2018

Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance

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

Giorgio Resta

Recommended Citation

Bignami, Francesca, Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance (2018). Francesca Bignami & Giorgio Resta, Human Rights Extraterritoriality:The Right to Privacy and National Security Surveillance in Community Interests Across International Law (Eyal Benvenisti & Georg Nolte,eds., Oxford University Press, forthcoming); GWU Law School Public Law Research Paper No. 2017-67; GWU Legal Studies Research Paper No. 2017-67. Available at SSRN: http://ssrn.com/abstract=3043771

Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance

Francesca Bignami and Giorgio Resta

I. Introduction

In theory, the digital world represents one of the most likely terrains for the emergence of community interests in international law. Because most aspects of human existence are now routinely digitalized and sent across global communications networks, it has become increasingly difficult to pinpoint the territorial location of human relations. For any single economic or social interaction that occurs over the Internet, a number of states can generally claim a legitimate interest in regulating that interaction. Thus the traditional organizing principle of the international legal order—territory—does not provide significant traction over the digital world. At the same time, the thickness of transborder social relations made possible by the digital revolution has created the promise of a global society in which human solidarity is experienced without regard for national borders and a common understanding of the rights and duties of citizenship in a global community can emerge. Individuals should come to demand a common set of legal and moral guarantees that are enjoyed by all participants in the digital world. In sum, the digital revolution has made community obligations both politically expedient and morally possible: the old international system of states and territory cannot serve as an ordering device for the borderless Internet, and the social interactions fostered by borderless digital communications should give rise to a common set of moral commitments that will gradually replace those of the nation-state.

Among the different interests at stake in the governance of the digital world, the right to privacy is one of the most important. It is also one that has been explicitly recognized in international law as a community interest. Article 17 of the International Covenant on Civil and Political Rights declares: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[1] It is a fundamental right enjoyed by all members of the human community and deserving of respect by all states whenever they act on their territory or enjoy "effective control" over persons.[2] Thus it appears that the promise of a community interest in digital governance is matched by the letter of the international law, at least with respect to the right to privacy.

This contribution explores the extent to which the state practice of digital privacy law lives up to the promise of the universal right to privacy. It examines the law of what are generally recognized as two of the most important jurisdictions for digital privacy: the United States and the European Union. And it focuses on a policy area that has been the subject of intense public interest and debate in recent times: national security surveillance by spy agencies.[3] Protecting national security is a policy area

[1] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]. Since Article 17 is central to this contribution, it is worthwhile reproducing it in full here:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.

[2] See discussion *infra*.

[3] One of the challenges of understanding state practice in this area is that states have created different organizational arrangements for the activity of protecting national security. We use the term "spy agency" to refer to any authority with powers in the national security domain, even though that authority might also be a police agency, i.e., one charged with prosecuting crimes, an immigration agency, i.e., one charged with controlling population movements, or a regulatory

that can be considered a "least likely" case for the right to privacy, under national constitutional law and, even more so, under international human rights law. In the national security arena, the state acts to defend the population against low probability but high impact violence that threatens the very existence and basic values of the national community. In this policy area, the imperatives of state action are at their peak. Surveillance designed to advance national security is often allowed to curtail substantially the right to privacy. This structural disadvantage is true of all privacy rights, including those enjoyed by national citizens under their domestic constitutions, but it is especially pronounced with regard to the international human right, since foreigners, who tend to be the most significant beneficiaries of the right, are often among those believed to threaten the security of the national community.

To summarize the exposition below: The safeguards afforded for privacy under the law of national security surveillance in the United States and the European Union appear to be motivated as much, if not more, by national self-interest as by a universal right to privacy. This is particularly true of the United States. There the law has traditionally distinguished between insiders (citizens and permanent residents) and outsiders (all others) and has protected the privacy rights of the insiders far more assiduously than those of the outsiders. It has also distinguished between surveillance in the national territory and surveillance abroad and has largely regulated only the former. As alluded to earlier, it has become increasingly difficult to identify the location of, and territory of, communications in the digital world. What is striking, however, is that many of the efforts that have been made to modernize surveillance law rely on the category of person and seek to improve privacy for insiders rather than relinquish that category in favor of an international human right that applies regardless of the identity of the party. The exception is Presidential Policy Directive-28, adopted in 2013, which requires that intelligence agencies recognize the privacy interests of all persons, but it remains unclear whether this has altered the differences in treatment of insiders and outsiders.

In the European Union, there is no power to act internally ("competence") in the national security domain, including legislation and adjudication on the right to privacy in the activities of national spy agencies. However, the European Union has certain powers to regulate privacy externally, in foreign spy agencies, to the extent that such agencies receive personal data from EU market or police actors. With respect to the United States, there are four bilateral agreements in place that touch on national security surveillance and that seek to improve privacy rights for outsiders. Unsurprisingly, given the bilateral nature of these agreements, they reflect the traditional, self-interested logic of international law designed to further the interests of the parties to the agreement rather than the broader international community. Although the EU-U.S. agreements have improved data privacy, they apply only to personal data transferred from the EU and to data subjects located in the EU; indeed, in the case of the agreement on police cooperation, certain rights are granted only to EU citizens.

Moving to surveillance by European spy agencies, the institution with the most comprehensive jurisdiction is the European Court of Human Rights (ECtHR). Largely because it is a human rights court, the ECtHR has taken a broader view of the territorial and personal scope of the right to privacy than is evident in U.S. and EU law. Put differently, in the language of this project, the Court takes the community interest in the right to privacy and the corresponding state duty to respect that community obligation very seriously. Because privacy is considered a human right, all persons are covered and are guaranteed the same treatment by the state. Moreover, like the UN Human Rights Committee, the

agency, i.e., one charged with regulating markets. For an analysis of the complex comparative law of police and spy agencies, see Jacqueline Ross, *The Emergence of Foreign Intelligence Investigations as Alternatives to the Criminal Process: A View of American Counterterrorism Surveillance through German Lenses*, *in* COMPARATIVE CRIMINAL PROCEDURE (Jacqueline E. Ross & Stephen C. Thaman, eds., 2016).

ECtHR applies an effective control test to determine the spatial circumstances under which states owe a duty to individuals and must abide by the community interest in human rights. Although the ECtHR has yet to issue a definitive pronouncement on how the effective control test applies to state surveillance, it appears likely that it will find that the test captures the surveillance of communications with an extraterritorial dimension, e.g., communications that originate or terminate abroad or that occur almost entirely abroad.

The rest of this chapter proceeds as follows. The next section explores the evolving content of the right to privacy in international human rights law. The chapter then turns to the law of national security surveillance in the United States, the European Union, and the European Convention of Human Rights. The last section concludes.

II. International Human Rights Law and the Promise of Privacy as a Community Interest

Privacy is widely recognized as a fundamental human right.[4] In the context of digital communications, however, the definition of the right is the subject of some dispute. At its core, the right to privacy safeguards an area of autonomous development and liberty, a "private sphere" that shall not be intruded upon by the unsolicited interventions of state actors or individuals and corporations. Beyond this core, many legal systems also recognize a freestanding and more far-reaching right to control the collection and use of one's own personal information. Such an expansive trend is clearly mirrored in the most recent regional human rights instruments, such as the European Charter of Fundamental Rights.[5] United Nations (UN) developments as well confirm the tendency to anchor data protection in the context of international human rights law.[6] Even though Article 12 of the Universal Declaration of Human Rights and Article 17 of the ICCPR have a traditional focus on intimacy and autonomy, the right to data protection has recently emerged at the forefront of the UN's agenda. Both the UN General Assembly, in its 2013, 2014 and 2016 Resolutions on the *Right to privacy in the digital age*, and the Human Rights Council, in its 2015 Resolution appointing a Special Rapporteur on the right to privacy, directly or indirectly confirmed that Article 17 of the ICCPR is implicated by the gathering and processing of personal data.[7]

The trigger for these international developments was Edward Snowden's revelation of massive electronic surveillance by the spy agencies of many Western states, most notably the U.S. National Security Agency (NSA). Because these surveillance programs generally involve a significant foreign component and because, as will be discussed below, U.S. law (as well as the law of many other countries) tends to afford foreign nationals less protection than citizens,[8] many activists, NGOs and

---

[4] Sarah Joseph, Jenny Schultz & Melissa Castan, THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 476-77 (2nd ed., 2004).

