10

Digital Communications and the Evolving Right to Privacy

Lisl Brunner

1 INTRODUCTION[1]

The meaning of the human right to privacy is evolving in response to developments in communications technology and an increasingly connected world in which data transits national boundaries imperceptibly. Although governments have had the capacity to access and store unprecedented quantities of digital communications data for some time, high-profile terrorist attacks and expanding transnational criminal activity have provided a strong motive to continue and expand these activities. When Edward Snowden revealed the global scope of existing communications surveillance capacity, states and civil society organizations turned to international law to seek clarity on how the right to privacy protects individuals, preserves legitimate state interests, and addresses the realities of the large-scale collection of data across traditional borders.

The tribunals and experts who interpret international human rights law have developed a rich body of standards on the right to privacy in communications, with European institutions leading the way. These standards address much of the present-day collection and use of digital communications, but significant gaps still exist. Until recently, there were few clear norms regarding the bulk collection of communications data, the responsibility of private companies to respect privacy rights, and the rules and protections that apply when communications data crosses borders.

This chapter explores the evolution of the right to privacy as it is established in international human rights law, and the ways in which human rights law is beginning to bridge these gaps. The first part provides an overview of the right to privacy and highlights developments in the digital age that international human rights law

[1] All opinions expressed in this chapter are those of the author alone and should not be attributed to any organization. Lisl would like to thank Sarah St. Vincent for her thoughtful comments on prior versions of this chapter.

https://doi.org/10.1017/9781316838952.010 Published online by Cambridge University Press

must urgently address. The second part outlines the scope and meaning of the right to privacy in communications as it appears in international human rights treaties and in interpretations of these treaties by international tribunals and experts. The chapter then examines how European institutions are interpreting data protection law in a way that seeks to bridge some of the gaps in privacy protection that have formed in international human rights law. The chapter concludes by describing the incipient steps that UN and European institutions are taking to address the privacy challenges presented by the seamless flow of data across borders.

II THE EVOLUTION OF THE RIGHT TO PRIVACY AND ITS PRESENT CHALLENGES

A *The Protection of Privacy in Human Rights Law*

The right to privacy has a broad scope. Scholars note that there is no universal conceptualization of privacy and that societies' notions of its scope have evolved in response to changing political contexts and technological landscapes.[2] Privacy has often been linked to the interests of limiting access to the self and exercising control over one's personal information and actions.[3] In its diverse characterizations, privacy has been closely linked to human dignity.

The right to privacy is protected in the International Covenant on Civil and Political Rights (ICCPR), which had 168 state parties as of November 2016. Article 17 provides the following:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.[4]

[2] *Report of the Special Rapporteur on the Right to Privacy, Joseph A. Cannataci*, ¶ 20, U.N. Doc. A/HRC/31/64 (March 8, 2016) ("Cannataci Report"); D. Solove, "Conceptualizing Privacy" (2002) 90 *California Law Review* 1088–89; D. Banisar and S. Davies, "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments" (1999) 18 *John Marshall Journal of Computer & Information Law* 1–113 at 6–8.

[3] *See, e.g.*, H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2010), pp. 69–70, 81–88; Solove, "Conceptualizing Privacy," at 1109–24. Solove has identified at least six different but interrelated conceptualizations of the essence of privacy: 1) the right to be let alone, 2) limited access to self, 3) secrecy, 4) control over personal information, 5) personhood (the protection of one's personality, individuality, and dignity), and 6) intimacy (control over one's intimate relations or aspects of life).

[4] International Covenant on Civil and Political Rights, in force March 23, 1976, GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, 999 UNTS 171, art. 17.

Article 12 of the Universal Declaration of Human Rights contains a nearly identical formulation,[5] and the right is also protected in the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention),[6] the Charter of Fundamental Rights of the European Union,[7] the American Convention on Human Rights,[8] and the Arab Charter on Human Rights.[9]

International and domestic tribunals have interpreted the right to privacy as protecting an individual's capacity to decide with whom she has intimate relationships,[10] when to have a family and who forms part of it,[11] and even when to end her own life.[12] Privacy in one's correspondence serves to limit the government's power to monitor its subjects, and it protects a sphere in which individuals can develop and express ideas, exchange confidences, and build relationships. When surveillance of communications occurs or is perceived to occur, individuals are inhibited from seeking and disseminating ideas, and self-censorship results.[13] In light of its relation

[5] Universal Declaration of Human Rights, GA res. 217A (III), U.N. Doc. A/810 at 71 (1948). Article 12 omits the two occurrences of the word "unlawful" from the first paragraph.

[6] European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, November 4, 1950, in force September 3, 1953, ETS 5; 213 UNTS 221. According to Article 8, "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[7] Charter of Fundamental Rights of the European Union, October 26, 2012, in force December 1, 2009, 2010 O.J. (C83) 389 (March 30, 2010), art. 7 ("Everyone has the right to respect for his or her private and family life, home and communications.").

[8] American Convention on Human Rights, San Jose, November 22, 1969, in force July 18, 1978, OAS Treaty Series No. 36; 1144 UNTS 123. Article 11 establishes: "1. Everyone has the right to have his honor respected and his dignity recognized. 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation. 3. Everyone has the right to the protection of the law against such interference or attacks."

[9] League of Arab States, *Arab Charter on Human Rights*, September 15, 1999. Article 17 establishes: "Private life is sacred, and violation of that sanctity is a crime. Private life includes family privacy, the sanctity of the home, and the secrecy of correspondence and other forms of private communication."

[10] *Dudgeon* v. *United Kingdom*, Eur. Ct. H.R., App. No. 7525/76 (October 22, 1981).

[11] *Atala Riffo and daughters* v. *Chile*, Judgement, Inter-Am. Ct. H.R. (ser. C) No. 239, ¶¶ 161–78 (February 24, 2012); *Artavia Murillo et al. ("In Vitro Fertilization")* v. *Costa Rica*, Judgement, Inter-Am. Ct. H.R. (ser. C) No. 257 (November 28, 2012); *Airey* v. *Ireland*, Eur. Ct. H.R., App. No. 6829/73 (October 9, 1979).

[12] *See, e.g.*, *Cruzan* v. *Director, Missouri Department of Health*, 497 U.S. 261 (1990) (describing lower court judgments on individual decisions to terminate medical treatment that were framed in terms of privacy rights, but declining to address the case in those terms).

[13] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, ¶ 24, U.N. Doc. A/HRC/23/40 (2013) ("La Rue Report 2013"); PEN America, *Global Chilling: The Impact of Mass Surveillance on International Writers* (2015); Human Rights Watch and the American Civil Liberties Union, *With Liberty*

https://doi.org/10.1017/9781316838952.010 Published online by Cambridge University Press

to all of these interests and other human rights, the right to privacy has been called "an essential condition for the free development of the personality."[14]

In human rights law, the state's duty to respect and ensure rights entails negative and positive obligations. The state fulfills its negative obligation by not interfering with an individual's right unless it acts in accordance with the law, in pursuit of a legitimate interest, and in a manner that is necessary and proportionate to the fulfillment of that interest.[15] The positive obligation encompasses "the duty of the States Parties to organize the governmental apparatus and, in general, all the structures through which public power is exercised, so that they are capable of juridically ensuring the free and full enjoyment of human rights."[16] With respect to the right to privacy, the UN Human Rights Committee[17] has affirmed that states must establish privacy protections in law as part of their duty to ensure rights.[18]

European institutions have led the way in interpreting the scope of the right to privacy in communications, and particularly in balancing it with the state's interests in gathering information for law enforcement and national security purposes. In 1978, the European Court of Human Rights established 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."[19] European leadership in this area stems from the region's experience during the Second World War, when census records facilitated the identification of the Jewish population and other groups targeted for persecution and extermination by Nazi and Nazi-influenced regimes.[20] Germany's particularly staunch defense of the right to privacy is also linked to the widespread use of surveillance by the Stasi secret police in East Germany and the elaborate files in which it detailed individuals' private lives.[21]

The European approach initially contrasted with the more stringent approach of the UN Human Rights Committee, whose 1988 General Comment on the right to privacy indicated that "[s]urveillance, whether electronic or otherwise, interceptions

to Monitor All: How Large-Scale U.S. Surveillance is Harming Journalism, Law, and American Democracy (July 2014).

[14] *In Vitro Fertilization*, ¶ 143; *see also* Cannataci Report, ¶ 8.

[15] *See, e.g.*, *General Comment No. 31, Nature of the General Legal Obligation on States Parties to the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (2004), ¶6.

