimistic perspective, the agreement is an important step in creating a transatlantic level playing field for privacy. Either way, the provisions of the agreement must be applied and interpreted in conformity with EU constitutional law, including fundamental rights as enshrined in the EU Charter of Fundamental Rights and as interpreted by the Court of Justice.

B. Protecting Privacy through Extraterritoriality

One of the key questions that has emerged in discussions about the human rights challenges posed by mass globalized surveillance is the extent to which the extraterritorial application of human rights law can provide meaningful privacy safeguards. In the United States, this question can be framed within the context of the discussion about the extraterritorial application of the Constitution.[386] The Supreme Court held in *Boumediene v. Bush* that, based on the specific facts of that case, the Constitution applies to enemy combatant detainees held at Guantanamo Bay.[387] This case represents an important step in establishing the extraterritorial application of the U.S. Constitution.[388] As Professor Sarah Cleveland has noted, *Boumediene* does not go as far as international human rights law because it focuses on control over territories, facilities, and proceedings instead of the control exercised over people.[389] Yet, as Cleveland also notes, *Boumediene*'s rejection of formal territorial restrictions and citizenship requirements, and its focus on practical control for determining when constitutional rights limit governmental conduct abroad, largely comport with modern international law's focus on effective control.[390]

Indeed, *Boumediene* brings the U.S. approach to extraterritorial jurisdiction closer to the approach taken by the European Court of Human Rights. In its ruling in *Al-Skeini*, the ECHR

386. *See generally* KAL RAUSTIALA, DOES THE CONSTITUTION FOLLOW THE FLAG?: THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW (2009).

387. Boumedine v. Bush, 553 U.S. 723, 794—95 (2008).

388. Sarah H. Cleveland, *Embedded International Law and the Constitution Abroad*, 110 COLUM. L. REV. 225 (2010).

389. *Id.* at 275.

390. *Id.* at 274.

explained that, in certain circumstances, the use of force by a state agent operating outside the state's territory may thereby bring the individual into the state's jurisdiction.[391] Reiterating its earlier case law, the court noted that "[w]hat is decisive in such cases is *the exercise of physical power and control over the person in question*."[392] In other cases, the court has gone even further and connected the extraterritorial application of the European Convention on Human Rights with the requirement to uphold the rule of law in a number of immigration cases.[393] In *Medvedyev*, the court ruled that the Convention applied extraterritorially in a case of suspected drug trafficking in the high seas.[394] Because France had exercised "full and effective control" over the boat and crew in question, "at least de facto, from the time of its interception, in a continuous and uninterrupted manner until they were tried in France, the applicants were effectively within France's jurisdiction for the purposes of Article 1 of the Convention."[395] The court reiterated these findings in *Hirsi*, which involved the exercise of jurisdiction by Italy, outside its national territory, in the territory of a third state (Libya).[396]

The discussion on the extraterritorial application of the U.S. Constitution and the European Convention on Human Rights is inextricably linked with the broader issue of their application to citizens versus non-citizens. The key difference between the United States on the one hand and the EU and the European Convention on Human Rights on the other is that, in terms of key human rights such as privacy, European instruments provide protection to *everyone*, whereas the U.S. Constitution was designed to protect primarily U.S. citizens.[397] This is perhaps why discussions on the extraterritorial

391. Al-Skeini and Others v. U.K., 53 Eur. Ct. H.R. 589, ¶ 136 (2011).

392. *Id*. (emphasis added).

393. On the extraterritorial application of the ECHR and the concept of "effective control" in the context of immigration cases, see VALSAMIS MITSILEGAS, THE CRIMINALISATION OF MIGRATION IN EUROPE: CHALLENGES FOR HUMAN RIGHTS AND THE RULE OF LAW 5 (2015); Mitsilegas, *Immigration Control in an Era of Globalisation: Deflecting Foreigners, Weakening Citizens, Strengthening the State*, *supra* note 121.

394. Medvedyev and Others v. France, App. No. 3394/03, 51 Eur. H.R. Rep. 39 (2010).

395. *Id*. ¶ 67.

396. Hirsi Jamaa and Others v. Italy, 55 Eur. Ct. H.R. 21 (2012).

397. *See, e.g.*, U.S. v. Vertugo-Urquidez, 494 U.S. 259, 261 (1990) (holding that the Fourth Amendment does not apply to the search and seizure of property overseas, where the person invoking the right is not an American citizen).

application of human rights law in the United States have focused largely on the extraterritorial application not only of the Constitution, but also of the International Covenant on Civil and Political Rights ("ICCPR"). The ICCPR states that each participating state must "respect . . . and ensure to all individuals within its territory and subject to its jurisdiction" the rights provided for in the covenant.[398] At the moment, the United States rejects any extraterritorial reach of the ICCPR's obligations, mainly arguing that the language of the ICCPR limits a state's duty to individuals "within its territory and subject to its jurisdiction."[399] According to this narrow view, the use of the conjunctive "and" signifies that an obligation arises only when both requirements have been satisfied.[400]

This position has been rejected by the Human Rights Committee in its case law and in General Comment No. 31,[401] as well as by the ICJ[402] and most legal scholarship. In particular, Thomas Buergenthal, judge of the International Court of Justice, has noted that this interpretation contravenes other provisions of the

---

398. International Covenant on Civil and Political Rights, art. 2(1), Dec. 16, 1966, 999 U.N.T.S. 171 (emphasis added).

399. U.S. Dep't of State, Second and Third Periodic Reports of the United States of America to the UN Comm. on Human Rights Concerning the International Covenant of Civil and Political Rights, at annex I (2005), http://www.state.gov/j/drl/rls/55504.htm#annex1 [hereinafter Second and Third Periodic Reports to the UN]. *See also* Michael J. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation*, 99 AM. J. OF INT'L L. 119, 123–24 (2005); Ashley Deeks, *Does the ICCPR Establish an Extraterritorial Right to Privacy?*, LAWFARE (Nov. 14, 2013), https://www.lawfareblog.com/does-iccpr-establish-extraterritorial-right-privacy. During the drafting of the covenant, the primary concern of the United States was that an extraterritorial application of ICCPR's rights would signify affirmative duties to enforce a comprehensive framework of rights to citizens of countries that were occupied after World War II. For an overview, see U.N. ESCOR, 6th Sess., 194th mtg. at 5, U.N. Doc. E/CN.4/SR.193 (May 15, 1950); U.N. ESCOR, 6th Sess, 194th mtg., U.N. Doc. E/CN.4/SR.193 (May 16, 1950).

400. Second and Third Periodic Reports to the UN, *supra* note 399.

401. Human Rights Comm. General Comment 31, *Nature of the General Legal Obligation on States Parties to the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (Mar. 29, 2004) [hereinafter General Comment 31].

402. R. Wilde, *Human Rights Beyond Borders at the World Court: The Significance of the International Court of Justice's Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties*, 12 CHINESE J. OF INTERNAT'L L. 639 (2013).

covenant.[403] An alternative reading argues that "and" should be read as "or" in order to achieve the ICCPR's purpose.[404] As a result, a state must respect and observe both the rights of individuals within its territory and those of individuals anywhere under the state's control.[405] A third approach to reading the ICCPR distinguishes duties of a state with respect to people "within its territory" from duties of a state with respect to people "subject to its jurisdiction." Under this reading, a state has the duty to respect the rights of individuals outside its territory but subject to its jurisdiction, while it has the higher duty to *provide* these rights for individuals within the state's territory.[406]

A key issue in determining the extraterritorial application of human rights law in the surveillance context is determining when a state has established "effective control" of an individual beyond the state's borders. Judicial definitions of effective control for the purpose of establishing extraterritorial jurisdiction have traditionally focused on the physical control of persons by a state. Surveillance operations are different. In a digital era, physical control over an individual to perform surveillance is unnecessary.[407] Accordingly, some have argued that "virtual control" (which may constitute surveillance depending on the intensity and scope of the control) should be the relevant standard in the surveillance context instead of effective control.[408] The Office of the United Nations Commissioner for Human Rights, on the other hand, has attempted to apply the effective control standard to surveillance:

> [D]igital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure,

---

403. Thomas Buergenthal, *To Respect and to Ensure: State Obligations and Permissible Derogations*, *in* INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS 72, 74 (Louis Henkin ed., 1981).

404. *Id*.

405. For the adoption of this viewpoint, *see* Al-Skeini and Others v. U.K., 53 Eur. Ct. H.R. 589 (2011); General Comment 31, *supra* note 401.

406. MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION ON HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY (2011).

407. Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2150–52 (2014).

408. Anne Peters, *Surveillance without Borders: The Unlawfulness of the NSA Panopticon, Part II*, EJIL: TALK! (Nov. 1, 2013), http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii/.

> wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty.[409]

To establish the applicability of human rights law in the field of surveillance, territorially or extraterritorially, we must shift our focus from control over the body of a person to control over personal data. Any type of processing of such data, from their initial collection to their further exchange, has a significant negative impact on the right to privacy of individuals. Therefore, the collection, exchange, transfer, processing, and sharing of personal data—together or individually—constitutes both effective control and virtual control, thus triggering the application of the right to privacy.

C. Toward Global Standards: What Should a Global Privacy Regime Include?

The evolution of a transatlantic level playing field for privacy and discussions on the extent of the extraterritorial application of the right to privacy have been accompanied by the realization of the need for global privacy standards to address the globalization of mass surveillance. At the UN level, the General Assembly has adopted a Resolution on the Right to Privacy in a Digital Age, and the post of a UN Special Rapporteur on the Right to Privacy in a Digital Age has since been established.[410] Its first holder, Joseph Cannataci, has called for the establishment of global standards in the form of a "new universal law on surveillance."[411]

---

409. U.N. High Comm'r for Human Rights, *The Right to Privacy in the Digital Age*, ¶ 34, U.N. Doc. A/HRC/27/37 (June 30, 2014).

410. G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Dec. 18, 2013).

411. Adam Alexander, *Digital Surveillance "Worse Than Orwell," Says New UN Privacy Chief*, THE GUARDIAN, Aug. 24, 2015, http://www.theguardian.com/

The adoption of global privacy standards is indeed a necessary way forward to address the current challenges of globalized surveillance. EU law offers lessons and benchmarks for the development of a global privacy regime. First, it is challenging to adopt detailed rules on the right to privacy, whose value lies in its all-encompassing character and its flexibility.[412] Yet it is still possible to establish and protect the right to privacy by adopting more detailed secondary law governing the relevant players; the EU has done just this by creating detailed law on the rights of suspects and the accused in criminal proceedings as a component of the right to a fair trial.[413] Second, a global instrument on privacy must specify that the right to privacy protects everyone, irrespective of citizenship or nationality. Third, a global instrument must provide certainty regarding the demarcation of jurisdictional borders in digital surveillance. Fourth, as with EU law, a global instrument should not be limited to data protection principles but should subsume them within a general right to privacy.

The use of data protection as a regulatory tool for surveillance offers a number of distinct advantages: data protection rules follow and regulate in detail instances of data collection, processing, and exchange; data protection rules have established and developed key substantive legal principles, such as the principle of purpose limitation; data protection focuses on issues of procedural justice by establishing remedies for the data subject; developments in data protection law have led to substantive legislative innovations in the field, including recent proposals of a "right to be forgotten";[414] and last but not least, data protection rules involve expert, dedicated supervisory bodies who advise on legislative developments impacting data protection and who enforce data protection law. However, there are two main limitations on the effectiveness of data protection alone to address the challenges posed by preemptive surveillance.

---

world/2015/aug/24/we-need-geneva-convention-for-the-internet-says-new-un-privacy-chief.

412. For more information on the flexibility of the right to privacy, see DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

413. *See* MITSILEGAS, EU CRIMINAL LAW AFTER LISBON: RIGHTS, TRUST AND THE TRANSFORMATION OF JUSTICE IN EUROPE, *supra* note 352.

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

The first limitation stems from the limited capacity of data protection to question the political choice to maximize and generalize the collection and processing of personal data. Data protection differs from privacy protection because it does not aim to create zones of non-interference by the state, but rather operates on a presumption that public authorities *can* process personal data. Indeed, as some scholars have noted, data protection principles "suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice," with data protection law creating "a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal."[415]

The second limitation of data protection as a way to protect privacy is the different specificity and focus of each. While data protection centers on the various categories of personal data, with the specific information collected and processed being the reference point, privacy focuses on *the person* in terms of identity and the self. The right to privacy thus provides a more holistic framework for assessing the impact of surveillance on the relationship between the individual and the state than data protection does alone. Moreover, the specificity in data protection, while useful in scrutinizing closely various instances of data processing, may lead to fragmentation and ignorance of the large-scale effects of the surveillance, such as profiling and discrimination.[416] A global instrument on the right to privacy should not rely on data protection alone, but should instead use data protection as a way to support a strong general right to privacy. Such an approach is key in the field of mass generalized surveillance, where privacy must embrace not only the processing of personal data, but also its very collection and transfer in the first place.

VII. CONCLUSION: THE CASE FOR A GLOBAL PRIVACY REGIME: FOUR KEY PRINCIPLES

The externalization and globalization of the paradigm of mass surveillance espoused by the United States in the War on Terror has created a number of existential challenges for the right to privacy. This

---

415. Paul De Hert & Serge Gutwirth, *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, *in* PRIVACY AND THE CRIMINAL LAW 61, 78 (Erik Claes, Antony Duff & Serge Gutwirth eds., 2006).

416. *See* Mitsilegas, *The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance*, *supra* note 6.

article has highlighted these challenges in the context of the development of U.S. law and executive action and its external impact and repercussions, most notably at the level of the EU. Transatlantic counterterrorism cooperation has thus far legitimized and extended the reach of this American model of mass surveillance. In the face of these developments, as well as rapid advances in technology and the blurring of the division between public and private in communications and surveillance, legal standards do not offer satisfactory responses or meaningful human rights protection. It is challenging to address concerns about mass surveillance at a national level, and it is even more challenging to do so at the transatlantic, regional, or global level. Yet it is precisely at these levels, and especially at the global level, where a meaningful legal response to strengthen privacy in the face of surveillance is urgently needed. As with other areas of the War on Terror, judiciaries have provided the most powerful responses to mass surveillance and upheld the right to privacy in a meaningful and expansive way. The role of the European Court of Justice is noteworthy in this context: in its recent case law it has emerged as a bold constitutional court by placing the protection of privacy at the top of its agenda. But judicial intervention is not enough. The development of a global privacy regime consisting of globally applicable privacy standards is critical to ensure appropriate responses to globalized mass surveillance.

In formulating the content of a global privacy regime, EU law can provide important guiding principles. Four key principles that should underpin the global privacy regime can be identified in this context. First, the right to privacy should apply to all individuals, irrespective of their nationality. The extension of privacy protection to everyone will place meaningful limits on foreign surveillance and confront the challenge of addressing global and extraterritorial systems of surveillance with territorial laws. Second, the right to privacy should cover not only the processing of personal data, but also should target and limit the very *collection* of such data and its storage and transfer. This is particularly important regarding the collection of everyday personal data stemming from legitimate transactions (such as booking a flight, arranging a bank transfer or making a phone call). A broad conceptualization and articulation of the right to privacy, which would encompass, but not be limited to, the right to data protection, is key in this context. Third, a global privacy regime must ensure effective remedies and meaningful avenues for redress for individuals claiming to be affected by surveillance activities. The EU

Court of Justice in *Schrems*[417] and the European Court of Human Rights in *Zakharov*[418] have both espoused approaches which enable standing and grant a remedy to individuals who cannot necessarily demonstrate that they have been affected individually by surveillance, but who raise the prospect of a risk of a breach of their privacy rights due to surveillance. This approach can form the basis of a minimum standard approach on standing at the global level. Fourth, national independent privacy supervisors should be used across the globe. The EU model is worthy of emulation here; independent supervision provides a rigorous avenue of scrutiny of compliance by the executive and the legislature, and also strengthens the right to an effective remedy by providing an avenue for affected individuals to bring privacy complaints before independent supervisory authorities with independent investigative and decision-making powers. Formal and informal avenues of cross-border and international cooperation between independent authorities can also be explored to address challenges of cross-border, extraterritorial, and increasingly globalized surveillance. These four principles will form the framework for the development of more detailed rules at a global level, but adherence to them has the potential to establish a global privacy regime, ensuring both a high level of privacy protection and a high level of legal certainty in an increasingly global level playing field.

417. Schrems, *supra* note 98.
418. Zakharov, *supra* note 99.