[5] Besides the right to privacy (art. 7), the Charter of Fundamental Rights in the European Union, 2000 O.J. (C 364) 1 explicitly guarantees the right to data protection (art. 8). *See* Stefano Rodotà, *Data Protection as a Fundamental Right*, *in* REINVENTING DATA PROTECTION?, 77 (Serge Gutwirth et al. eds.,, 2009).

[6] *See* Kriangsak Kittichaisaree & Christopher Kuner, *The Growing Importance of Data Protection in Public International Law*, EJIL:TALK (Oct. 14, 2015), http://www.ejiltalk.org/the-growing-importance-of-data-protection-in-public-international-law/.

[7] G.A. Res. 68/167, The Right to Privacy in the Digital Age (Jan. 21, 2014); G.A. Res. 69/166, The Right to Privacy in the Digital Age (Dec. 18, 2014); G.A. Res. 71/199, The Right to Privacy in the Digital Age (Dec. 19, 2016); Human Rights Concil Res. 28/16 (Mar. 24, 2015). In the pre-Snowden era, the Human Rights Committee stated, in its General Comment no. 16, that "effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant." (Int'l Human Rights Instrument, Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1, at 21 ¶ 10 (July 29, 1994),

[8] *See* Amit K. Chhabra, *FISA Surveillance and Aliens,* 82 FORDHAM L. REV. RES GESTAE 17 (2014).

political actors have increasingly resorted to international human rights law as a possible shield against abuses. Using international human rights law as a regulatory framework for national security surveillance is undoubtedly a promising development from the overall perspective of this book.[9] It is not, however, an easy task, since the substantive content of an international right to privacy, as well as the breadth and depth of the community obligations in this policy area, is a matter of dispute. On the one hand, national security surveillance is generally regarded as a form of spying, and espionage has traditionally been considered an activity at the margin of the law, a policy area in which the imperatives of the state are at their peak.[10] On the other hand, technological developments have strongly altered the physiognomy and contemporary significance of national security surveillance. It is no longer targeted at government actors, but has turned into a massive "data machine," which has a wide-ranging and particularly serious impact on the private life of average citizens as well as on the functioning of democracy.[11] In the context of Article 17 of the ICCPR, two issues in particular have given rise to debate: the scope of its application, namely its extraterritorial reach, and the appropriate framework for balancing privacy and security. The remainder of this section considers each in turn.

The scope of ICCPR rights is governed by Article 2(1), under which the state parties "undertake […] to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant." It is uncontroversial that any interception of communications taking place within national borders, involving either a state's citizen or an individual physically present in that state, satisfies the conditions of Article 2(1) and hence the right to privacy under Article 17 applies.[12] More complicated is the question of state obligation in the case of surveillance that is not purely domestic. This may be surveillance of communications that take place entirely beyond national borders, or surveillance of communications that cross states' borders, e.g., a telephone communication between a state national and a foreigner, or an electronic communication between foreigners that is routed through the national communication infrastructure. In either case, some or all of the individuals involved are not within the territory of the state and the controversial issue of the extraterritorial application of human rights arises.[13]

On the extraterritoriality issue, Article 2(2) has been construed in different ways. The most restrictive interpretation is the one asserted by the United States, on the basis of a literal and narrow reading of the text.[14] According to the United States, the ICCPR's safeguards apply only to persons who are both *within* the state's territory *and* subject to the state's jurisdiction. Under such an interpretation, communications involving individuals abroad, which are the focus of many NSA programs, are not covered by the "international right to privacy." The only binding restrictions would be the ones deriving from U.S. domestic laws, as described in the next section. The U.S. position, however, is the minority position, and has been criticized by other states, human rights experts, and

---

[9] *See* Eyal Benvenisti, *Community Obligations in International Adjudication, in* COMMUNITY INTERESTS ACROSS INTERNATIONAL LAW XX (Eyal Benvenisti & Georg Nolte, 2017).

[10] Ashley Deeks, *An International Legal Framework for Surveillance,* 55 VA. J. INT'L L. 291, 313-314 (2015).

[11] Zygmunt Bauman et al., *After Snowden: Rethinking the Impact of Surveillance,* 8 INT'L POL. SOC. 121 (2014).

[12] Deeks, *supra* note 10, at 311.

[13] For a taxonomy of various typologies of surveillance (foreign, transnational, domestic), see *id*. at 300; Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. J. INT. L. 81, 86, 121 (2015).

[14] For an analysis (and critical assessment) of the traditional U.S. position, see Harold Hongju Koh (Legal Advisor, U.S. Dep't of State), *Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights*, (Oct. 19, 2010), https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf; *see also* Beth Van Schaak, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change,* 90 INT'L L. STUD. 20 (2014).

treaty bodies as fundamentally flawed.[15] Indeed, the majority opinion asserts a broader interpretation of Article 2 of the ICCPR, downplaying its literal wording, namely the use of the conjunctive "and," and holding that any state party must respect and ensure the rights guaranteed by the ICCPR *both* within its territory *and* whenever it has "jurisdiction" over either foreign territory or a person.[16] In particular, the Human Rights Committee, in its case law and its General Comment, Number 31, has firmly taken the position that "a State Party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[17] In international human rights courts and treaty bodies, whether a state exercises "effective control" over a territory or a person today operates as the main test for settling the threshold issue of jurisdiction.

How does the "effective control" test apply to the virtual world of electronic surveillance? This test was originally developed with regard to physical infringements of human rights, as in the case of torture or deprivation of liberty. On the basis of a narrow reading of the "effective control" test, some scholars deny that the Covenant can be triggered by interferences of a purely incorporeal character, such as electronic surveillance.[18] In other words, if the victim of a violation is not in custody or subject to other forms of physical control by the surveilling state, Article 17 is not implicated. This narrow reading, however, leads to illogical results. The very same state action that would be prohibited "at home" would be permitted if committed beyond the national borders, even though Article 17 establishes a universal right to privacy that should not turn on a purely factual criterion that is largely divorced from normative evaluation of the interests at stake. Rather, it appears that the better approach is to tailor the application of the effective control test to the specific character of the right at issue.[19] It should not be forgotten that even the right to life might be violated without exercising effective control over person or territory, as in the case of killings by drones. In the virtual world of digital communications, conventional modes of exercising control such as police searches of physical premises are rarely employed. Yet technology enables massive intrusions into the private sphere of individuals, through, for instance, the bulk collection of electronic communications data. In view of this reality, a teleological interpretation of the ICCPR appears preferable and the "effective control" test should be applied flexibly in order to cope with the challenges arising from technological advances. Indeed, it can be argued that whenever a state collects personal data, it is indirectly exercising control over those persons that generated the data; therefore it should abide by the rules laid down in the ICCPR, in particular Article 17, irrespective of the modalities or place of the collection or the nationality of the data subject.[20]

---

[15] Ilina Georgieva, *The Right to Privacy under Fire – Foreign Surveillance under the NSA and the GCHQ and Its Compatibility with Art. 17 ICCPR and Art. 8 ECHR*, 31 UTRECHT J. INT'L & EUROP. L. 104, 110 (2015).

[16] Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2146 (2014); Deeks, *supra* note 10, at 307-08.

[17] Human Rights Comm., General Comment no. 31, Nature of the General Legal Obligation on State Parties to the Covenant, ¶ 10, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004).

[18] See the post by Jennifer Daskal, *Extraterritorial Surveillance Under the ICCPR…The Treaty Allows It!,* JUST SECURITY (Mar. 7, 2014), https://www.justsecurity.org/7966/extraterritorial-surveillance-iccpr-its-allowed/; John B. Bellinger III, Testimony Before the Privacy & Civil Liberties Oversight Board (Mar. 19, 2014), http://www.pclob.gov/Library/20140319-Testimony-Bellinger.pdf; *see also, generally*, Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015).

[19] *See* Milanovic, *supra* note 13, at 120; Manfred Nowak, Letter to the Editor, *What Does Extraterritorial Application of Human Rights Mean in Practice?*, JUST SECURITY (Mar. 11, 2014), https://www.justsecurity.org/8087/letter-editor-manfred-nowak-extraterritorial-application-human-rights-treaties-practice/.

[20] In a similar vein, see Milanovic, *supra* note 13, at 120-30; Margulies, *supra* note 16, at 2150; Georgieva, *supra* note 15, at 113-14.