[16] *Velasquez Rodriguez* v. *Honduras*, Judgement, Inter-Am. Ct. H.R. (ser. C) No. 4, ¶ 166 (July 29, 1988); *see also General Comment No. 31*, ¶¶ 7, 13; *Airey* v. *Ireland*, ¶ 32.

[17] The Human Rights Committee is the UN body charged with receiving periodic reports from states parties to the ICCPR on implementation of the treaty, as well as interpreting the ICCPR through its general comments and, where a state has recognized its competence, through reports issued in response to communications. International Covenant on Civil and Political Rights, arts. 28, 40–41.

[18] *General Comment No. 31*, ¶ 8.

[19] *Klass and others* v. *Germany*, Eur. Ct. H.R., App. No. 5029/71 (September 6, 1978), ¶ 42.

[20] W. Seltzer, "Population Statistics, The Holocaust, and the Nuremberg Trials" (1998) **24** *Population and Development Review* 511–52.

[21] *See, e.g.*, T. Coombes, "Lessons from the Stasi," *The European* (April 1, 2015).

of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[22] This pronouncement appears strikingly categorical and out of step with state practice. It has historically been regarded as a legitimate state interest to gather foreign intelligence in order to prevent, detect, and prosecute crime and threats to national security.[23]

Over time, however, a more uniform set of global standards on the right to privacy in digital communications has formed, and other human rights institutions have looked to the European Court's extensive case law to inform interpretations of this right. Until the beginning of this century, interpretations of the right to privacy in communications by the European Court and UN mechanisms generally focused on articulating guidelines for conducting targeted surveillance. But advances in technology, coupled with rising national security concerns, have facilitated and incentivized the amassing of large quantities of data by governments. Revelations by Edward Snowden and others have demonstrated the areas in which Western states fall short of meeting existing human rights standards, as well as the areas in which these standards are poorly developed or absent.

B *The Impact of the Snowden Revelations on Privacy in the Digital Age*

Beginning in June 2013, the Snowden disclosures gave the public a wealth of detail about the scope and nature of government surveillance of communications in the digital age, primarily focusing on intelligence programs in the United States and the United Kingdom. The documents describe how the US government collected call detail records of millions of individuals from telecommunications companies on an ongoing basis, performed queries on the records in order to identify potential suspects of terrorism and other international crimes, and used "contact-chaining" to review the records of individuals within three levels of communication of the initial suspect to identify other potential suspects.[24] Through the PRISM program, the US government

[22] *General Comment No. 16: Article 17 (Right to Privacy)*, U.N. Doc. CCPR/GC/16 (1988), ¶ 8.

[23] *See, e.g.*, A. Deeks, "An International Legal Framework for Surveillance" (2015) **55** *Virginia Journal International Law* 291–368 at 300, 301–05, 313 ("Most scholars agree that international law either fails to regulate spying or affirmatively permits it."); R. J. Bettauer, "Questions Relating to the Seizure and Detention of Certain Documents and Data (*Timor-Leste* v. *Australia*). Provisional Measures Order" (2014) **108** *American Journal of International Law* 763–69. In its first case involving espionage issues, the International Court of Justice determined that "a State has a plausible right to the protection of its communications with counsel relating to an arbitration or to negotiations, in particular, to the protection of correspondence between them, as well as to the protection of confidentiality of any documents and data prepared by counsel to advise that State in such a context." *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor Leste v. Australia)*, International Court of Justice, Request for the Indication of Provisional Measures, Order of March 3, 2014, ¶ 27.

[24] G. Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 6, 2013; Privacy and Civil Liberties Oversight Board (United States), *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on*

compelled electronic communications service providers to provide the contents of online communications in response to requests that identified specific attributes of interest (i.e., "selectors"). Through the "upstream" method of surveillance, authorities gained access to the contents of telephone and Internet communications from the cables that transmit the communications internationally.[25]

The Snowden documents suggested that the United Kingdom had obtained the contents of communications in bulk by tapping undersea cables[26] and had intercepted and stored webcam images (including a large number of nude images) from nearly two million user accounts globally.[27] Agencies of both governments purportedly defeated encryption standards to access secure communications,[28] intercepted the communications of diplomatic missions and world leaders, including Angela Merkel and Dilma Rousseff,[29] and used listening stations in their foreign embassies to intercept communications traffic abroad.[30]

Although the Snowden revelations largely focused on the United States, the United Kingdom, and their English-speaking partners in Canada, Australia, and New Zealand (the Five Eyes Alliance), information has also been published suggesting that large-scale surveillance programs exist in France,[31] Sweden,[32] Russia,[33]

the Operations of the Foreign Intelligence Surveillance Court (January 23, 2014), pp. 21–31 ("PCLOB Report on Section 215"). Through these methods, it was estimated that the US government may have retained records related to more than 120 million telephone numbers.

[25] Privacy and Civil Liberties Oversight Board (United States), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), pp. 32–41; G. Greenwald and E. MacAskill, "NSA Prism program taps into user data of Apple, Google, and others," *The Guardian*, June 7, 2013. For a description of several US intelligence programs disclosed by Edward Snowden, see A. Toh, F. Patel, and E. Gotein, "Overseas Surveillance in an Interconnected World," Brennan Center for Justice, New York University School of Law (2016), pp. 5–10.

[26] E. MacAskill et al., "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, June 21, 2013.

[27] S. Ackerman and J. Ball, "Optic Nerve: Millions of Yahoo webcam images intercepted by GCHQ," *The Guardian*, February 28, 2014.

[28] J. Ball, J. Borger, and G. Greenwald, "Revealed: How U.S. and U.K. spy agencies defeat internet privacy and security," *The Guardian*, September 6, 2013.

[29] E. MacAskill et al., "GCHQ intercepted foreign politicians' communications at G20 summits," *The Guardian*, June 17, 2013; E. MacAskill and J. Borger, "New NSA leaks show how US is bugging its European allies," *The Guardian*, June 30, 2013; J. Burke, "NSA spied on Indian embassy and UN mission, Edward Snowden files reveal," *The Guardian*, September 25, 2013; J. Ball, "NSA monitored calls of 35 world leaders after US official handed over contacts," *The Guardian*, October 25, 2013.

[30] "The NSA's Secret Spy Hub in Berlin," *Der Spiegel*, October 27, 2013.

[31] F. Johannes and J. Follorou, "In English: Revelations on the French Big Brother," *Le Monde*, July 4, 2013.

[32] J. Borger, "GCHQ and European spy agencies worked together on mass surveillance," *The Guardian*, November 1, 2013.

[33] I. Poetranto, "The Kremlin's new Internet surveillance plan goes live today," The Citizen Lab, November 1, 2012, https://citizenlab.ca/2012/11/the-kremlins-new-internet-surveillance-plan-goes-live-today/; S. Walker, "Russia to monitor 'all communications' at Winter Olympics in Sochi," *The Guardian*, October 6, 2013.

China,[34] Ethiopia,[35] and Colombia,[36] among other countries. Researchers and WikiLeaks have alleged that government authorities in the Middle East, Africa, and Latin America have obtained spyware that allows them to hack into communications devices remotely in order to monitor individuals.[37]

The Snowden revelations had a more direct impact on international law than prior reports because they also signaled that US and UK surveillance programs targeted powerful allies. Germany, Brazil, and other states brought their grievances to the United Nations, and in December 2013, the General Assembly called on states "[t]o review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law."[38] The General Assembly requested the Office of the High Commissioner for Human Rights (OHCHR) to prepare a report on the right to privacy in the digital age, and the following year it encouraged the Human Rights Council to create a special mandate dedicated to the subject.[39] Joseph Cannataci was appointed as the first Special Rapporteur on the right to privacy in 2015, with a mandate to gather information and raise awareness regarding challenges facing the right to privacy, both generally and in the digital age.[40] Civil society organizations have also advocated for limitations on state surveillance at the international level, developing the Necessary and Proportionate Principles, which are based on the international human rights legal standards described below.[41]

The US government responded to the Snowden revelations by terminating its bulk collection of telephony metadata under one legal authority and committing to greater transparency regarding its communications surveillance programs.[42] Seven months

[34] OpenNet Initiative, *Internet Filtering in China* (2009), pp. 14–17; Human Rights Watch, *Freedom of Expression and the Internet in China* (2001).

[35] Human Rights Watch, *They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia* (2014).

[36] Privacy International, *Shadow State: Surveillance, Law and Order in Colombia* (2015), pp. 27–31.

[37] *See, e.g.*, B. Marczak et al., "Mapping Hacking Team's 'Untraceable' Spyware," The Citizen Lab, February 2014; W. R. Marczak, J. Scott-Railton, and M. Marquis-Boire, "When Governments Hack Opponents: A Look at Actors and Technology," Twenty-Third USENIX Security Symposium (August 2014); *see also* A. Hern, "Hacking Team hack casts spotlight on murky world of state surveillance," *The Guardian*, July 11, 2015; WikiLeaks, "The Hacking Team Archives," July 8, 2015, https://wikileaks.org/hackingteam/emails/.

[38] "The Right to Privacy in the Digital Age," U.N. Doc. A/RES/68/167, December 18, 2013).

[39] "The Right to Privacy in the Digital Age," U.N. Doc. A/RES/69/66, December 18, 2014.

[40] "The Right to Privacy in the Digital Age," U.N. Doc. A/HRC/RES/28/16, April 1, 2015;

[41] A. Alexander, "Digital surveillance 'worse than Orwell,' says new UN privacy chief," *The Guardian*, August 24, 2015.

[42] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA FREEDOM Act), Public Law 114–23, 129 Stat. 268 (June 2, 2015).

after the revelations, its signals intelligence policy was updated to establish principles circumscribing the collection and use of signals intelligence.[43] The policy directive recognized the "legitimate privacy interests" of all persons, and it required that intelligence gathering "include appropriate safeguards for the personal information of all individuals" regardless of their nationality or location. These steps represent progress, but debate about the proportionality of surveillance programs operated by US authorities continues.

On the opposite side of the Atlantic, the United Kingdom, France, and Switzerland have recently passed new laws expanding their surveillance powers.[44] The UK Investigatory Powers Act establishes broad powers for the government to engage in bulk collection of communications data, obtain data located overseas from companies with a UK presence, require the decryption of communications, and perform "bulk equipment interference."[45] Some experts have praised the clarity of the bill and its oversight provisions; privacy experts and advocates have been highly critical of its sweeping powers.[46]

The next section discusses the well-developed body of international human rights law that applies to the surveillance programs revealed by Edward Snowden. While these standards are not well defined in a few areas, such as bulk collection of data, the tribunals and experts that interpret them are moving to fill these gaps.

III HUMAN RIGHTS LAW AND PRIVACY IN DIGITAL COMMUNICATIONS

The language of human rights treaties is general, and it falls to international tribunals, human rights mandate holders, expert bodies, and national courts to interpret the scope and meaning of a right. The European Court of Human Rights defines the obligations of the forty-seven contracting parties of the European Convention on Human Rights. Interpretations of the ICCPR, in turn, are generated by UN bodies including the International Court of Justice (ICJ), the

[43] The White House, Presidential Policy Directive/PPD-28, Signals Intelligence Activities, January 17, 2014.

[44] Loi No. 2015–912 of July 24, 2015 (France); "Swiss endorse new surveillance powers," BBC, September 25, 2016; "Switzerland votes in favour of greater surveillance," AFP, September 25, 2016; "Wet op de inlichtingen – en veiligheidsdiensten 20" (Netherlands), September 1, 2015; Y. Bahceli, "'Dutch intelligence-gathering reform bill sparks privacy concerns," Reuters, September 1, 2015.

[45] Investigatory Powers Act of 2016 (November 29, 2016), www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm.

[46] *See, e.g.*, D. Anderson QC, "Oral Evidence Taken Before the Joint Committee for the Investigatory Powers Bill," December 2, 2015, Questions 61–75, www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf. *But see* Cannataci Report, ¶ 39; E. MacAskill, "'Extreme surveillance' becomes UK law with barely a whimper," *The Guardian*, November 19, 2016; I. Ashok, "UK passes Investigatory Powers Bill that gives government sweeping powers to spy," *International Business Times*, November 18, 2016.

Human Rights Committee, special mandate holders, and the Office of the High Commissioner for Human Rights (but only the decisions of the ICJ are legally binding on parties). The Court of Justice of the European Union has also begun to interpret the rights to privacy and data protection as contained in the EU Charter of Fundamental Rights. The Inter-American Commission and Inter-American Court of Human Rights interpret the American Convention on Human Rights. Consistent with the principle that human rights are universal, these entities draw on one another's interpretations of rights and have thereby begun generating a fairly uniform body of international law on the right to privacy.

A *Legality, Necessity, and Proportionality*

Human rights law is implicated when a state interferes with the right to privacy, which occurs when the contents of communications or communications data are collected by state authorities, regardless of whether the data is examined.[47] Once authorities examine data that has been collected, a second interference takes place. Retaining data over time interferes with the right to privacy,[48] as does sharing communications data with other parties.[49] Restricting anonymity in digital communications is also considered to be an interference with the right to privacy, because anonymous and secure communications allow the free exchange of information and ideas, and anonymity "may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality."[50]

In order to be consistent with international human rights law, an interference with a qualified right such as privacy must meet the tests of legality, necessity, and

[47] *See, e.g., Malone* v. *United Kingdom*, Eur. Ct. H.R., App. No. 8691/79, ¶ 84 (August 2, 1984); Office of the UN High Commissioner for Human Rights, "The right to privacy in the digital age" ("OHCHR Report"), U.N. Doc. A/HRC/27/37, ¶ 19; *Escher* v. *Brazil*, Judgement, Inter-Am. Ct. H.R. (ser. C) No. 200, ¶ 114 (July 6, 2009).

[48] *See, e.g., Amann* v. *Switzerland*, Eur. Ct. H.R., App. No. 27798/95, ¶ 69 (February 16, 2000); *Rotaru* v. *Romania*, Eur. Ct. H.R. App. No. 28341/95, ¶ 46 (Grand Chamber, May 5, 2000); *S. and Marper* v. *United Kingdom*, App. Nos. 30562/04 and 30566/04, ¶ 86 (Grand Chamber, December 4, 2008); *Digital Rights Ireland* v. *Minister of Communications*, Eur. Ct. H.R., App. Nos. 293/12 and 594/12, ¶¶ 34–35 (April 8, 2014).

[49] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, ¶¶ 26–28, U.N. Doc. A/HRC/14/46 (May 17, 2010) ("Scheinin Report 2010"); *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, ¶¶ 35, 48, U.N. Doc. A/HRC/10/3 (Feb. 4, 2009) ("Scheinin Report I 2009"); *Tristan Donoso* v. *Panama*, Judgement, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶ 83 (January 27, 2009).

[50] *Report of the Special Rapporteur for the promotion and protection of the right to freedom of opinion and expression, David Kaye*, ¶ 12, U.N. Doc. A/HRC/29/32 (May 22, 2015). As David Kaye has noted, "[e]ncryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks." Ibid., ¶ 16; *see also* La Rue Report 2013, ¶¶ 23, 47–49.

proportionality.[51] In terms of legality, the action constituting the interference (such as interception of communications) must be previously established in a law that is publicly accessible, clear, and precise, meaning that its consequences are foreseeable.[52] An interference must be in pursuit of a legitimate aim, and it must be a necessary and proportionate means of achieving that aim. For the European Court of Human Rights, the measure must be "necessary in a democratic society," meaning that it must answer a "pressing social need," and state authorities must provide "relevant and sufficient" justifications for the measure.[53]

The court has established that states have a margin of appreciation in determining whether a measure is necessary and proportionate, particularly when the protection of national security is concerned.[54] When a state engages in secret surveillance, the analysis focuses on whether the measures are "strictly necessary for safeguarding the democratic institutions" and whether "adequate and effective guarantees against abuse" are in place.[55] Because individual applicants can rarely prove that they have been the subject of such surveillance, the European Court has permitted challenges to intelligence laws *in abstracto* in certain circumstances, at times finding a violation of Article 8 where the legal framework did not meet the legality test,[56] and at other times looking at whether the law itself is necessary and proportionate.[57]

For the European Court, laws containing a great degree of specificity are more likely to be deemed consistent with the European Convention. The law should specify the nature of the offenses for which surveillance can be ordered,[58] which

[51] While Article 8(2) of the European Convention specifies this, human rights bodies, experts, and tribunals have interpreted the ICCPR and the American Convention to require this test as well. *See, e.g., Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, ¶¶ 16–19, U.N. Doc. A/HRC/13/37 (December 28, 2009) ("Scheinin Report II 2009"); OHCHR Report ¶ 23; *Escher* v. *Brazil*, ¶ 116; *Weber and Saravia* v. *Germany*, Eur. Ct. H.R., App. No. 54934/00, ¶ 80 (June 29, 2006).

[52] OHCHR Report, ¶ 23; *Escher* v. *Brazil*, ¶¶ 130–31; *Zakharov* v. *Russia*, Eur. Ct. H.R., App. No. 47143/06, ¶ 229 (Grand Chamber, December 4, 2015).