To conclude this discussion, it should be noted that a number of human rights bodies have confirmed the expansive interpretation of "effective control" in the area of electronic surveillance. The Human Rights Committee, in its *Concluding observations on the fourth periodic report of the United States of America*, urged that the United States take "all necessary measures to ensure that its surveillance activities, *both within and outside the United States*, conform to its obligations under the Covenant, including article 17" (emphasis added).[21] In a similar vein, the UN High Commissioner for Human Rights, in his Report *The Right to Privacy in the Digital Age*, firmly took the position that digital surveillance

> 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, 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.[22]

In particular, given the universal nature of the protected rights and the global reach of surveillance techniques, no discrimination between citizens and foreigners should be admissible. This point has been made very clearly and convincingly by the special UN Rapporteur on the right to privacy, Joseph A. Cannataci. In his last report issued on February 24, 2017, he noted that

> it is of utmost importance that states respect the right to privacy, which is based on human dignity, on a global level. Surveillance activities, regardless of whether they are directed towards foreigners or citizens, must only be carried out in compliance with fundamental human rights such as privacy. Any national laws or international agreements disregarding this fact, must be considered outdated and incompatible with the universal nature of privacy and fundamental rights in the digital age[23]

We now move from the scope issue to the question of how Article 17 and the international right to privacy apply in the domain of national security surveillance. The wording of Article 17 of the ICCPR makes clear that privacy is only protected against "unlawful" and "arbitrary" interferences. As stated by the UN Human Rights Committee (UNHRC) in its General Comment, Number 16, the term "unlawful" implies that any interference can only take place "on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."[24] In addition, the law authorizing the interference must be precise and well defined, specifying in detail "the precise circumstances in which such interferences may be permitted."[25] As regards arbitrariness, the Committee made clear that the notion is "intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."[26] The principle of proportionality is therefore implicated by the concept of "arbitrary interference";[27] as openly stated by the UNHRC,

---

[21] Human Rights Comm., Concluding Observations on the Fourth Periodic Rep. of the United States, U.N. Doc. CCPR/C/USA/CO/4, at 10 (Apr. 23, 2014).

[22] *See* High Commissioner for Human Rights, *Rep. on the Right to Privacy in the Digital Age*, ¶¶ 34-35, U.N. Doc. A/HRC/27/37 (June 30, 2014).

[23] *See* Report of the Special Rapporteur on the right to privacy, ¶ 29, U.N. Doc. A/HRC/34/60 (February 24, 2017).

[24] Int'l Human Rights Instrument, *supra* note 7, ¶ 3.

[25] *Id.* ¶ 4.

[26] *Id.* ¶ 4.

[27] Joseph, Schultz & M. Castan, *supra* note 4, at 483.

"any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[28]

These privacy requirements apply in the policy area of national security surveillance too.[29] Any surveillance program should comply with a certain set of procedural and substantive standards, on which there is growing consensus among the various international and regional human rights bodies and courts that have been called upon to assess national practices.[30] As recently summarized by the UN High Commissioner for Human Rights, in his Report *The Right to Privacy in the Digital Age*, any surveillance measure must be carried out on the basis of a law, having the following features: (a) it is publicly accessible; (b) it contains provisions that ensure that the collection and processing of data pursue legitimate aims (the protection of national security surely counts among such legitimate aims); (c) it is sufficiently precise, specifying in detail circumstances, modalities and limits of such interference, so as to enable the potential victims to reasonably foresee the consequences of their conduct; (d) it provides for effective safeguards against abuse.[31] As further stated by the UN High Commissioner for Human Rights, interferences with the right to privacy are compatible with the ICCPR only insofar as they are necessary and proportionate to the legitimate aims pursued, and can never be applied "in a manner that would impair the essence of a Covenant right."[32]

Whether, based on this framework, the surveillance programs disclosed by Edward Snowden are compatible with the ICCPR has been the subject of heated debate.[33] Both the UN General Assembly, in its Resolutions 69/166 and 71/199,[34] and the UN Human Rights Committee, in its *Concluding observations on the fourth periodic report of the USA*,[35] openly challenged the legality of such measures as being in conflict with Article 17 of the ICCPR. It remains to be seen to what extent these findings by international human rights bodies will actually influence the behavior of states, which consider themselves at the forefront of the war on terrorism and increasingly rely on big-data collection and predictive analytics to counter threats to their national security.[36] As will be explored below, in the case of the United States and the NSA, such influence has been rather limited until now. Improvements for the privacy rights of foreign nationals located outside the territory of the United States have been introduced in large part as a result of the self-interest logic of bilateral negotiations rather than in furtherance of the idea of a community interest in privacy.

---

[28] Int'l Human Rights Instrument, *supra* note 7, ¶ 8.3.

[29] Res. 69/166,*supra* note 7.

[30] The European Court of Human Rights, which is considered by many to be a veritable forerunner in this policy area, is analyzed at the end of this chapter. On the convergence between the UNHRC approach and the ECtHR case law on secret surveillance, see Milanovic, *supra* note 10, at 133.

[31] High Commissioner for Human Rights, *Rep. on the Right to Privacy in the Digital Age supra* note 22, ¶ 28.

[32] Human Rights Comm., *supra* note 17, ¶ 6.

[33] The scholarly work that has dealt with this question has come to different conclusions. Peter Margulies is of the opinion that most surveillance programs carried out by the NSA on non-U.S. persons outside the United States cannot be considered "arbitrary" under Article 17 of the ICCPR, because they target "terrorists, national security threats, and espionage in a tailored fashion" (Margulies, *supra* note 20, at 2153). To reach this conclusion, he reads Article 17 of the ICCPR in tandem with the law of armed conflict and UN Security Council resolutions on counterterrorism, advancing a "model of procedural pluralism that gives states flexibility in creating protections if they honor core principles such as notice, oversight, and minimization." Ilina Georgieva, by contrast, raises serious doubts about the legality of the mass surveillance programs, arguing that the bulk collection of metadata and the indiscriminate interception of communications – as implemented by the NSA and the GCHQ – constitute "a disproportionate restriction of the privacy rights under Art. 8 ECHR and Art. 17 ICCPR" (Georgieva, *supra* note 20, at 124).

[34] G.A. Res. 69/166 and G.A. Res. 71/199, *supra* note 7.

[35] Human Rights Comm., *supra* note 21.

[36] *See generally* Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773 (2015).

III. The United States: The Limits on Privacy Protection for Non-U.S. Persons

How does U.S. law on national security surveillance measure up to the community interest set down in Article 17 of the ICCPR? As evident from the previous section, there are two somewhat distinct issues, namely the territorial scope of the right to privacy and, once it is recognized that an individual does enjoy the right to privacy, whether the state surveillance in question satisfies the framework for balancing security and privacy. In light of the aims of this volume, this analysis of U.S. law focuses on territorial scope, but it should be recognized that even in situations in which it is recognized that Article 17 clearly applies, there remains the question of whether the right to privacy has been adequately protected.

Under U.S. law, the right to privacy in the national security domain turns on both the place of the surveillance and the territorial affiliation of the individual. The constitutional right to privacy is found in the Fourth Amendment. Setting aside the debates on what kinds of surveillance practices are covered,[37] there are important territorial limitations on the application of the Fourth Amendment.[38] The view has long been that, within the United States, the constitutional right to privacy in the Fourth Amendment applies whenever the government conducts a search or seizure in the national territory, regardless of the citizenship of the person.[39] By contrast, when the government conducts searches outside the territory of the United States, the Fourth Amendment applies only to that "class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[40] Territory—the location of the data and police access to that data—is critical for determining the scope of application of the right to privacy.[41] When surveillance occurs within the United States, the assumption is that the person is entitled to Fourth Amendment protection, whereas outside the United States the reverse is the case.

Moving from police activity to national security, the reach of the Fourth Amendment is even more limited. Under constitutional law, repressive state activity is divided into three categories: ordinary criminal investigations, domestic intelligence operations, and foreign intelligence investigations.[42] These distinctions were first drawn in the *Keith* case, decided by the Supreme Court in 1972.[43] In that case, the government had engaged in warrantless wiretapping of a member of a radical domestic group (the "White Panthers") who was eventually prosecuted for bombing a CIA recruitment office.[44] When faced with the issue of whether the warrantless wiretapping was in line with the constitutional requirements of the Fourth Amendment, the Supreme Court acknowledged that there was a difference between surveillance connected to "ordinary crime" and to "national security."[45] The latter was conducted pursuant to the President's constitutional power to "preserve, protect, and defend the Constitution of the United States" and was designed to "protect our Government against those who

---

[37] There is no general right to data protection in the U.S. Constitution and therefore many new technologies and data collection practices are not automatically covered by the Fourth Amendment. The Supreme Court has moved only slowly to provide guidance on what types of new data collection practices, such as government access to private search engine data and cell phone location tracking, are covered by the Fourth Amendment. *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014).

[38] *See generally* KAL RAUSTIALA, DOES THE CONSTITUTION FOLLOW THE FLAG? THE EVOLUTION OF TERRITORIALITY IN AMERICAN LAW 157-86 (2009).

[39] Daskal, *supra* note 18, at 336-37.

[40] United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990). For a reading of the case law that is more favorable to nonresident aliens, see Alec Walen, *Fourth Amendment Rights for Nonresident Aliens*, 16 GERMAN L.J. 1131 (2015).

[41] *See generally* Daskal, *supra* note 18.

[42] Ross, *supra* note 3 at 3.

[43] United States v. United States District Court, 407 U.S. 297 (1972).

[44] Trevor W. Morrison, *The Story of United States v. United States District Court (Keith):The Surveillance Power*, *in* PRESIDENTIAL POWER STORIES 287 (Christopher Schroeder & Curtis A Bradley eds., 2008).

[45] 407 U.S. at 313, 321.

would subvert or overthrow it by unlawful means."[46] In the Court's analysis, national security could be further divided into two parts: the "domestic aspects of national security," which applied to the defendant, who was involved in purely domestic radicalism, and the "activities of foreign powers or their agents," inside or outside the United States.[47] The Court found that in the case of *domestic security surveillance*, the government was required to follow the warrant requirements of the Fourth Amendment. In so holding, it was driven by the danger that unchecked government surveillance would burden democratic debate and dissent. The Court, however, expressly left open the different question of whether the warrant requirement applied in the case of surveillance of foreign powers or agents of foreign powers, which quite obviously were not beneficiaries of the democratic freedoms of the U.S. Constitution. This exception to the warrant requirement for national security surveillance with a foreign dimension could apply to any individual, U.S. citizen or otherwise, since any individual could serve as the agent of a foreign power. The Court's scheme reflected the characteristic American view of privacy, which emphasizes more the importance of privacy for the democratic process and less the deontological, dignitarian value of privacy. It also drew a distinction that is unknown to the international privacy law reviewed earlier in this chapter, one based not on the *location* of the surveillance but on the *purpose* of the surveillance. In doing so, the Court left a constitutional loophole in a situation in which, even under the most conservative approaches to international human rights law, the United States is clearly bound by the right to privacy.[48]

As a result of the *Keith* case, state surveillance follows one of two paths and is governed by one of two privacy standards. If the police conduct an ordinary criminal investigation or gather intelligence on purely domestic groups, such as white supremacists, they are covered by the Fourth Amendment as well as, in the case of the federal police, the extensive federal legislation that is applicable to surveillance.[49] If, however, the state conducts foreign intelligence surveillance then the Supreme Court's case law under the Fourth Amendment affords precious little guidance. Rather, spy agencies are subject to legislation designed to fill the gap left by the constitutional law: the Foreign Intelligence Surveillance Act (FISA),[50] originally enacted by Congress in 1978, and Executive Order 12333, promulgated by President Reagan in 1981.[51] While FISA applies to national security surveillance *inside* the United State, Executive Order 12333 regulates surveillance *outside* the United States as well as other residual forms of surveillance. To understand the territorial and personal limitations on the right to privacy, it is helpful to take each in turn.

Broadly speaking, FISA standards seek to ensure that government surveillance conducted pursuant to FISA is truly directed at national security threats (as opposed to ordinary crime) and at foreign threats (as opposed to domestic ones), thereby not circumventing the privacy protections of the Fourth Amendment. Because of the importance of targeting threats that are foreign, as opposed to domestic, in origin, the identity of the person under surveillance is pivotal in the FISA scheme.

---

[46] *Id.* at 310.

[47] *Id.* at 308, 322.

[48] Although the Supreme Court has not pronounced on the matter, the lower courts have applied the more general Fourth Amendment framework of "administrative searches" to assess the constitutionality of government interferences with the right to privacy in the foreign intelligence domain. *See generally* L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits*, 66 VAND. L. REV. 1343 (2013); Stephen F. Schulhofer, *An International Right to Privacy? Be Careful What You Wish for*, 14 INT'L J. CONST. L. 238, 258 (2016). This framework, however, does not apply to those that cannot claim rights under the Fourth Amendment, i.e., the nonresident aliens at issue in United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

[49] The primary law is the Electronic Communications Privacy Act 0f 1986, 18 U.S.C. §§ 2510-2710 (1982 & Supp. IV1986), which includes the Wiretap Act, the Pen Register Act, and the Stored Communications Act.

[50] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 (2007).

[51] Exec. Order No. 12333, 3 C.F.R. 200 (1981), *reprinted in* 50 U.S.C. § 401 app. at 44-51 (1982) [hereinafter Executive Order 12333].

FISA creates the classes of "U.S. persons" (defined as citizens and permanent residents) and "non-U.S. persons" (defined as everyone else) and allows for more surveillance of "non-U.S. persons."[52] This was true as originally enacted but has become especially apparent since 9/11. Perhaps the most vivid example is Section 702 of the FISA Amendments Act, enacted in 2008.[53] It has been used as the authority for PRISM, the National Security Agency (NSA) program that collects content and metadata from a variety of Internet companies located in the United States, as well as for upstream collection, the NSA program which intercepts personal data that transit through cables and switches in the United States, and which gathers both Internet traffic and telephone calls, including the content of those calls.[54] Section 702 allows the government to collect foreign intelligence information, including all types of electronic surveillance, on any non-U.S. person reasonably believed to be located outside the United States when their communications cross U.S. soil. Foreign intelligence is defined as information "related" to the protection of national security against foreign threats as well as information that advances the foreign affairs and national defence interests of the United States.[55] The government is required to follow targeting and minimization procedures approved by a special court (the FISA Court), but these procedures mostly run to the benefit of U.S. persons: the targeting procedures are designed to ensure that the selectors, e.g., email addresses, IP addresses, etc., used to sweep up the data are indeed likely to produce data on non-U.S. persons abroad; the minimization procedures are crafted so as to eliminate the data on U.S. persons inadvertently swept up in the Section 702 surveillance.[56]

Turning to Executive Order 12333, it sets down the organization and powers of the government agencies that comprise the intelligence community and also regulates electronic surveillance. It applies to the extent that such surveillance is not already regulated by the more precise and robust guarantees of FISA and therefore is generally understood to apply mostly to surveillance conducted outside the United States. The principal privacy guarantee is that the relevant agencies collect, retain, and disseminate information only in accordance with procedures set down under departmental guidelines and approved by the Attorney General.[57] But this requirement applies only to "information concerning U.S. persons." Executive Order 12333 also contains other provisions on privacy, but they are all worded so as to apply only to intelligence gathering conducted within the United States or concerning U.S. persons. In sum, even more so than FISA, non-U.S. persons are entirely unprotected under Executive Order 12333.

The digital revolution alluded to earlier in this contribution has prompted a number of actual and proposed changes to the traditional legal framework for national security surveillance. To the extent that these changes have been motivated by privacy (as opposed to national security) concerns, they have been focused largely on improving privacy for U.S. persons. The FISA Amendments Act of 2008 contained three important provisions: Section 702, discussed above, and Sections 703 and 704.[58]

---

[52] 50 U.S.C. § 1801(a)(1).

[53] Codified at 50 U.S.C. §1881a. Section 702 is due to expire in December 2017, see FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012), and the terms of Congress's reauthorization of this intelligence gathering program are currently being debated.

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

[55] 50 U.S.C. § 1801(e).

[56] DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS ch. 17 (2d ed. 2012).

[57] Executive Order 12333, *supra* note 51, at § 2.3.

[58] Section 703 of the FISA Amendments Act, codified at 50 U.S.C § 1881b, applies when acquisition of the data occurs within the United States; Section 704, codified at 50 U.S.C. § 1881c, applies when acquisition occurs outside the United States.

These latter two transferred the surveillance of U.S. persons located abroad from Executive Order 12333 to FISA, considered to be more privacy protective.[59] At least part of the rationale was the increasing volume of U.S.-person data located outside the United States, with the explosion of global communications and the Internet, and the need to treat it under roughly the same rubric as squarely domestic communications.