[53] *See, e.g., S. and Marper* v. *United Kingdom*, ¶ 101.

[54] *Leander v. Sweden*, Eur. Ct. H.R., App. No. 9248/41, ¶ 59 (March 26, 1987); *S. and Marper* v. *United Kingdom*, ¶ 102; *Weber and Saravia*, ¶ 106; *Zakharov* v. *Russia*, ¶ 232.

[55] *Klass* v. *Germany*, ¶ 42; *Weber and Saravia* v. *Germany*, ¶ 106; *Zakharov* v. *Russia*, ¶ 232; *see also* OHCHR Report, ¶ 25.

[56] *See, e.g., Liberty and others* v. *United Kingdom*, Eur. Ct. H.R., App. No. 58243/00, ¶¶ 64–70 (July 1, 2008); *Malone* v. *United Kingdom*, ¶¶ 80–82; *Rotaru* v. *Romania*, ¶ 62; *Amann* v. *Switzerland*, ¶ 63; *Association for European Integration and Human Rights and Ekimdzhiev* v. *Bulgaria*, Eur. Ct. H.R., App. No. 62540/00, ¶ 93 (June 28, 2007).

[57] *See, e.g., Kennedy* v. *United Kingdom*, Eur. Ct. H.R., App. No. 26839/05, ¶ 155 (March 18, 2010); *see also Klass* v. *Germany*; *Zakharov* v. *Russia*; *Szabo and Vissy* v. *Hungary*, Eur. Ct. H.R., App. No. 37138/14 (January 12, 2016).

[58] *Kennedy* v. *United Kingdom*. Although *Weber and Saravia* was an admissibility decision, the court deemed the German G-10 law to be *prima facie* consistent with the European Convention. The law provided for nontargeted communications surveillance in order to identify or prevent six specific offenses: "1) an armed attack on the Federal Republic of Germany; 2) the commission of international terrorist attacks in the Federal Republic of Germany; 3)

individuals' communications can be monitored,[59] and which authorities are empowered to request, order, and carry out surveillance, as well as the procedure to be followed.[60] It should provide for "a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed."[61] Laws that restrict the right to privacy "must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination."[62]

The European Court of Human Rights has determined on two occasions that the German G-10 Act of 1968 satisfied the rigorous standards for legality that a communications surveillance law must meet.[63] It has also approved provisions of the UK Regulation of Investigatory Powers Act on the interception of domestic communications.[64] In contrast, the court has found that other laws in the United Kingdom, as well as in Russia, Switzerland, Bulgaria, Romania, and Hungary, lacked the necessary specificity and gave the authorities overly broad discretion to conduct communications surveillance.[65]

B *The Necessity and Proportionality of Bulk Collection*

For years, human rights bodies have emphasized that although advances in communications technology require evolution in legal safeguards, the tests of legality, necessity, and proportionality continue to apply.[66] Yet many have questioned

international arms trafficking within the meaning of the Control of Weapons of War Act and prohibited external trade in goods, data-processing programmes and technologies in cases of considerable importance; 4) the illegal importation of drugs in substantial quantities into the territory of the Federal Republic of Germany; 5) the counterfeiting of money (Geldfälschung) committed abroad; 6) the laundering of money in the context of the acts listed under points 3 to 5." *Weber and Saravia*, ¶ 27.

[59] *See, e.g.*, *Klass* v. *Germany*, ¶ 51.

[60] *See, e.g.*, *Escher* v. *Brazil*, ¶ 131.

[61] *Szabo and Vissy* v. *Hungary*, ¶ 56; *Weber and Saravia* v. *Germany*, ¶ 95; *see also Escher* v. *Brazil*, ¶ 131; OHCHR Report, ¶ 28; La Rue Report 2013, ¶ 81.

[62] OHCHR Report, ¶ 23; *Klass* v. *Germany*, ¶ 51.

[63] *Klass* v. *Germany*; *Weber and Saravia* v. *Germany*. As mentioned above, *Weber and Saravia* was an admissibility decision rather than a judgment on the merits, but the court conducted a thorough examination of the G-10 law and determined that there were "adequate and effective guarantees against abuses of the State's strategic monitoring powers," making the applicants' claims under Article 8 "manifestly ill-founded." *Weber and Saravia*, ¶¶ 137–38.

[64] *Kennedy* v. *United Kingdom*.

[65] *Zakharov* v. *Russia*, ¶¶ 244–52; *Amann* v. *Switzerland*; *Malone* v. *United Kingdom*; *Association for European Integration and Human Rights and Ekimdzhiev* v. *Bulgaria*; *Rotaru* v. *Romania*; *Szabo and Vissy* v. *Hungary*.

[66] *See, e.g.*, *Klass* v. *Germany*, ¶ 48; La Rue Report 2013, ¶ 50; *Szabo and Vissy*, ¶¶ 68–70; *Report on Terrorism and Human Rights*, I/A C.H.R., OEA/Ser.L/V/II.116 Doc. 5 rev. 1 corr. (2002) ¶ 371; *Escher* v. *Brazil*, ¶ 115.

whether programs that collect or retain data from millions of individuals who are not implicated in criminal activity or terrorism can ever be necessary and proportionate means of protecting the state and its people. For several UN Special Rapporteurs, the answer is no.[67] The OHCHR, the European Court of Human Rights, and the Court of Justice of the European Union have taken a more measured approach. While they have condemned indiscriminate or generalized surveillance measures, they have indicated that the principles that apply to targeted interception of communications and large-scale collection are generally the same.[68]

When analyzing bulk surveillance programs, the European Court employs a higher level of scrutiny, and it has found that programs that are clearly circumscribed by law and accompanied by robust oversight mechanisms can be consistent with the right to privacy.[69] In *Weber and Saravia* v. *Germany*, the court deemed "strategic monitoring" of communications to be consistent with the European Convention, because the law provided sufficient guarantees against abuses of state power.[70] The law permitted interception based on "catchwords" designed to identify communications linked to one or more of six specific crimes. The guarantees included clear rules governing every aspect of data collection and use, as well as oversight by the three branches of government and a civilian agency.[71]

In contrast, bulk surveillance programs that do not clearly circumscribe state power in law and in practice have been deemed inconsistent with Article 8 of the Convention. The court has ruled that the indefinite retention of biometric data of persons who were suspected (but not convicted) of committing criminal offenses was not necessary in a democratic society.[72] In *Liberty* v. *United Kingdom*, the bulk interception of external communications pursuant to a 1985 law was deemed to violate Article 8 because it gave the executive unfettered discretion as to which of the intercepted communications could be examined.[73] In the 2015 case *Zakharov* v. *Russia*, the court found the government's system of direct access to communications networks by state authorities (known as "SORM") inconsistent with the European Convention. The court noted that interception could take place for a broad range of offenses (including pickpocketing), and that judges had limited powers to order and oversee interception.[74] Because interception orders were not

[67] La Rue Report 2013, ¶ 62; Scheinin Report I 2009, ¶ 30.
[68] *Liberty* v. *United Kingdom*, ¶ 63; OHCHR Report, ¶ 20.
[69] OHCHR Report, ¶ 20.
[70] *Weber and Saravia* v. *Germany*, ¶¶ 117, 137–38. *But see* La Rue Report 2013, ¶ 59 (suggesting that the G-10 law's provisions on warrantless interception for national security purposes is overly broad).
[71] *Weber and Saravia*, ¶¶ 96–102, 115–22, 137.
[72] *S. and Marper* v. *United Kingdom*, Eur. Ct. H.R., App. No. 30562/04 (Grand Chamber, December 12, 2008) ¶ 125.
[73] *Liberty* v. *United Kingdom*, ¶ 64.
[74] *Zakharov* v. *Russia*, ¶¶ 244–52.

presented to communications service providers, the court questioned whether judicial control existed in practice.[75]

Most recently, in *Szabo and Vissy* v. *Hungary*, the court determined that broadly drafted laws and weak oversight of surveillance (primarily by political officials of the same agency that conducted the surveillance) rendered bulk interception of communications inconsistent with the Convention. Deeming "strategic, large-scale interception" for national security purposes to be "a matter of serious concern," the court stated: "A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding [of] the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation."[76] "An individual operation" might be one with a specific target[77]; it might also be an effort to locate and apprehend a terrorist by collecting all communications in a certain area during a particular period. Both *Weber and Saravia* and the recent *Tele2 Sverige* judgment of the Court of Justice of the European Union support the latter position. The court will have more opportunities to determine whether bulk collection should be further circumscribed, as at least three cases challenging bulk surveillance programs in the United Kingdom are pending before it.[78]

For their part, several UN human rights experts have concluded that the bulk surveillance of communications is inherently incompatible with the protection of Article 17 of the ICCPR. The former UN Special Rapporteur for counterterrorism and human rights, Martin Scheinin, has indicated that intelligence-gathering programs should be "case-specific interferences [with the right to privacy], on the basis of a warrant issued by a judge on showing of probable cause or reasonable grounds."[79] The current Special Rapporteur, Ben Emmerson, and the Special Rapporteur on the right to privacy, Joseph Cannataci, have made similar determinations.[80] While Scheinin and others have emphasized the need for strong oversight mechanisms and strict regulations on the use of data that is collected, he and the

[75] Ibid., ¶¶ 261–72.

[76] *Szabo and Vissy* v. *Hungary*, ¶¶ 69, 73.

[77] *See* S. St. Vincent, "Did the European Court of Human Rights Just Outlaw 'Massive Monitoring of Communications' in Europe?," Center for Democracy and Technology, January 13, 2016, https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/.

[78] *Big Brother Watch and others* v. *United Kingdom*, Eur. Ct. H.R., App. No. 58170/13 (September 4, 2013); *Bureau of Investigative Journalism and Alice Ross* v. *United Kingdom*, Eur. Ct. H.R., App. No. 62322/14 (September 11, 2014); 10 *Human Rights Organizations and others* v. *United Kingdom*, Eur. Ct. H.R., App. No. 24960/15 (May 20, 2015).

[79] Scheinin Report I 2009, ¶ 30.

[80] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson*, U.N. Doc. A/HRC/25/59 (March 11, 2014) ¶¶ 52, 59; Cannataci Report, ¶ 39. *But see* La Rue Report 2013 (which does not state that bulk surveillance is per se incompatible with the ICCPR).

other experts suggest that these safeguards are insufficient to make bulk surveillance consistent with the right to privacy.[81]

It seems unlikely that the European Court will shift to the UN rapporteurs' more categorical condemnation of bulk collection, especially as the Court of Justice of the European Union has recently reaffirmed the standards of its case law to date. The European Court's position is logical: Communications surveillance is not prohibited by international law, and it is practiced by prominent European states. As a policy matter, however, it is problematic that human rights law should legitimize a practice that few states will conduct in a rights-respecting manner, and which leads to ever-increasing amounts of data being accessible to actors with a variety of motivations.

C *Effective Oversight of Communications Surveillance*

International human rights law generally provides that large-scale surveillance can be consistent with the right to privacy if it is accompanied by robust oversight mechanisms. Yet oversight of intelligence services and their covert operations has always proved challenging, even in societies where the rule of law is well established. Legislative committees conduct oversight of the intelligence services in the United States and the United Kingdom, but the Snowden revelations raised doubts as to whether these committees have access to the information necessary to perform their roles effectively.[82] In the United States, oversight of signals intelligence activities conducted by executive order is limited.[83] Additionally, while the US Foreign Intelligence Surveillance Court provides judicial authorization and oversight of several intelligence-gathering programs, for many years the confidential nature of its opinions obscured its surprisingly broad interpretation of a provision that permitted the collection of information "relevant to an authorized investigation."[84] That court's authority to examine the collection of foreign intelligence under the PRISM and upstream programs revealed by Snowden is also limited to assessing the government's targeting and minimization procedures.[85]

UN bodies and the European Court have recognized that *ex ante* authorization of communications surveillance by the judiciary provides a powerful safeguard against

[81] Scheinin Report I 2009, ¶¶ 37, 74.

[82] *See, e.g.*, D. Feinstein, "Feinstein Statement on Intelligence Collection of Foreign Leaders," (October 28, 2013); Z. Carpenter, "Can Congress Oversee the NSA?" *The Nation*, January 30, 2014; House of Commons Home Affairs Committee [United Kingdom], Seventeenth Report: Counterterrorism, Chapter 6 (April 30, 2014).

[83] "Overseas Surveillance in an Interconnected World," 32–34.

[84] E. Gotein and F. Patel, "What Went Wrong with the FISA Court," Brennan Center for Justice (2015), 22; PCLOB Report on Section 215, 59–60; *American Civil Liberties Union v. Clapper*, 785 F.3d 787, 811–19 (2d Cir. 2015).

[85] PCLOB Report on Section 215, 177; "What Went Wrong with the FISA Court," 27, 29.

abuse,[86] but they have declined to deem it a requirement of adequate surveillance laws, given the often limited powers of the judiciary to access relevant information or to assess the necessity and proportionality of surveillance.[87] Instead, they recommend that oversight be performed by all branches of government, including executive inspectors general or supervisory bodies, as well as civilian agencies.[88] For these authorities, oversight mechanisms must have sufficient resources and access to pertinent information in order to serve as an effective check on the power of law enforcement or security agencies.[89] There must also be a measure of public scrutiny; for example, anyone should be able to bring a claim before an oversight body, and its periodic reports and decisions about individual complaints should be publicly accessible.[90]

As the European Court recognized in *Zakharov*, communications service providers also have the potential to be a check on intelligence services and law enforcement agencies.[91] Communications service providers execute judicial orders for surveillance and can challenge those that are overly broad or illegal.[92] They can also increase transparency about how surveillance is conducted by disclosing the numbers of requests for interception and communications data that they receive.[93] Whistleblowers offer another potential check on the power of public authorities to conduct surveillance, and experts have emphasized the need for protections for those who act in good faith when disclosing information "to the media or the public at large if they are made as a last resort and pertain to matters of significant public concern."[94]

[86] La Rue Report 2013, ¶ 81; Office of the Special Rapporteur for Freedom of Expression, Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, OEA/Ser.L/V/II.CIDH/RELE/INF. 11/13 (December 31, 2013) ¶ 165.

[87] *See, e.g.*, OHCHR Report, ¶ 37; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, ¶¶ 84, 87; *Rotaru* v. *Romania*, ¶ 59; *Zakharov* v. *Russia*, ¶¶ 258–63.

[88] *See* OHCHR Report, ¶ 37; Scheinin Report 2010, ¶ 8.

[89] *See, e.g.*, Scheinin Report 2010, ¶ 9; *Zakharov* v. *Russia*, ¶¶ 274–81. The former UN Special Rapporteur for counterterrorism and human rights has praised the Norwegian parliamentary oversight mechanism, and the European Court has approved systems in Germany and the United Kingdom. Scheinin Report I 2009, ¶ 45; *Klass and others* v. *Germany*; *Weber and Saravia* v. *Germany*; *Kennedy* v. *United Kingdom*, ¶¶ 166–68; *Szabo and Vissy* v. *Hungary*, ¶¶ 82–83. *But see* La Rue Report 2013, ¶ 59 (expressing concern that the German G-10 law permits warrantless surveillance of communications by the intelligence services).

[90] *See, e.g.*, *Szabo and Vissy* v. *Hungary*, ¶¶ 82–83.

[91] *Zakharov* v. *Russia*, ¶ 270.

[92] OHCHR Report, ¶ 38.

[93] La Rue Report 2013, ¶ 92; Inter-American Commission for Human Rights, *Freedom of Expression and the Internet*, ¶ 113; "Report of the Freedom Online Coalition Working Group Three, Privacy and Transparency Online," November 2015, pp. 43–45.

[94] Scheinin Report II 2009, ¶ 16; La Rue Report 2013, ¶¶ 52, 79, 84; UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Inter-American Commission on Human Rights Special Rapporteur for Freedom of Expression, "Joint Statement on WikiLeaks" (December 21, 2010).

D *Access to Effective Remedy*

Closely linked to oversight is the requirement that states ensure access to an effective remedy for anyone who claims that her rights have been violated.[95] The remedy may be through a judicial or nonjudicial mechanism that has the capacity to bring about the investigation, prosecution, and sanction of those responsible for violations (if applicable) and to provide an adequate remedy for the victim.[96] Any mechanism should be independent and have access to the evidence necessary to determine claims before it.[97]

The secret nature of communications surveillance can render access to justice more tenuous for those who claim a violation of their right to privacy. As a result, human rights tribunals and experts are increasingly recommending that authorities provide notice to targets of surveillance once the surveillance has ceased.[98] States, however, have generally resisted this practice as impractical or detrimental to surveillance operations and methods. If a state does not provide notice, it should have liberal rules on standing to bring claims that challenge covert surveillance regimes.[99] If an individual's right to privacy is found to have been violated, adequate remedies may include a declaratory judgment, damages, and injunctive relief against the orders that permit data to be intercepted or retained. Publication of decisions determining the rights of complainants also contributes to transparency and constitutes part of such a remedy.[100]

Although significant gaps between law and practice remain, a fairly comprehensive set of rules has emerged in the jurisprudence of the European Court of Human Rights. Surveillance programs are more likely to be consistent with international human rights law when they are strictly regulated by law, overseen by a number of independent and properly resourced bodies, capable of being challenged, and marked by the greatest degree of transparency possible. At the same time, human rights law itself has fallen short in two respects. First, its rules apply to states, rather than to the private actors who hold this personal data, and second, it has only recently begun to address the privacy protections that should apply to communications when they transit borders. The next section examines how European

[95] ICCPR art. 2(3); European Convention art. XX; American Convention art. 25.