In contrast with Sections 703 and 704, Section 702 significantly loosened legal controls on national security surveillance and has come under heavy fire from civil rights advocates. By far the most critical was a report issued by the liberal think tank, the Brennan Center.[60] It has called for the repeal of Section 702.[61] Yet even in the Brennan Center report, the case for eliminating Section 702 is based on the vast quantities of data on U.S. persons that are swept up in surveillance supposedly directed exclusively at non-U.S. persons abroad.[62] The government oversight body, the Privacy and Civil Liberties Board, has issued a far milder assessment of Section 702. Although it recommended a couple of improvements designed to reduce the burden on U.S.-person privacy rights, it left Section 702 largely intact and deferred entirely the question of the rights of non-U.S. persons under international human rights law to a possible future report.[63] Last, a special presidential commission, convened in the wake of the Snowden revelations, has recommended that Section 702 be curtailed, but largely with respect to U.S. persons, not non-U.S. persons.[64]

There is one legal innovation, introduced in response to the Snowden revelations, aimed squarely at non-U.S. persons: Presidential Policy Directive-28 (PPD-28).[65] PPD-28 mandates privacy protections for non-U.S. persons in the domain of foreign intelligence surveillance.[66] While avoiding any specific reference to the international right to privacy, its language clearly invokes the discourse of human rights:

> Our signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information.[67]

The guarantees for non-U.S. persons contained in PPD-28 hew closely to a classic data protection framework. It contains a general commitment to proportionality,[68] limits use, dissemination and retention,[69] addresses security and accuracy concerns,[70] and provides for oversight.[71] Although PPD-28 is of considerable symbolic value, it is unclear whether it has made a significant change to agency

---

[59] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y 117, 138-40 (2015).

[60] ELIZABETH GOITEIN & FAIZA PATEL, WHAT WENT WRONG WITH THE FISA COURT (2015).

[61] *Id.* at 45.

[62] *Id.* at 27, 42.

[63] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., *supra* note 54, at 5-14.

[64] RICHARD A. CLARKE ET AL., THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD 151-57 (2013).

[65] There was some concern that one section of President Trump's immigration executive order of January 25, 2017 would override the privacy rights afforded to non-U.S. persons under PPD-28 and the Judicial Redress Act (discussed later in this chapter). See Aaron Tantleff & Jule Kadish, *Will Trump's Executive Order Impact Agreemenets Between the U.S. and EU on Cross-Border Data Transfers?* 22 No. 2 CYBERSPACE LAWYER, March 2017. However, the common view is that this did not occur.

[66] David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SECURITY L. & POL'Y 209, 289 (2014).

[67] Presidential Policy Directive No. 28, Signals Intelligence Activities § 1 (Jan. 17, 2014) [hereinafter PPD-28], https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[68] *Id.* at § 1(d).

[69] *Id.* §§ 2, 4(a)(i).

[70] *Id.* § 4(a)(ii); § 4(a)(iii).

[71] *Id.* § 4(a)(iv).

practices. Academic opinion is divided.[72] Commentators have voiced two types of reservations. Some have argued that many of the guarantees announced in PPD-28 are already in place, including those related to security, access, accuracy, and retention (for data held in mixed U.S. person and non-U.S. person databases.[73] In addition, Daniel Severson argues that the guarantees related to collection and use in PPD-28 are not as robust as those in Executive Order 12333.[74]

IV. European Union: Improving Privacy for EU Data Subjects in U.S. Surveillance

There is a curious divide in the European law regulating national security surveillance. With respect to surveillance by non-EU spy agencies, including the NSA, EU law controls. With respect to surveillance by EU spy agencies, the European Convention on Human Rights (and the European Court of Human Rights) controls. This chapter first considers EU law, which has expanded the rights of EU data subjects subject to NSA surveillance. It then turns to the right to privacy under Article 8 of the ECHR and discusses the ECtHR's liberal approach to the application of that right; as will be discussed, states are bound to respect the right to privacy whenever they exercise virtual control over individuals, including when they intercept the communications of individuals. .

In recognition of the uniquely transboundary character of personal data, most early privacy laws contained an extraterritorial component designed to protect the privacy of personal data when it was transferred abroad.[75] Consistent with this approach, the first (and still operative) EU data protection law also sought to regulate international data transfers.[76] Under Article 25 of the Directive, data transfers are permitted only if the third county ensures an "adequate level" of data protection. If the third country does not guarantee an adequate level of data protection, the transfer must be blocked or one of the channels set down in the Directive must be followed. One such channel is diplomatic negotiations that improve the level of data protection afforded by the law of the third country and that result in a favorable adequacy assessment. Although, in line with the market-based origins of the European Union, the Directive only covers data transfers by market actors, the adequacy assessment extends to the entire law of the third country. Police, immigration, and spy agencies are increasingly relying on the personal data generated in the private sector—including the private sector data transferred from the European Union—for their surveillance activities and therefore the safeguards applicable to these public actors have also become the subject of adequacy assessments. By contrast, the European Union does not have competence, internally, over spy agencies because Member States have retained their powers in this sensitive area of national sovereignty.[77] Thus the paradoxical situation obtains whereby EU institutions are called upon to review and potentially regulate spy agencies abroad, even though they do not exercise this same power over Member State spy agencies.

This extraterritorial dimension of EU law has generated three EU-U.S. agreements designed to protect the privacy of EU data once transferred to the United States, including in the area of national

---

[72] For the skeptical view, see Daniel Severson, *American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change*, 56 HARV. INT'L L. J. 465 (2015); Kris, *supra* note 66, at 294. For the favorable view of PPD-28, see Timothy H. Edgar, *The Good News About Spying*, FOREIGN AFFAIRS (Apr. 13, 2015), https://www.foreignaffairs.com/articles/united-states/2015-04-13/good-news-about-spying.

[73] Kris, *supra* note 66, at 293; Severson, *supra* note 72, at 482-85.

[74] Severson, *supra* note 72, at 482-83.

[75] These include the laws of Sweden, France, and Germany, as well as the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, 1496 U.N.T.S. 65.

[76] Council and European Parliament Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31. In 2018, the Directive will be replaced by Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1.

[77] Treaty on European Union, July 29, 1992, 1992 O.J. (C 191) 1, art. 4(2).

security surveillance.[78] These agreements have sought, in part, to remedy the lacunae in U.S. law discussed earlier for non-U.S. persons. The first in the series involves the passenger name records (PNR) collected by airlines and transferred to U.S. authorities for counterterrorism and crime-fighting purposes. The PNR Agreement contains the full panoply of data protection guarantees required under EU law.[79] The terms of the PNR Agreement apply largely to the personal *data* transferred from the European Union. To the extent that *individuals* are protected, in the provisions guaranteeing access and correction rights and administrative and judicial redress, they are expressly protected irrespective of their territorial affiliation: "any individual, regardless of nationality, country of origin, or place of residence" has a right of access, correction, and redress.[80]

The second EU-U.S. agreement concerns financial data on bank transfers, gathered by the U.S. Treasury Department under a program known as the Terrorist Finance Tracking Program (TFTP).[81] Like the PNR Agreement, the TFTP Agreement contains a variety of data protection guarantees. Also like the PNR Agreements, those guarantees apply to all the personal data transferred from the European Union and, to the extent that individuals are directly concerned, to "any person,"[82] or, as stated in the redress section, to "all persons regardless of nationality or country of residence."[83]

Most recently, in July 2016, the European Union and the United States adopted the so-called "Privacy Shield."[84] The Privacy Shield is designed to overcome the across-the-board, transatlantic differences in privacy law and to allow market actors of all types to transfer EU data to the United States without running afoul of EU law. It replaces the earlier Safe Harbor Agreement, from 2000, which had a similar purpose.[85] One of the most important novelties of the Privacy Shield is that it pays considerable attention to the privacy guarantees in place when public authorities, including spy agencies, obtain EU personal data from market actors. This is the direct result of *Schrems v. Data*

---

[78] For a more thorough discussion of these agreements, current through 2015, see Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & CONTEMP. PROBS. 101 (2015). It bears mentioning that the jurisprudence of the European Court of Justice in the privacy area is constantly evolving and that the recent cases of Joined Cases C-203/1 & C-698/15, Tele2 Sverige, ECLI: EU:C:206:970, and Opinion 1/2015 (Canada-EU PNR Agreement), ECLI:EU:C:2016:656, have implications for these EU-U.S. agreements.