[96] *See, e.g.*, *General Comment No. 31*, ¶¶ 8, 15–19; *Velasquez Rodriguez* v. *Honduras*, ¶¶ 174 et seq.

[97] Scheinin Report II 2009, ¶¶ 10–12.

[98] *See, e.g.*, La Rue Report 2013, ¶ 82; *Weber and Saravia* v. *Germany*, ¶ 135; *Zakharov* v. *Russia*, ¶ 287. *But see* OHCHR Report, ¶ 40 (determining that subsequent notice is not necessary but closely related to the question of effective remedy); *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department* v. *Tom Watson and Others*, Eur. Ct. H.R., App. Nos. 203/15 and 698/15, ¶ 121 (December 21, 2016).

[99] *Zakharov* v. *Russia*, ¶¶ 171, 298.

[100] *See, e.g.*, *Association for European Integration and Human Rights and Ekimdzhiev* v. *Bulgaria*, ¶ 102; *Kennedy* v. *United Kingdom*, ¶ 167.

institutions seek to fill the first gap by interpreting EU data protection norms in light of the rights to privacy and data protection. The following section describes how both UN and European interpretations of the right to privacy are evolving to address the flow of digital communications across national borders.

IV DATA PROTECTION AND THE RIGHT TO PRIVACY

While human rights law sets out the obligations of states that are parties to human rights treaties, data protection laws and principles regulate practices of both state and private actors that can affect the right to privacy. The protection of personal information has historically been regarded as a component of the right to privacy,[101] yet with the adoption of the Charter of Fundamental Rights of the European Union in 2009, data protection became a distinct fundamental right in Europe.[102] UN Special Rapporteur Martin Scheinin has opined that a right to data protection is emerging at a global level as well.[103] While it is not recognized as such in human rights treaties outside of Europe, interpretations of data protection law that are closely tied to international human rights standards may convert this body of law into an effective tool for protecting rights at the domestic and international levels.

In terms of international law and guidelines, data protection principles are contained in the Council of Europe's Data Protection Convention,[104] the OECD Privacy Framework,[105] and the Asia Pacific Economic Cooperation Privacy Framework.[106] They are reflected in the newly adopted EU General Data Protection Regulation, which applies in the 28 EU member states, and in the proposed EU Regulation on Privacy and Electronic Communications.[107] They include the

[101] *See, e.g.*, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, January 8, 1981, C.E.T.S. No. 108, in force October 1, 1985, art. 1 ("Data Protection Convention"); *S. and Marper* v. *United Kingdom*, ¶ 103; *Van Hulst* v. *Netherlands*, Comm. No. 903/1999, U.N. Doc. CCPR/C/82/D/903/1999 (November 15, 2004) ¶ 7.9; Scheinin Report II 2009, ¶ 55; *General Comment No. 16*, ¶ 10; Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, ¶¶ 138–42; Solove, "Conceptualizing Privacy."

[102] Charter of Fundamental Rights of the European Union, art. 8(1); Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, pp. 47–390, art. 16(1).

[103] Scheinin Report II 2009, ¶ 12.

[104] Data Protection Convention, arts. 5–8.

[105] Organisation for Economic Co-operation and Development, Recommendation of the Council Concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, C(80)58/FINAL, as amended on July 11, 2013 by C(2013)79 ("OECD Privacy Framework").

[106] APEC Privacy Framework, Publication APEC#205-SO-01.2 (December 2005).

[107] Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88; European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/

principles that the collection and use of personal data – including communications data – should be in accordance with the law, subject to limitations, and strictly for the fulfillment of purposes that are clearly articulated to the data subject. Data should be deleted when it is no longer necessary for the purposes that justified collection. The entity collecting personal data should only disclose that data to other parties by the authority of the law or if the data subject has consented. Individuals should have notice about, and a measure of control over, the ways in which their data is collected, used, and shared, as well as ways to hold states and private actors accountable for violations.[108] These principles echo the international human rights standards laid out in the previous section, and they form the basis of strong domestic data protection laws in states such as Canada, Argentina, Israel, and Japan.[109]

The Court of Justice of the European Union (CJEU) has interpreted EU data-protection law in light of the rights to privacy and data protection established in the EU Charter of Fundamental Rights, and its recent decisions have had sweeping impacts on public and private actors in Europe and beyond its borders. In 2014, the CJEU ruled that an EU law that allowed member states to mandate the storage of communications metadata for periods of between six months and two years was inconsistent with the rights to data protection and privacy.[110] According to the CJEU, telephony metadata "may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained." It determined that the retention of data of persons who were not linked to crimes was problematic, and the legal framework lacked clear rules as to how authorities should access and use that data.[111]

The CJEU reiterated its holding in *Tele2 Sverige*, indicating that "the general and indiscriminate retention of all traffic and location data" was not strictly necessary to achieve the aim of fighting serious crime and terrorism.[112] It added that member states' laws could permit the targeted retention of metadata for the purpose of fighting serious crime; they could also permit the retention of data from one or more geographical areas where "objective evidence" demonstrates a clear link "to fighting serious crime or to preventing a serious risk to public security."[113] These holdings are consistent with *Weber and Saravia*, *S. and Marper*, and other case law

EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 (final), January 10, 2017.

[108] *See* Data Protection Convention, arts. 5–10; OECD Privacy Framework.

[109] *See, e.g.*, Federal Law for the Protection of Personal Data in the Possession of Private Actors (Mexico) (July 5, 2010); Law on the Protection of Personal Data (Argentina), Law 25.326 (October 30, 2000); *see also* "Global Trends in Privacy Protection."

[110] *Digital Rights Ireland*.

[111] Ibid., ¶¶ 27, 58–68.

[112] *Tele2 Sverige*, ¶ 103. Where *Digital Rights Ireland* dealt with the EU Data Retention Directive, *Tele2 Sverige* addressed domestic data-retention laws in the United Kingdom and Sweden.

[113] Ibid., ¶¶ 106–111. The CJEU also held that authorities must notify individuals whose data has been retained once notification is unlikely to jeopardize the relevant investigations. Ibid., ¶ 121.

of the European Court of Human Rights,[114] but unlike the latter judgments, they could be implemented immediately by private actors, who were no longer subject to the retention mandate. As such, the judgments had the practical effect of limiting the amount of data accessible to state authorities for surveillance.

In the *Google Spain* case, the CJEU further demonstrated the capacity of data-protection law to regulate the privacy practices of non-state actors. The CJEU held that search engine providers must respond to requests from individuals to de-index their names from search results. Such requests must be honored when the information linked to their names is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue," unless the public interest in finding this information is determined to outweigh the individual's privacy rights.[115] Several civil society organizations have argued that the decision improperly placed private companies in the role of public authorities charged with balancing rights and interests. The counterpoint is that perhaps any actor that can impact an individual's fundamental rights, as defined in the EU Charter, should assume this level of responsibility.

By providing an explicit legal link between the practices of some of the largest multinational corporations and human rights, EU law creates more opportunities for individuals to challenge the practices of large entities. Similarly, it increases the power of European authorities to regulate these companies, both in Europe and abroad. The CJEU's decisions may also help to define the scope of companies' responsibility to respect users' privacy rights, a topic that is explored in greater depth in Chapter 11 of this volume.[116]

As human rights norms become a greater foundation for data protection law, EU authorities are also increasingly applying the latter to data that crosses international borders. The next section examines how the challenge of cross-border data flows is gradually being met by developments in both international human rights law and EU data protection law. It also notes the outstanding dilemmas to which neither body of law has definitively spoken yet.

[114] *S. and Marper* v. *United Kingdom*, ¶ 125. In this case, the European Court looked to the Data Protection Convention to interpret the scope of the right to privacy enshrined in Article 8 and held that the indefinite retention of biometric data of individuals suspected of committing criminal offenses was inconsistent with Article 8.

[115] *Google Spain SL and Google Inc.* v. *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, CJEU, C-131/12, ECLI:EU:C:2014:317 (May 13, 2014), ¶¶ 94, 97.

[116] Civil society organizations and human rights experts have increasingly analyzed private companies' data-collection practices in light of their responsibilities per the UN Guiding Principles on Business and Human Rights. *See, e.g.*, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, A/HRC/32/38 (May 11, 2016); Cannataci Report ¶ 46(f); Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, ¶ 112; "Report of the Freedom Online Coalition Working Group Three, Privacy and Transparency Online"; Ranking Digital Rights, 2015 Corporate Accountability Index (November 2015), pp. 16–18.

V ENSURING THE RIGHT TO PRIVACY EXTRATERRITORIALLY

The privacy protections contained in human rights law have traditionally addressed states' conduct regarding their subjects' data within their own borders. But digital communications flow seamlessly across borders, challenging traditional paradigms of jurisdiction over individuals and information.[117] This means that privacy protections may be illusory when governments with sophisticated surveillance capabilities can access the communications data of people who are not subject to their jurisdiction.

A *The Extraterritorial Application of the Right to Privacy*

International human rights law provides little guidance as to the obligations of states vis-à-vis non-nationals located beyond their territories whose communications are targeted or simply swept up in bulk surveillance programs.[118] The ICCPR requires a state party "to respect and to ensure to all individuals within its territory and subject to its jurisdiction" the rights contained in the Convention without discrimination.[119] The Human Rights Committee and the ICJ have interpreted this language as a disjunctive, meaning that a state's duty extends to "anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[120] A contrary interpretation would allow states to avoid their human rights obligations when exercising jurisdiction outside of their territories and be inconsistent with the object and purpose of the treaty.[121] The United States and Israel have disagreed with this position, and for many years the United States advocated a "strict territoriality" reading of Article 2 of the ICCPR, although its position seems to have softened in recent years.[122]

When the European Court of Human Rights has addressed the extraterritorial conduct of its Contracting Parties, it has found effective control to be present in two types of situations: when state agents "exerci[se] control and authority over an

[117] *See, e.g.*, J. Daskal, "The Un-territoriality of Data (2015) **125** *Yale Law Journal* 326–397.

[118] *See, e.g.*, *Weber* v. *Saravia*, ¶72 (in which the European Court declined to determine whether a complaint filed by applicants located outside of Germany alleging violations of their privacy rights by the German state was admissible *ratione personae*); *see also* Submission of Privacy International et al., OHCHR consultation in connection with General Assembly Resolution 68/167, "The right to privacy in the digital age," April 1, 2014.

[119] ICCPR art. 2(1).

[120] *General Comment No. 31*, ¶ 10; *see also Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 ICJ Rep. 136, ¶¶ 109–11; I/A C.H.R., Report No. 109/99, Case 10.951, *Coard et al.* (United States), September 29, 1999, ¶ 37.

[121] *Legal Consequences of the Construction of a Wall*, ¶ 109.

[122] *See, e.g.*, United States Department of State, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights, October 19, 2010; UN Human Rights Committee, "Human Rights Committee considers report of the United States," March 14, 2014, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14383; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ¶ 110.

individual" (the personal model of jurisdiction), or when a state occupies a foreign territory through military action and assumes responsibility for some or all of the public functions normally performed by the government in that territory (the spatial model).[123] Yet this analysis of the degree to which state agents exercise physical control over individuals is ill-suited to the nature of communications surveillance, where control over infrastructure and individuals is virtual.[124] Communications surveillance programs most often involve a state's collection and review of data from its own territory, even though the communications may originate and terminate in other states and the rights holders may be beyond the collecting state's jurisdiction.[125] Some types of collection more clearly involve extraterritorial action – e.g., a state's interception of communications traffic via equipment located in its embassies abroad – but the impact on rights occurs in a different manner from the exercise of "effective control" over persons or territory.

Noting the mismatch between the prevailing test for extraterritorial obligations and the facts surrounding communications surveillance, several human rights experts have maintained that when analyzing a state's exercise of jurisdiction, one should look at its control over *rights* rather than over individuals or territory. Therefore, in the context of communications surveillance, it is the assertion of authority in ways that affect the rights of individuals that triggers a state's human rights obligations, even with respect to a person with no connection to that state.[126] For Marko Milanovic, in most (if not all) of the situations described in the Snowden documents, the state's obligation to *respect* the human rights of impacted individuals outside of its territory should apply.[127] Consequently, the state's interference with an

[123] *Al-Skeini* v. *United Kingdom*, Eur. Ct. H.R., App. No. 55721/07, ¶¶ 133–40 (Grand Chamber, July 7, 2011). Notably, the two cases before the European Court dealing with extraterritorial communications surveillance involved applicants who were both nationals and non-nationals, and the court did not address the state's obligations to the latter. *Weber and Saravia*, ¶¶ 72; *Liberty* v. *United Kingdom*, Eur. Ct. H.R., App. No. 58243/00 (July 1, 2008).

[124] *See* J. Daskal, "Extraterritorial Surveillance under the ICCPR … The Treaty Allows It!," *Just Security*, March 7, 2014, www.justsecurity.org/7966/extraterritorial-surveillance-iccpr-its-allowed/.

[125] *See, e.g.*, M. Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015) **56**(1) *Harvard International Law Journal* 81–146.

[126] *See, e.g.*, Letter to the Editor from M. Nowak, "What does extraterritorial application of human rights treaties mean in practice?," *Just Security*, March 11, 2014, www.justsecurity.org/8087/letter-editor-manfred-nowak-extraterritorial-application-human-rights-treaties-practice/; Letter to the Editor from Former Member of the Human Rights Committee, M. Scheinin, *Just Security*, March 10, 2014, www.justsecurity.org/8049/letter-editor-martin-scheinin/; P. Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism" (2014) **82** *Fordham Law Review* 2137–2167 at 2148–52 (arguing that a state exercises "virtual control" over communications infrastructure when it conducts surveillance).

[127] *See, e.g.*, "The NSA in Global Perspective"; "Human Rights Treaties and Foreign Surveillance," 118–119; *see also* Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights, pp. 49–50, 55–56 (arguing that a state may have obligations based on a sliding scale, and proposing that "once a state exercises authority or effective control over an individual or context, it becomes obligated to respect Covenant rights to the extent of that exercise of authority").

individual's privacy rights must be in pursuit of a legitimate aim and be a necessary and proportionate means of achieving that aim. The state's positive obligation to ensure rights, however, would only apply to individuals located within its territory. Others would eschew the control test entirely and contend that laws that offer distinct protections based on the nationality or location of the subject of surveillance are difficult to justify under human rights law.[128]

In *The Right to Privacy in the Digital Age*, the OHCHR found several of the aforementioned arguments regarding a state's extraterritorial human rights obligations to be compelling at a high level, writing:

> [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, 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.[129]

The report adds that, according to the principle of nondiscrimination contained in the ICCPR, states must respect the legality, necessity, and proportionality principles regardless of the nationality or location of the subject of communications surveillance.[130]

The OHCHR explicitly declined to limit the scope of the state's obligations to subjects of communications surveillance beyond its borders to that of merely respecting rights, in a manner similar to the statements of the ICJ and the Human Rights Committee. This leaves open the question of whether, under the ICCPR, a state may have a duty to *ensure* the rights of these individuals, even though the basis for jurisdiction may be a fleeting or virtual action. If this is the case, many of the obligations outlined above could flow to state action that has a definitive impact on the privacy rights of individuals beyond its territory. Extraterritorial surveillance would have to be based on laws that are consistent with international human rights standards and be subject to effective oversight. Any individual whose rights were

[128] A. Deeks, "An International Legal Framework for Surveillance" (2015) **55** *Virginia Journal of International Law* 251–367 at 310–11; *see also* Daskal, "Extraterritorial Surveillance" (arguing that the conduct of surveillance on foreign nationals abroad is not covered by the ICCPR).

[129] OHCHR report, ¶ 34.

[130] Ibid. ¶ 36; *see also* La Rue Report 2013, ¶¶ 64, 87; *Concluding observations on the fourth periodic report of the United States of America*, U.N. Doc. CCPR/C/USA/CO/4 (April 23, 2014), ¶ 22 (maintaining that the state's obligations in the realm of privacy rights do not differ depending on the nationality or location of the target of surveillance).

impacted must have access to an effective remedy, and regulation of non-state actors would extend to extraterritorial actions as well.