[79] There have been three successive PNR agreements: the original 2004 agreement, its 2007 replacement, and the agreement currently in force, from 2012. Commission Decision 2004/535/EC of 14 May 2004 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States Bureau of Customs and Border Protection, 2004 O.J. (L 235) 11; Agreement Between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), EU-U.S., 23-26 July, 2007, 2007 O.J. (L 204) 18; Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, EU-U.S., Dec. 14, 2011, 2012 O.J. (L 215) 5 [hereinafter PNR Agreement].

[80] PNR Agreement, *supra* note 79, at arts. 11-13.

[81] There have been two EU-U.S. TFTP Agreements, the first dating to 2007 and the one currently in force adopted in 2010. *See* Notice: Publication of U.S./EU Exchange of Letters and Terrorist Finance Tracking Program Representations of the United States Department of the Treasury, 72 Fed. Reg. 60054-02 (Oct. 23, 2007); 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, EU-U.S., June 28, 2010, 2010 O.J. (L 195) 5 [hereinafter TFTP Agreement].

[82] TFTP Agreement, *supra* note 81, art. 15 ("Right of Access"), art. 16 ("Right to Rectification, Erasure, or Blocking").

[83] *Id.* art. 18 ("Redress").

[84] Commission Implementing Decision (EU) of July 12, 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C(2016) 4176 final, 2016 O.J. (L 207) 1 [hereinafter Privacy Shield].

[85] *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 69–79 (2000); U.S. Dept. Commerce, Issuance of Safe Harbor Principles and Transmission to European Commission, 65 Fed. Reg. 45666-01 (July 24, 2000).

Protection Commissioner, in which the European Court of Justice (CJEU) annulled the Safe Harbor Agreement on the grounds that the European Union had allowed an open-ended exception to the data protection principles "to the extent necessary to meet national security, public interest, or law enforcement requirements"[86] without assessing the adequacy of the applicable legal framework.[87] The Court's decision was based in large part on the massive transfer of personal data to the NSA, including that of EU nationals, that had been revealed by Snowden and that is authorized under the U.S. law discussed earlier in this chapter. The Privacy Shield, therefore, unlike the earlier Safe Harbor Agreement, includes representations and commitments not just from the U.S. agencies responsible for regulating the market (Department of Commerce, the Federal Trade Commission, and the Department of Transportation), but also from the U.S. agencies responsible for national security and law enforcement (the Director of National Intelligence and the Department of Justice).

In the national security domain, the Privacy Shield contains two sections aimed at demonstrating the adequacy of U.S. privacy law. The first is a letter from the Office of the Director of National Intelligence (ODNI), which provides an overview of U.S. law that curtails intelligence activities related to non-U.S. persons. The letter is a response to the allegations made in the course of the *Schrems* litigation of "mass and indiscriminant NSA surveillance"[88] and the observation by the Court that "in particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 [of the EU Charter of Fundamental Rights]."[89] In conducting this overview, ODNI pays special attention to the legal guarantees for non-U.S. persons put into place by PPD-28, as well as the limits on bulk collection generally speaking, set down in both PPD-28 and Section 702,[90] The letter explains that whenever Section 702 applies (that is, whenever electronic data is gathered in the United States on non-U.S. persons overseas from Internet companies like Facebook), data is collected based on "the use of individual selectors, such as email addresses or telephone numbers, which U.S. intelligence personnel have determined are likely being used to communicate foreign intelligence information of the type covered by the certification submitted to the court."[91] When surveillance is conducted under the more general authority conferred by Executive Order 12333 and only PPD-28 applies, bulk collection is conducted only when the use of specific selectors is not feasible.[92]

The second element of the Privacy Shield aimed at national security surveillance is a commitment from the U.S. State Department establishing a Privacy Shield Ombudsperson, located in the State Department and independent from the Intelligence Community. [93] The Ombudsperson has responsibility for the access and redress guarantees of data protection law. As outlined in the Privacy Shield, to exercise their access and redress rights, EU data subjects must file a complaint with their responsible data protection authority (DPA). That complaint is then sent to a central "EU individual

[86] Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions Issued by the US Department of Commerce, annex I, 2000 O.J. (L 215) 7.

[87] Case C‑362/14, Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650.

[88] Opinion of the Advocate General, Case C‑362/14, Schrems v. Data Protection Comm'r, ECLI:EU:C:2015:650, at para. 36 (recounting procedural history of reference from the Irish High Court).

[89]Id. at para. 94.

[90] Privacy Shield, *supra* note 84, annex VI (Letter from General Counsel Robert Litt, Office of the Director of National Intelligence).

[91] *Id.* at 11.

[92] *Id.* at 3.

[93] Privacy Shield, *supra* note 84, annex III, annex A.

complaint handling body" which transmits the complaint to the Ombudsperson. In response, the Ombudsperson is charged with giving the following, two-part answer to the EU body:

> (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied.[94]

Like the PNR and TFTP Agreements, the Privacy Shield is generally directed at protecting personal data. Therefore, as long as the data has been transferred from the European Union, it is covered, irrespective of the nationality or the residence of the data subject. The same is the case with the access and redress procedures that are available to data subjects, with the exception of those that require the individual to approach first their EU DPA before the matter will be taken up by the U.S. authorities. In those cases, the individuals, as set out under EU law, must be data subjects "in the Union."[95] The section of the Privacy Shield directed specifically at national security follows this pattern. The review of U.S. law provided by the ODNI highlights the privacy rights of all non-U.S. persons, not simply EU persons, following the terms of the U.S. law. By contrast, the Ombudsperson provisions only apply to data subjects in the European Union, since they must initially approach their EU DPAs before they are entitled to a reply from the Ombudsperson.

In view of the focus of this project, it is important to mention the last major EU-U.S. agreement in this area, the Umbrella Agreement covering data transfers for law enforcement purposes.[96] After over five years of negotiations, it has entered the final stages of the ratification process. The Umbrella Agreement is designed to ensure a common standard of data protection in the area of police cooperation, including national security investigations, which in the United States can involve both police and spy agencies. In contrast to the EU-U.S. agreements already discussed, it is based on the European Union's competence in police and judicial cooperation. Compared to the other agreements, the provisions governing the personal scope of privacy rights are more limited. As a general matter, the Umbrella Agreement is drafted to apply to, and to protect, all "personal information" transferred by EU authorities to U.S. authorities regardless of the origin of that information.[97] Moreover, all individuals are entitled to seek access to their personal data, correction, and administrative redress.[98] But two critical guarantees apply only to the citizens of the respective parties: the right to nondiscrimination based on nationality[99] and the right of judicial redress.[100]

To summarize the above discussion, the four bilateral agreements with ramifications for national security surveillance contain obligations that apply to any personal data as long as it is transferred from the European Union. In addition, they all contain rights that can be invoked by any individual with respect to their EU personal data. The Privacy Shield, however, contains inter-institutional mechanisms for obtaining redress that must be invoked by data subjects located in the European Union. The Umbrella Agreement also restricts certain rights to EU (and U.S) nationals. Furthermore,

---

[94] *Id.* at 4.e.

[95] General Data Protection Regulation, *supra* note 76, art. 3.2.

[96] 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, EU-U.S., 2 June, 2016, 2016 O.J. (L 336) 3 [hereinafter Umbrella Agreement]. *See generally* Sergio Carrera, Gloria González Fuster, Elspeth Guild & Valsamis Mitsilegas, ACCESS TO ELECTRONIC DATA BY THIRD-COUNTRY LAW ENFORCEMENT AUTHORITIES 38 (2015).

[97] Umbrella Agreement, *supra* note 96, art. 3.

[98] *Id.* at arts. 16, 17, 18.

[99] *Id.* at art. 4.

[100] *Id.* at art. 19.

all four agreements are bilateral agreements and therefore follow the bilateral logic of protecting only data subjects with a connection to the European Union.

V. European Human Rights System: International Privacy Rights for European Spy Agencies

Different from EU law, the European Convention of Human Rights (ECHR) governs all the activities of the Contracting Parties, including national security surveillance. Indeed, several decisions of the European Court of Human Rights (ECtHR) deal with the secret surveillance of electronic communications and its impact on the right to privacy under Article 8.[101] Since the NSA revelations, human rights activists and NGOs have filed three applications challenging the joint surveillance conducted by the UK Government Communications Headquarter (GCHQ) and the U.S. NSA, known as the TEMPORA program.[102] Although, as of today, none of these cases have been decided, the ECtHR's case law gives a strong indication of how it will rule on these mass surveillance programs. Following the same scheme used to analyze Article 17 of the ICCPR, it is helpful to discuss, first, the scope of application and extraterritorial reach of the ECHR and, second, the privacy guarantees that apply to national security surveillance.