The United States' 2014 update to its signals intelligence policy, requiring that intelligence gathering "include appropriate safeguards for the personal information of all individuals" irrespective of their nationality or location,[131] is the most explicit action taken by a state to date to extend protections to those impacted by its extraterritorial surveillance. In light of the broad powers contained in the UK Investigatory Powers Act and other laws, more detailed interpretations of these obligations from UN mechanisms or from the European Court are needed to guide state action.

B *EU Data Protection Law and Extraterritorial Privacy Protections*

This chapter has argued that European authorities are interpreting data protection law in a way that fills the gaps in privacy protections left by international human rights law. As part of this effort, they are also increasingly applying EU data protection law extraterritorially, in an attempt to fill the void of uncertainty regarding the protections that adhere to individuals' communications data when it crosses borders. In doing so, EU authorities may ultimately elevate privacy protections for communications well beyond the European continent.

The new EU General Data Protection Regulation and the proposed Privacy and Electronic Communications Regulation specify that they are binding on companies located outside of the EU that offer services to data subjects within the EU or otherwise monitor their behavior.[132] Since 1995, EU law has restricted the transfer of personal data outside of Europe to states that are deemed to have an adequate level of legal protection for the privacy rights of individuals.[133] The CJEU has interpreted this provision to mean that a third country must offer "a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union" in order for general transfers to that country to be approved.[134] A multinational company may also transfer data to a state that has not been deemed adequate if the company commits to providing adequate safeguards.[135] Furthermore, the recently adopted EU-US Umbrella Agreement establishes privacy protections for the personal data of Europeans (as well as persons from the United

[131] Presidential Policy Directive/PPD-28, Signals Intelligence Activities, The White House, January 17, 2014.

[132] Regulation (EU) 2016/679, art. 3; Proposal for a Regulation on Privacy and Electronic Communications, art. 3.

[133] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031–0050, arts. 25, 26(2).

[134] *Maximilian Schrems* v. *Data Protection Commissioner*, CJEU, C-362/14, ECLI:EU:C:2015:650, ¶ 73 (emphasis added).

[135] Regulation (EU) 2016/679, arts. 44–50.

States) in the context of criminal law enforcement cooperation.[136] With these instruments, EU authorities aim to achieve a baseline level of privacy protection for their subjects' communications and other personal data vis-à-vis foreign actors from the private and public sectors, regardless of where they are located or where they handle that data.

National authorities in the EU are also seeking to apply EU data protection law extraterritorially by requiring companies to comply on a worldwide basis, as opposed to only with reference to sites directly aimed at the specific jurisdiction in question. For example, following the CJEU's *Google Spain* decision, French data protection authorities ordered Google to de-index search results that fit the judgment's criteria on a global scale, in order to protect data subjects' privacy rights more effectively.[137] Google had previously ensured that no users located in the European Union could access de-indexed results, but French authorities seek to make de-indexing decisions applicable across the global Internet. If upheld on appeal, this judgment could extend the reach of certain European data protection norms internationally.[138]

In addition to strengthening protections for the privacy rights of Europeans regardless of where their data flows, the European approach may also elevate privacy protections for individuals outside of the region. A handful of non-EU states have been designated as having adequate data protection standards by the European Commission, and this stable basis for data transfer is attractive for trading partners. In the wake of the Snowden revelations, the CJEU used this mechanism to push for changes in US surveillance law. In the *Schrems* case of 2015, the CJEU invalidated the European Commission's decision that the US legal regime offered an adequate level of protection for data subjects under the Safe Harbor Agreement reached between the US government and the European Commission. The CJEU determined that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications" for national security purposes was inconsistent with the right to privacy.[139]

The *Schrems* decision had the potential to halt a significant portion of the transatlantic flow of personal data, prompting US and EU authorities to negotiate the Privacy Shield agreement as a replacement.[140] US authorities have also supplemented the agreement with detailed explanations of US surveillance law and

[136] Council of the European Union, "Umbrella agreement: EU ready to conclude with the US," December 2, 2016, www.consilium.europa.eu/en/press/press-releases/2016/12/02-umbrella-agreement/.

[137] A. Hern, "Google says non to French demand to expand right to be forgotten worldwide," *The Guardian*, July 30, 2015.

[138] A. Hern, "Google takes right to be forgotten battle to France's highest court," *The Guardian*, May 19, 2016.

[139] *Schrems*, ¶ 93. The CJEU also found insufficient evidence that Europeans could obtain an effective remedy for violations of their privacy rights. Ibid. ¶ 95.

[140] *See* www.privacyshield.gov.

practice. Nevertheless, the adequacy of the US legal regime continues to be impugned.[141] States beyond Europe are also following the region's example when updating data protection laws, by limiting the legal bases for collecting personal data and restricting the flow of data to states that are deemed adequate.[142] Thus, the ultimate legacy of the *Schrems* case may be a gradual harmonization of data protection standards among key parts of the data economy, with EU rules serving as the foundation.

Despite the evolution of international human rights law and EU data protection law regarding privacy and cross-border data flows, clear rules have not yet emerged to address which state's privacy protections should apply to communications data when multiple governments assert jurisdiction over it.[143] In a case involving Microsoft in the United States, a federal appeals court ruled that the location of the data should determine which state may claim jurisdiction (and which privacy protections apply).[144] The UK Investigatory Powers Act allows the government to issue extraterritorial warrants for communications data if the data is held by a company that is subject to its regulatory jurisdiction.[145] For Jennifer Daskal, both approaches to jurisdiction are unsatisfactory, given the mobility of data, the incentives for companies and governments to decide who may access data based on where it is stored, and the conflict of laws which companies may face.[146] Instead, Daskal poses that the law should allow for multiple jurisdictional triggers to be evaluated, including the nationality and location of the data subject.[147] The absence of clear rules on jurisdiction and privacy protections in this scenario has led to calls for international law to fill the void through the negotiation of an international treaty[148] or smaller bilateral or multilateral agreements.[149] From a human rights perspective, the OHCHR's position should guide the development of any such framework: The

[141] *Digital Rights Ireland* v. *Commission*, T-670/16, Action brought September 16, 2016.

[142] *See, e.g.*, E. Kosinski and S. Asayama, "Transfer of Personal Data under Japan's Amended Personal Information Protection Act," White and Case Technology Newsflash, October 13, 2015; P. A. Palazzi, "New Draft of Argentine Data Protection Law Open for Comment," International Association of Privacy Professionals, February 8, 2017; "Brazil Releases Draft Data Protection Bill," Hunton and Williams Privacy and Information Security Law Blog, February 6, 2015.

[143] Daskal, "The Un-territoriality of Data" at 365–70, 373–78; J. Daskal, "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues" (2016) 8 *Journal of National Security Law & Policy* 473–501.

[144] *In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp.*, Case 14–2985, Document 286–1 (2d Cir. July 14, 2016).

[145] Investigatory Powers Act, §§ 41–43, 85, 52, 126–27, 149, 168–69, 190.

[146] "The Un-territoriality of Data," 389–95; "Law Enforcement Access to Data Across Borders," 487–91.

[147] "The Un-territoriality of Data," 395.

[148] B. Smith, "Time for an international convention on government access to data," Microsoft Corporate Blogs, January 20, 2014.

[149] Daskal, "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues" at 492–94.

privacy protections that attach to a person's communications when she transits borders or when jurisdiction is disputed should be those that are contained in international human rights law. Any state that impacts those rights – by accessing the data or sharing it with another state – should be required to ensure those protections. UN experts and the European Court of Human Rights can support efforts to establish robust and predictable privacy protections that transcend borders by continuing to develop standards on the universality of privacy rights in the digital age.

VI CONCLUSION

Developments in communications technology, coupled with revelations by Edward Snowden and others, have demonstrated that while human rights law has a well-developed body of standards on the right to privacy in communications, there are key areas where these standards fall short. The bulk collection of communications data seems generally permitted but circumscribed in human rights law, although few states appear to conduct such surveillance in accordance with these limits. Rules regarding the protections that apply to communications and other personal data when they are in the hands of private companies or when they transit borders are evolving, but at present are incomplete.

The most impactful recent development in this space may be the interpretation of EU data protection law in a way that incorporates or converges with the right to privacy. EU institutions are using data protection norms and enforcement mechanisms to give individuals stronger protections against the public and private actors that access their communications, regardless of location. This approach has the potential to contribute to stronger privacy protections beyond Europe, as its norms are increasingly replicated by other states seeking determinations of adequacy. Ideally, the European approach will also prompt UN mechanisms and governments to come together to devise more global solutions for the protection of privacy in the digital age, with international human rights law as their foundation.