The ECtHR has been a forerunner in the field of extraterritorial application of human rights, often inspiring the behavior of other international human rights bodies and courts.[103] Article 1 of the ECHR lays down the state parties' obligation to "secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention." As an initial matter, it should be underscored that the ECHR, as a veritable human rights instrument, does away with any notion of citizenship and guarantees rights protection for "everyone." Turning to the jurisdictional clause, it has been interpreted liberally by the ECtHR. In a well-known series of judgments, the Court has recognized, within certain limits, that the ECHR has extraterritorial effect.[104] Although its case law has not always been consistent, the Court has generally held that the state parties must abide by the Convention not only when they act within their national borders, but also whenever they exercise effective control over either a person or foreign territory.[105]

The effective control principle may very well render the Convention applicable not only in situations of physical control over a foreign territory or person located overseas, such as in

---

[101] For an overview, see MICHELE NINO, TERRORISMO INTERNAZIONALE, PRIVACY E PROTEZIONE DEI DATI PERSONALI [INTERNATIONAL TERRORISM, PRIVACY AND PROTECTION OF PERSONAL DATA] 147-320 (2012).

[102] The three applications against the UK are Big Brother Watch v. United Kingdom, App. N. 58170/13 (Sept. 2013); Bureau of Investigative Journalism v. United Kingdom, App. N. 62322/14 (Sept. 2014); 10 Human Rights Organisations v. United Kingdom, App. N. 24960/15 (May 2015). For a detailed list of all the pending cases in the field of secret surveillance, see Mo nika Ermert, *Europe: Queue of Complaints Against Snooping Laws Grows by the Month*, INTERNET POLICY REVIEW (Mar. 12, 2016), http://policyreview.info/articles/news/europe-queue-complaints-against-snooping-laws-grows-month/397.

[103] CARLO FOCARELLI, TRATTATO DI DIRITTO INTERNAZIONALE [INTERNATIONAL LAW TREATY] 1042 (2015). In this chapter we do not deal with the different, albeit equally important issue, of the extraterritorial application of EU data protection law outside the area of national security surveillance. For a discussion of this issue, see Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on US Businesses*, 50 STAN. J. INT'L L. 53 (2014); Lokke Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?*, 1 INT'L DATA PRIVACY L. 28 (2011); Cedric Ryngaert, *Special Issue Extraterritoriality and EU Data Protection*, 5 INT'L DATA PRIVACY L. 221 (2015).

[104] Among the various decisions, see Loizidou v. Turkey, 310 Eur. Ct. H.R. (ser. A) (1995); Al-Skeini v. United Kingdom, 53 Eur. Ct. H.R. 18 (2011).

[105] MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES AND POLICY 37-48 (2011); FOCARELLI, *supra* note 103, at 1042-47.

peacekeeping or state-building missions, but also in cases of "virtual" control, as in the interception of communications taking place or originating outside of the country. For instance, in the 2008 case of *Liberty and others v. UK*, the Grand Chamber of the ECtHR found a violation of two Irish NGOs' right to privacy, neither of whom was physically present in the territory of the UK, because their private communications had been monitored by the British government by way of its Electronic Test Facility (ETF) at Capenhurst, Cheshire.[106] The facts in *Weber and Saravia v. Germany* were similar. There, the applicants claimed that their Article 8 rights had been violated by Germany since their telephone communications from abroad had been intercepted by the German security agency. Both of the applicants resided in Uruguay (and one was not a German national) and the German government contested the Court's jurisdiction, but the Court did not rule on the point, since the application was declared inadmissible on other grounds.[107] The Court will shortly have the chance to finally settle the jurisdictional issue: in one of the pending mass surveillance cases, *10 Human Rights Organisations v. UK*, the majority of the applicants are based outside of Britain and claim to be victims of a violation of their right to privacy as a result of the implementation of the TEMPORA program by the UK GCHQ.[108] Recently, the UK Investigatory Powers Tribunal held that "a contracting state owes no obligation under Art. 8 to persons both of whom are situated outside its territory in respect of electronic communications between them which pass through that state."[109] It is by no means obvious, however, that the European Court will adopt the same stance and opt for a narrow reading of the jurisdictional clause of Art. 1 of the ECHR in the context of electronic communications. In light of the Court's overall approach to the extraterritorial application of human rights, it cannot be excluded that the ECHR will be held applicable to the electronic surveillance of communications between individuals abroad, at least when, as in the British case, the state has effective control over the digital communications infrastructure.

Having concluded the analysis of state jurisidiction, let us turn to the privacy (Article 8) obligations imposed on surveilling states.[110] At this point in the discussion, it is worthwhile flagging the standing issue. The ECtHR has held on several occasions that, provided certain conditions are satisfied, a person can claim to be the victim of an Article 8 violation by virtue of the mere existence of legislation permitting secret surveillance.[111] There is no need to allege that surveillance measures were in fact applied to the complainant.[112] This is important because in most surveillance cases one of the biggest legal hurdles for the victim is the evidentiary one, since the measures taken by spy

[106] The respondent government did not contest in this case the applicability of the Convention *ratione personae*, therefore the Court did not have the chance to directly address the threshold jurisdictional issue (Liberty v. United Kingdom, Eur. Ct. H.R. (2008), http://hudoc.echr.coe.int/eng?i=001-87207).

[107] Weber v. Germany, 2006-XI Eur Ct. H.R..

[108] 10 Human Rights Organisations, *supra* note 102.

[109] Human Rights Watch Inc. v. The Secretary of State for the Foreign and Commonwealth Office, [2016] UKIPTrib 15_165-CH [60].

[110] We will focus here only on negative obligations, although positive obligations might have particular relevance with regard to the behavior of private corporations, such as Internet providers, which collect enormous amounts of data that might be accessed by foreign governments, as demonstrated by the NSA programs. On this point, see Mistale Taylor, *The EU's Human Rights Obligations in Relation to Its Data Protection Laws with Extraterritorial Effect*, 5 INT'L DATA PRIVACY L. 246 (2015).

[111] The ECtHR most recently stated the conditions for derogating from the concreteness requirement (and the principle that generally denies individuals the right to challenge a law *in abstracto*) in Zacharov v. Russia, Eur. Ct. H.R. ¶ 171 (2015), http://hudoc.echr.coe.int/eng?i=001-159324.

[112] Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) (1978); Weber v. Germany, *supra* note 107; Kennedy v. United Kingdom, Eur. Ct. H.R. (2010), http://hudoc.echr.coe.int/eng?i=001-98473; Szabó v. Hungary, Eur. Ct. H.R. (2015), http://hudoc.echr.coe.int/eng?i=001-160020.

agencies are generally, by definition, secret.[113] The significance of the ECtHR's approach to standing can be appreciated through comparison with the U.S. Supreme Court, which has held that the mere threat of surveillance does not establish standing to sue.[114]

As regards the privacy standards governing national security surveillance, the ECtHR employs a framework similar to the one discussed earlier in the section on Article 17 of the ICCPR. Under Article 8, interferences with the right to privacy must be set down in law, must further a legitimate purpose, and must be limited by a number of substantive and procedural guarantees to ensure proportionality. The ECtHR has consistently held that surveillance measures should be explicitly authorized by a law, which must be accessible to the person concerned, sufficiently detailed as regards the procedures and limits of the monitoring, and foreseeable as to its effects.[115] The "quality" of the authorizing law is crucial in the Strasbourg court's approach to secret surveillance, since an overbroad definition of the scope of the monitoring would give the executive power unfettered discretion. The ECtHR has also adhered to a fairly rigorous set of requirements under the proportionality analysis. As early as 1978, in *Klass and Others v. Germany*, the Court observed that "[p]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."[116]

The ECtHR's recent case law on secret surveillance has continued to apply a quite rigorous approach, notwithstanding the challenges arising from global terrorism.[117] In *Szabó and Vissy v. Hungary*, its first NSA-style surveillance case, the Court manifested serious concerns over the technological advances that have enabled state authorities to collect enormous masses of personal data and build detailed individual profiles.[118] It stated that the new threats to privacy are to be subjected to even closer scrutiny and that the requirements of the existing case law on surveillance are to be enhanced.[119] In one particularly telling passage, the Court concluded that "it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives."[120]

More specifically, in *Szabó and Vissy v. Hungary*, the Court held that the phrase "strictly necessary in a democratic society" (art. 8, par. 2) means not only (as in *Klass*) that secret surveillance measures must be "strictly necessary for safeguarding the democratic institutions," but also that they must be "strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation."[121] Surveillance, in other words, must be individualized. In this way the court seems to rule out, in the absence of a previous judicial authorization, the blanket collection of content and communications data referring to a wide range of persons and unrelated to a specific threat previously identified. This finding is coherent not only with the firm position recently taken by the

---

[113] *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1962 (2013).

[114] Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013).

[115] It is worthwhile noting that the requirements of accessibility and foreseeability are aimed at protecting both an individual and a general interest in controlling the way in which executive power is exercised. *See* Szabó v. Hungary, *supra* note 112, ¶ 65.

[116] Klass v. Germany, *supra* note 112, ¶ 42.

[117] In this respect, the jurisprudence of the ECtHR mirrors that of the Court of Justice of the European Union (CJEU). In both its Grand Chamber decision in Zacharov v. Russa, *supra* note 111 and its Fourth Section decision in Szabó v. Hungary, *supra* note 112, the ECtHR has expressly referred to the jurisprudence of the CJEU.

[118] See lastly Szabó v. Hungary, *supra* note 112, ¶¶ 68, 70.

[119] *Id.* ¶ 70.

[120] *Id.* ¶ 68.

[121] *Id.* ¶ 73.

European Court of Justice with regard to the large-scale surveillance programs, but also with the Strasbourg court's longstanding case law on secret surveillance. While recognizing that states enjoy a certain margin of appreciation in balancing privacy and national security and tailoring surveillance programs to the particular aims to be accomplished, the Court has always stressed the need for the states to put in place "adequate and effective guarantees against abuse."[122] The Court conducts its assessment on a case-by-case basis, taking into account the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorizing and supervising authorities, and the kind of remedy provided by the national law. Among the minimum safeguards imposed by the Court are, at the authorizing stage, the presence of an impartial and independent supervisory authority, which in principle should be a judicial authority (but on this point the position of the Court is not always consistent); and, once the surveillance has been terminated, the possibility of challenging the legality of such measures retrospectively, in court.[123] In both *Szabó* and *Zakharov v. Russia*, a state surveillance case decided shortly beforehand, the ECtHR found that the respondent states had failed to satisfy the authorization requirement: in *Zakharov* , because the Russian security services were allowed to intercept telephone communications at their discretion and without a previous judicial order; in *Szabó*, because the Hungarian Anti-Terrorism Task Force could monitor all kinds of communications simply on the basis of a warrant of the Ministry of Justice, without having to obtain judicial authorization and to provide evidence in support of their request.

VI. Conclusion

There are many hurdles to the establishment, in state practice, of community obligations. In the domain of privacy and national security, as we have argued in this chapter, the United States does not subscribe to a strong version of community obligations. By contrast, European countries, which are subject to a powerful regional human rights court, are legally obliged to respect the privacy rights of all individuals subject to state surveillance. To return to the overarching themes of this volume, one reason for this difference is to be found in the different conceptualizations of privacy—including the community interest in privacy—in the two places.

The U.S. Supreme Court has traditionally focused on rights, including privacy, as an instrument for maintaining a healthy democracy. This is linked to the theory of rights announced in the famous *Carolene Products* case: unlike the earlier, vilified Lochner-era case law, the Court stated that it would vigorously protect only those rights specifically recognized in the constitutional text and those rights essential to the democratic process.[124] By contrast, European constitutional courts, including the regional courts, safeguard a broader range of substantive rights and use the omnipresent proportionality test to balance rights against the imperatives of state action.[125] This contrast is what one of us has called elsewhere the difference between the "ballot-box democracy" and the "fundamental rights" models of judicial review.[126]

The comparative law consequences of the judicial philosophy announced in *Carolene Products* are relatively well known in the area of economic and social rights.[127] What is less well understood is how the Supreme Court's reluctance to elaborate a robust core of fundamental rights has shaped

[122] Klass v. Germany, *supra* note 112, ¶ 50.

[123] See, in particular, Zacharov v. Russia, *supra* note 111, ¶ 233.

[124] United States v. Carolene Products, 304 U.S. 144, 152n. 4. (1938). *See generally* Tom Colby & Peter Smith, *The Return of Lochner*, 100 CORNELL L. REV. 527 (2015).

[125] AHARON BARAK, PROPORTIONALITY, (Doron Kalir transl., 2012).

[126] Francesca Bignami, *Regulation and the Courts: Judicial Review in Comparative Perspective*, *in* COMPARATIVE LAW AND REGULATION (Francesca Bignami & David Zaring eds., 2016).

[127] Jud Mathews & Alec Stone Sweet, *All Things in Proportion? American Rights Review and the Problem of Balancing*, 60 EMORY L. J. 797 (2011); Bignami, *supra* note 126.

the content and scope of classic liberal rights like privacy and, of particular relevance for this volume, how those rights apply to the members of global society. The exclusion of political outsiders and "foreign" threats from the guarantees of the Fourth Amendment is tied to the conceptualization of privacy as primarily a safeguard against despotism and a vehicle for democracy. Democracy, virtually everywhere, is practiced and conceived at the national or local level, not at the global level, and therefore it is not unreasonable to suggest that outsiders should not benefit from the same treatment as insiders when subject to state power. But, of course, in the realm of philosophical discourse and the jurisprudence of other courts, including European constitutional courts and the European Court of Human Rights, privacy is also protected because it is the sine qua non of liberal personhood. Without privacy, it is impossible to conceive of individuals capable of freely choosing and pursuing their own life projects;[128] for this reason, privacy (and, in particular, information privacy) has been defined as a precondition for the effective exercise of most fundamental freedoms.[129] And in liberal theory, personhood and individualism are to be enjoyed by all human beings; in this day and age, it is difficult to devise good reasons for denying liberal rights and personhood, including privacy, to those individuals who are situated on the outside, in different social and historical communities. A flexible approach towards the extraterritorial application of privacy, such as the one that might be deployed by the European Court of Human Rights, reflects this theory of fundamental rights.

The jurisprudential roots of state practice in this area suggest that the different attitudes towards the community interest in privacy will persist for some time to come. Case law and courts are notoriously resistant to change, as has been demonstrated by theories of path dependence.[130] At the same time, there are a number of alternative routes, including legislation and special-purpose human rights bodies, that exist domestically for safeguarding rights. In the case of the United States, these can be enlisted to comply with any bilateral or multilateral international legal obligations that emerge to govern national security surveillance. And in the case of Europe, the same alternatives to traditional courts can be used to effectuate the legal principles that have been established by the European Court of Human Rights, but that have often found little traction on the ground, in the law and practice of domestic spy agencies.[131]

---

[128] J. Roland Pennock, *Introduction*, *in* NOMOS XIII: PRIVACY, at xi (J. Roland Pennock & John W. Chapman eds., 1971); Stanley I. Benn, *Privacy, Freedom and Respect for Persons*, *in* NOMOS XII: PRIVACY, *supra*, at 1. *See also* Ernst Benda, *Menschenwürde und Persönlichkeitsrecht* [*Human Dignity and Personality Right*], *in* I HANDBUCH DES VERFASSUNGSRECHTS 173 (Ernst Benda, Werner Maihofer & Hans Jochen Vogel eds., 1995).

[129] Spiros Simitis, *Datenschutz: Voraussetzung oder Ende der Kommunikation?* [*Data protection: Prerequisite or End of Communication?*], *in* II EUROPAÏSCHES RECHTSDENKEN IN GESCHICHTE UND GEGENWART 511 (Helmut Coing et al. eds,1982); Stefano Rodotà, *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla privacy* [*Between fundamental rights and the elasticity of legislation: the new Privacy Code*], *in* EUROPA E DIRITTO PRIVATO 1, 5 (2004).

[130] Paul Pierson, POLITICS IN TIME (2004); Oona A. Hathaway, *Path Dependence in the Law: The Course and Pattern of Legal Change in a Common Law System*, 86 IOWA L. REV. 601 (2001).

[131] For instance, the Article 29 Data Protection Working Party, which is an organ with advisory status set up under EU Directive 95/46/EC and is mainly composed of representatives of domestic data protection authorities, has been instrumental in bringing to light the failure of national governments to comply with their data protection duties in the field of foreign surveillance. *See* Data Protection Working Party, Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes, Doc. 819/14/EN, WP 215 (Apr. 10, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf.