Fordham Law Review

Volume 82 | Issue 5 Article 7

2014

The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism

Peter Margulies
Roger Williams University School of Law

THE NSA IN GLOBAL PERSPECTIVE: SURVEILLANCE, HUMAN RIGHTS, AND INTERNATIONAL COUNTERTERRORISM

*Peter Margulies**

INTRODUCTION

Revelations that the U.S. National Security Agency (NSA) conducts substantial surveillance abroad[1] have reinvigorated debate about the applicability of human rights law to surveillance performed outside a nation's territory. Recently, scholars have asserted that human rights law, including the International Covenant on Civil and Political Rights (ICCPR),[2] either does or should give foreign nationals abroad rights against U.S. surveillance.[3] Since the U.S. Supreme Court has generally extended rights against search and seizure under the Fourth Amendment only to U.S. citizens, legal permanent residents, or those physically present in the United States,[4] surveillance of non-U.S. persons abroad is typically not problematic under domestic law. The United States, however, may also have obligations under international law. President Obama's speech and policy directive on privacy in January 2014 proclaiming that "[*a*]*ll persons* should be treated with dignity and respect" and have "legitimate privacy interests in the handling of their personal information"[5] has intensified the focus on U.S. international obligations.

---

* Professor of Law, Roger Williams University School of Law. J.D., Columbia Law School; B.A., Colgate University. I thank Ken Anderson for comments on a previous draft.

1. *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 132–41 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter PRESIDENT'S REVIEW GRP.].

2. Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

3. *See* Marko Milanovic, *Foreign Surveillance and Human Rights*, EJIL: *TALK!* (Nov. 27, 2013), http://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-3-models-of-extraterritorial-application/; *cf.* David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SECURITY (Oct. 29, 2013, 12:48 PM), http://justsecurity.org/2013/10/29/foreigners-nsa-spying-rights/ (critiquing U.S. surveillance policy as shortsighted); Jennifer Granick, *Foreigners and the Review Group Report: Part 2*, JUST SECURITY (Dec. 19, 2013, 12:47 PM), http://justsecurity.org/2013/12/19/foreigners-review-group-report-part-2/ (same).

4. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990). This Article will refer to U.S. citizens and lawful permanent residents as "U.S. persons."

5. *See* Press Release, The White House, Office of the Press Sec'y, Presidential Policy Directive/PPD-28, at 5 (Jan. 17, 2014) [hereinafter PPD-28] (emphasis added), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/2014sigint.mem_.ppd_.rel_.pdf; *see also* Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE (Jan. 20, 2014, 11:02 AM), http://www.lawfareblog.com/2014/01/the-presidents-

Article 17 of the ICCPR protects individuals from "arbitrary or unlawful interference with [their] privacy, family. home or correspondence."[6] Under Article 2(1) of the ICCPR, each state that is a party to the agreement must "respect and . . . ensure to all individuals within its territory and subject to its jurisdiction" the rights provided for in the Covenant.[7] Debate has centered on the meaning of Article 2(1) for the United States since well before the NSA revelations.

While the United States' position has not been uniform since the ICCPR's drafting, its current position is that the ICCPR does not apply extraterritorially.[8] To support this position, the United States relies on the language of Article 2(1), which limits a state's duty to individuals "within its territory *and* subject to its jurisdiction."[9] However, international tribunals and most scholars reject this view. Many argue that the United States' reading of Article 2(1) is less persuasive than it appears to be, and that to achieve the ICCPR's purpose, a state must "respect" and "ensure" ICCPR rights both within its territory and anywhere else it has "effective control" of either territory or persons.[10] A broad view of both Article 2(1) and Article 17's bar on arbitrary interference with privacy would present substantial legal obstacles to the NSA's foreign surveillance.

This Article takes a middle ground that acknowledges that the United States has an extraterritorial duty under Article 2(1) to "respect" ICCPR rights including privacy, but then construes Article 17's prohibition on

---

speech-and-ppd-28-a-guide-for-the-perplexed/#.Ut23FKMo6po (analyzing the president's speech and policy directive).

6. ICCPR, *supra* note 2, art. 17.

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

8. *See* U.S. DEP'T OF STATE, SECOND AND THIRD PERIODIC REPORTS OF THE UNITED STATES OF AMERICA TO THE UN COMMITTEE ON HUMAN RIGHTS CONCERNING THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, at annex I (2005), *available at* http://www.state.gov/j/drl/rls/55504.htm#annex1; *see also* Michael J. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation*, 99 AM. J. INT'L L. 119, 123–24 (2005); Ashley Deeks, *Does the ICCPR Establish an Extraterritorial Right to Privacy?*, LAWFARE (Nov. 14, 2013, 12:00 PM), http://www.lawfareblog.com/2013/11/does-the-iccpr-establish-an-extraterritorial-right-to-privacy/#.Ut26AaMo6po. The latest report of the United States may reflect a softening of the U.S. position, although it is not a definitive shift. *See* U.S. DEP'T OF STATE, FOURTH PERIODIC REPORT OF THE UNITED STATES OF AMERICA TO THE UN COMMITTEE ON HUMAN RIGHTS CONCERNING THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS ¶ 505 (2011), *available at* http://www.state.gov/j/drl/rls/179781.htm#iii (noting the prior U.S. position, while acknowledging that the United States is "mindful" of the contrary U.N. Human Rights Committee view); *see also* Charlie Savage, *U.S. Seems Unlikely To Accept That Rights Treaty Applies to Its Actions*, N.Y. TIMES, Mar. 7, 2014, at A6. While the U.S. government will apparently not shift its stance, the matter generated substantial internal debate. *Cf.* Memorandum from Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, (Oct. 19, 2010), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1053853/state-department-iccpr-memo.pdf (urging that the United States agree that ICCPR requires that it "respect" rights extraterritorially).

9. ICCPR, *supra* note 2, art. 2(1).

10. *See* Al-Skeini v. United Kingdom, App. No. 55721/07, 53 Eur. H.R. Rep. 589, 647–50 (2011); *see also* Thomas Buergenthal, *To Respect and To Ensure: State Obligations and Permissible Derogations*, *in* THE INTERNATIONAL BILL OF RIGHTS 72, 74 (Louis Henkin ed., 1981).

arbitrary interference narrowly to permit NSA surveillance abroad, given the legal constraints already in place governing the NSA's efforts. With respect to Article 2(1), this Article makes two arguments. First, it asserts that the text of Article 2(1), viewed in light of other language in the ICCPR and the agreement's purpose, requires extraterritorial application. However, that application extends only to "respect" for ICCPR rights displayed in direct acts of U.S. officials, and not to a broader duty to "ensure" that non-U.S. officials or entities provide such rights. Second, the piece argues that the current "effective control" test for extraterritorial jurisdiction is too narrow to do justice to the pervasive capabilities of electronic surveillance. To better meet this challenge, the piece suggests a "virtual control" test that would make the ICCPR applicable when a state can assert control over an individual's communications, even though it lacks control over the territory in which the individual is located, or over the physical person of that individual.

However, the threshold Article 2(1) issue is only a prelude to the merits, which entail an inquiry into whether U.S. surveillance abroad is an arbitrary intrusion into privacy prohibited by Article 17 of the ICCPR. This portion of the piece also makes two arguments. First, I note that, despite differences in tone and emphasis, European law on privacy and national security surveillance does not diverge significantly from U.S. law. The European Court of Human Rights (ECHR) has upheld provisions in both British and German law that permit bulk surveillance of communications of foreign nationals abroad based on very broad substantive criteria, including national security, "serious criminal offences," and economic threats, as long as officials query bulk data with identifiers linked to those criteria.[11] Strikingly, the ECHR has understood that more detailed specification of conduct allowing surveillance would trigger a costly trade-off, as wrongdoers "adapt" their behavior to avoid surveillance and slip underneath the radar.

Second, I argue that even where the European and U.S. approaches diverge, the complementarity principle provides a measure of deference to U.S. approaches. Complementarity counsels deference based on both the imperatives of sovereignty[12] and other provisions of international law, including the law of armed conflict and U.N. Security Council resolutions that require global cooperation to combat terrorism. The deference prompted by complementarity allows a state to practice what I call procedural pluralism: flexibility in the procedural safeguards the state chooses, as long as those safeguards provide meaningful constraints on government. The U.S. surveillance policy fits within this zone of deference, because of the robust role of the Foreign Intelligence

11. *See, e.g.*, Weber v. Germany, 2006-XI Eur. Ct. H.R. 309 (upholding the German bulk content collection program).

12. Michael A. Newton, *A Synthesis of Community Based Justice and Complementarity*, *in* INTERNATIONAL CRIMINAL JUSTICE AND 'LOCAL OWNERSHIP': ASSESSING THE IMPACT OF JUSTICE INTERVENTIONS (Carsten Stahn ed., forthcoming) (manuscript at 5–10), *available at* http://ssrn.com/abstract=2081904.

Surveillance Court (FISC), which contrasts with the more limited role played by courts in Europe regarding surveillance requests. This increased judicial role compensates for the greater recourse that European law provides to subjects of surveillance, particularly given the significant exceptions to that recourse approved by European tribunals.

This Article proceeds in three parts. Part I briefly summarizes NSA surveillance abroad, including the parameters set out in President Obama's January 2014 speech and policy directive. Part II addresses the exterritorial application of the ICCPR. It describes the U.S. position and the opposing position taken by scholars who stress broad treaty coverage, and suggests a middle way. Part III argues that, based on complementarity and substantial overlap between NSA surveillance and programs approved by the ECHR, U.S. surveillance abroad meets the standard set out in Article 17 of the ICCPR. This Part also briefly suggests further reforms that would reinforce the case for the compliance of the United States.

I. NSA SURVEILLANCE ABROAD

Edward Snowden's disclosures have thus far centered on two NSA programs. One is domestic—the so-called metadata program, operated pursuant to section 215 of the USA PATRIOT Act,[13] and entailing the bulk collection of call record information, including phone numbers and times of calls.[14] The other is foreign—the PRISM program, operated pursuant to section 702 of the Foreign Intelligence Surveillance Act (FISA).[15] Under section 702, the government may conduct surveillance targeting the contents of communications of non-U.S. persons reasonably believed to be located abroad when the surveillance will result in acquiring foreign intelligence information.[16] The FISC must approve any government request for surveillance under section 702, although these requests can

13. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88 (codified at 50 U.S.C. § 1861 (2006)).

14. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y (forthcoming 2014), *available at* http://ssrn.com/abstract=2344774; Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, 1 LAWFARE RES. PAPER SERIES 1 (Sept. 1, 2013), http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf; David S. Kris, *On the Bulk Collection of Tangible Things*, 1 LAWFARE RES. PAPER SERIES 1 (Sept. 29, 2013), http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf; *cf.* Peter Margulies, *Evolving Relevance: The Metadata Program and the Delicate Balance of Secrecy, Deliberation, and National Security* (Roger Williams Univ. Sch. of Law Legal Studies Research Paper Series, Research Paper No. 146, 2014), *available at* http://ssrn.com/abstract=2400809 (arguing that section 215 should be read as entailing a fiduciary duty to safeguard both privacy and national security in light of fluid threats and technological shifts).

15. 50 U.S.C. § 1881a (Supp. V 2011).

16. *Id.* § 1881a(a).

describe broad types of communications without identifying particular individuals.[17]

Under section 702, "foreign intelligence information" that the government may acquire includes a number of grounds related to national security, such as information relating to an "actual or potential attack" or "other grave hostile acts of a foreign power or an agent of a foreign power."[18] It also includes information relating to possible sabotage[19] and clandestine foreign "intelligence activities."[20] Another prong of the definition appears to sweep more broadly, including information relating to "the conduct of the foreign affairs of the United States."[21] Despite the greater breadth of this provision, President Obama informed a domestic and global audience that U.S. intelligence agencies seek a narrow range of information centering on the national security and foreign intelligence concerns described above.[22] While the U.S. intelligence agencies acquire a substantial amount of data that does not fit under these rubrics, the president's speech confirmed that U.S. analysts do not rummage through such data randomly or for invidious purposes.[23] A scatter-shot approach of this kind would be unethical, illegal, and ineffective. Instead, NSA officials query communications using specific "identifiers" such as phone numbers and email addresses that officials reasonably believe are used by non-U.S. persons abroad to communicate foreign intelligence information.[24] The government must also have in place minimization procedures to limit the acquisition, retention, and dissemination of nonpublic information about U.S. persons.[25] The NSA deletes all irrelevant content, including content from non-U.S. persons, after five years.[26]

In acknowledging the "legitimate privacy interests" of both U.S. and non-U.S. persons, President Obama affirmed the U.S. commitment to core principles in January 2014.[27] First, he narrowed the operating definition of

17. *See* PRESIDENT'S REVIEW GRP., *supra* note 1, at 135–37. The attorney general and director of national intelligence can issue a determination that permits surveillance without prior FISC approval when exigent circumstances so require because without immediate action "intelligence important to the national security of the United States may be lost or not timely acquired." 50 U.S.C. § 1881a(c)(2). In this exigent situation, the attorney general and director of national intelligence must submit a certification to the FISC seeking authorization within seven days. *Id.* § 1881a(g)(1)(B).

18. 50 U.S.C. § 1801(e)(1)(A).

19. *Id.* § 1801(e)(1)(B).

20. *Id.* § 1801(e)(1)(C).

21. *Id.* § 1801(e)(2)(B).

22. *See* PPD-28, *supra* note 5, at 3–4.

23. *See id.*

24. *See* PRESIDENT'S REVIEW GRP., *supra* note 1, at 136; *cf. In re* Gov't's Ex Parte Submission of Reauthorization Certification for 702 Program, slip op. at 15–16, 22 (FISA Ct. Oct. 3, 2011) (Bates, J.), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf (describing the government's use of designated "facilities" and "selectors" with links to terrorism or other foreign intelligence information, including not only communications to or from phone numbers or e-mail addresses, but communications "about" these identifiers).

25. *See In re* Gov't's Ex Parte Submission, slip op. at 14.

26. *Id.* at 24.

27. PPD-28, *supra* note 5, at 5.

foreign intelligence information, limiting it to "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists."[28] In addition, he asserted that the NSA would engage in bulk collection of communications for purposes of "detecting and countering" terrorism, espionage, nuclear proliferation, threats to U.S. forces, and financial crimes, including evasion of duly enacted sanctions.[29] Addressing anticipated concerns that these limits still left the NSA with too much discretion, President Obama declared what the United States would *not* do. First, it would not collect communications content "for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion."[30] Second, it would disseminate and store information regarding any person based on criteria in section 2.3 of Executive Order 12,333[31]: cases involving "foreign intelligence or counterintelligence," public safety, or ascertainment of a potential intelligence source's credibility.[32]

Of course, President Obama's speech did not quell the complaints of NSA critics. One could argue that even the description the president provided has legal flaws under domestic and/or international law. One can also argue that the president's policy directive, statutory provisions, and case law cannot wholly eliminate the possibility of systemic or individual abuse of NSA authority. That said, there are compelling reasons for treating the president's speech and directive as an authoritative and binding statement of U.S. policy. The most compelling reason may be the simplest: no American president has ever been so forthright on the subject of intelligence collection, and few heads of state around the globe have ventured down the path that President Obama chose.[33] That alone counsels treating President Obama's guidance as more than "cheap talk."

II. EXTRATERRITORIALITY UNDER THE ICCPR

Despite President Obama's candor about some aspects of U.S. intelligence collection, the president said nothing about U.S. duties under the ICCPR. Because the section 702 program affects the communications of foreign nationals, that issue is vital. The threshold question concerns the extraterritorial reach of the ICCPR's obligations. Some bodies, like the U.N. Human Rights Committee (HRC) and some commentators, take the sweeping view that the ICCPR requires a state party to both respect and ensure that individuals are provided treaty rights within that state party's

28. *Id.* at 2 n.2 (citing Exec. Order No. 12,333, 3 C.F.R. 200, 204–05 (1981), *amended by* Exec. Order No. 13,470, 3 C.F.R. 218, 227 (2008), *reprinted as amended in* 50 U.S.C. § 401 app. at 934–43 (Supp. V 2011)).

29. *Id.* at 4.

30. *Id.* at 3.

31. *Id.* at 6.

32. *See* Exec. Order No. 12,333, 3 C.F.R. 200, 204–05, *amended by* Exec. Order No. 13,470, 3 C.F.R. 218, 227, *reprinted as amended in* 50 U.S.C. § 401 app. at 934–43.

33. *See* Wittes, *supra* note 5.

territory *or* whenever an individual falls under the state's jurisdiction.[34] The United States now asserts a starkly contrasting position: the ICCPR *never* applies extraterritorially.[35] I submit that the best path lies between these poles: considering the ICCPR's purpose of promoting human rights, but also taking into account the practical issues with requiring a state to both respect *and* ensure observance of those rights around the globe.

A. The Narrow View

The United States has for some years (although not always) taken the view that the text of Article 2(1) of the ICCPR does not support imposing extraterritorial application of the treaty's duties.[36] Article 2(1) binds each state party "to respect and to ensure to all individuals within its territory *and* subject to its jurisdiction the rights recognized in the present Covenant."[37] The principles of treaty construction in the Vienna Convention on the Law of Treaties[38] (VCLT) (accepted as customary by the United States) require reading a treaty "in accordance with the ordinary meaning . . . [of its] terms."[39] The "ordinary" meaning of two conditions connected by the conjunctive, "and," is that an obligation arises only upon satisfaction of *both* conditions. In other words, a state incurs obligations under the ICCPR only to individuals who are both "within its territory" *and* "subject to its jurisdiction."[40] This reading rules out extraterritorial application of the ICCPR's substantive duties. However, although this reading seems plausible at first blush, a fuller reading of the ICCPR's text raises substantial doubts.

As the distinguished scholar (and former International Court of Justice judge) Thomas Buergenthal has noted, this reading of the text of Article 2(1) clashes with other provisions of the agreement. At least two of the

34. CCPR General Comment 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant, U.N. Human Rights Comm., 80th Sess., Mar. 29, 2004 ¶ 10, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004) [hereinafter CCPR General Comment 31], *available at* http://www.unhchr.ch/tbs/doc.nsf/0/58f5d4646e861359c1256ff600533f5f?Opendocument; *see also* Buergenthal, *supra* note 10, at 72, 74. *See generally* Sarah H. Cleveland, *Embedded International Law and the Constitution Abroad*, 110 COLUM. L. REV. 225, 232–62 (2010) (discussing issues of extraterritorial application under the U.S. Constitution and international law).

35. Brian J. Bill, *Human Rights: Time for Greater Judge Advocate Understanding*, ARMY LAW., June 2010, at 54, 58; Robert J. Delahunty & John C. Yoo, *What Is the Role of International Human Rights Law in the War on Terror?*, 59 DEPAUL L. REV. 803, 835 (2010); Dennis, *supra* note 8, at 123–24.

36. *See* Cleveland, *supra* note 34 (plotting the course of the U.S. position over time); Dennis, *supra* note 8, at 123–24; Beth Van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now Is the Time for Change*, 90 INT'L L. STUD. 20, 57–59 (2014), *available at* http://www.usnwc.edu/getattachment/a88e97e5-11ec-4dfb-a013-4cfa5f8efe5a/The-United-States--Position-on-the-Extraterritoria.aspx. *But see* Boumediene v. Bush, 553 U.S. 723, 771 (2008) (holding that the U.S. naval base at Guantánamo Bay, Cuba, was within U.S. jurisdiction for purposes of the Constitution's Suspension Clause, although the base was on Cuba's territory).

37. ICCPR, *supra* note 2, art. 2(1) (emphasis added).

38. May 23, 1969, 1155 U.N.T.S. 331 [hereinafter VCLT].

39. *Id.* art. 31(1).

40. *See* Delahunty & Yoo, *supra* note 35, at 825.

ICCPR's substantive provisions, those involving the right of the nationals of a state to return to that state[41] and the right not to be tried in absentia,[42] make no sense if they do not protect individuals at least temporarily outside of a state's territory.[43] The provision regarding nationals' right to return would become a nullity if the ICCPR had no application outside a state's sovereign territory. The prohibition on trial in absentia would similarly have to be read to include entirely arbitrary distinctions between defendants absent from a trial but within a state's territory and those outside that territory. While scholars sympathetic to the narrow reading of the ICCPR have urged reading these particular provisions as exceptions to a general rule against extraterritorial application of the ICCPR,[44] this position seems unduly facile. If the ICCPR's substantive provisions do not square with a narrow reading of Article 2(1), that reading is less plausible than a reading of Article 2(1) in isolation suggests. Even looking only at the agreement's text, therefore, the "ordinary meaning" of the treaty as a whole modifies the meaning we should ascribe to the conditions set forth in Article 2(1).

These doubts expand if we move beyond the text of the ICCPR to other items that are integral to interpretation under Article 31 of the VCLT, including the drafting history of the provision. Eleanor Roosevelt, the U.S. chief delegate to the United Nations during the initial drafting of the ICCPR, insisted in 1950 on the mention of "territory" in Article 2(1) for a more modest reason than the rationale now posited by the United States. The key fear of the United States, as articulated by Roosevelt, was that in some cases exterritorial application would impose upon the United States affirmative duties to enforce a comprehensive regime of rights within each of the defeated Axis powers that the United States and its allies had occupied after World War II. The early wording of Article 2 imposed on a signatory state the duty to "*guarantee* to all persons residing on their territory and within their jurisdiction the rights defined in the present covenant."[45] The use of the term "guarantee" could have resulted in a U.S. commitment to assure the protection of rights within the states of the former Axis—countries whose commitment to democratic institutions was nascent and highly uncertain. As Roosevelt stated, the United States wanted to avoid "assuming an obligation to *ensure* the rights recognized in [the covenant] to the citizens of countries under United States occupation."[46]

Ensuring those rights would have presented significant difficulties for the United States under both domestic and international law. To properly ensure such rights, the United States might have been required to enact legislation establishing the rights of citizens of the then-occupied territories

41. *See* ICCPR, *supra* note 2, art. 12(2), (4).
42. *Id.* art. 14(3)(d).
43. *See* Buergenthal, *supra* note 10, at 74.
44. *See* Delahunty & Yoo, *supra* note 35, at 835.
45. *See* U.N. ESCOR, 6th Sess., 193d mtg. at 13, U.N. Doc. E/CN.4/SR.193 (May 15, 1950) [hereinafter HRC 193d mtg.] (emphasis added).
46. U.N. ESCOR, 6th Sess., 194th mtg. at 5, U.N. Doc. E/CN.4/SR.194 (May 16, 1950) [hereinafter HRC 194th mtg.] (emphasis added).

of Germany, Austria, and Japan.[47] Because the United States never intended to annex those states, whose continued sovereignty was central to the postwar plans of the Allies, Congress might not have had constitutional authority to legislate regarding rights of citizens of the Axis powers. Even absent constitutional objections, such legislation would have been extraordinarily difficult politically, a concern which all of the drafters of the ICCPR understood.

Moreover, "ensuring" the rights of Germans and other Axis citizens would have conflicted with the international law of occupation. Under that law, an occupying power must respect the prior laws of the occupied state. While an occupying power has some authority to decline to enforce laws that violate fundamental human rights, ensuring Axis compliance with all of the ICCPR's provisions would have exceeded this minimum standard.[48] Under the law of occupation, compliance with those provisions should have been left, as it was, to officials of the occupied state upon the conclusion of occupation.

The reluctance of the United States to stand surety for the former Axis powers did not indicate a refusal to accept responsibility for *direct actions* taken by U.S. personnel abroad. At one point in the debates over the drafting of the ICCPR, Eleanor Roosevelt acknowledged that "troops, although maintained abroad, remained under the jurisdiction of the State."[49] This acknowledgment, in response to comments by delegates from other states about the scope of state duties, strongly suggests that the United States conceded responsibility for the acts of its own personnel in the course of occupation. The acknowledgement is evidence that the United States did not regard the "jurisdiction" and "territory" requirements of Article 2(1) as conjunctive in all cases, but only in those situations that imposed unmanageable duties on states to ensure foreign governments' compliance.[50]

---

47. *See* HRC 193d mtg., *supra* note 45, at 13. In this passage, Roosevelt explained that, without the amendment including the term "territory" conjunctively with "jurisdiction," the treaty

> could be interpreted as obliging a contracting party to adopt legislation applying to persons outside its territory . . . [including persons] in the occupied territories of Germany, Austria and Japan, as persons living in those territories were in certain respects subject to the jurisdiction of the occupying Powers but were in fact outside the legislative sphere of those Powers.

Id.

48. *See* Adam Roberts, *Transformative Military Occupation: Applying the Laws of War and Human Rights*, 100 AM. J. INT'L L. 580, 585 (2006); *cf.* Marco Sassòli, *Transnational Armed Groups and International Humanitarian Law* 23–24 (Harvard Univ. Program on Conflict Resolution Occasional Paper Series, No. 6), *available at* http://www.hpcrresearch.org/sites/default/files/publications/OccasionalPaper6.pdf (discussing links between the law of occupation and the law on conflict with violent transnational groups such as al Qaeda).

49. HRC 194th mtg., *supra* note 46, at 9.

50. While the current U.S. position on extraterritorial application of the ICCPR has contributed to a certain global cynicism about the U.S. view of international law, the United States has often displayed high regard for international law and taken a leadership role, as Eleanor Roosevelt's participation in the drafting of the ICCPR illustrates. *See, e.g.*, Rebecca Ingber, *Interpretation Catalysts and Executive Branch Legal Decisionmaking*, 38 YALE J.

Moreover, the subsequent drafting history of the ICCPR reveals that the twin conditions imposed by Article 2(1) also focused on limiting the reach of the term, "ensure," regarding a state's obligations to its nationals abroad. Without textual restrictions, a state party to the ICCPR might be required to ensure the safety of its citizens abroad against the actions of another state in which those citizens were located. While a state may use diplomatic channels to protect its nationals abroad, it cannot ensure their safety against the actions of other states. The language adopted in Article 2(1) made clear that state parties to the treaty did not assume this impossible burden.[51] In addition, Article 1 of the First Optional Protocol to the ICCPR supports a disjunctive test, by acknowledging HRC authority to entertain complaints from "individuals subject to [a State Party's] jurisdiction."[52]

B. The Protective Approach

If the narrow approach favored by the United States fails to persuade, so does the sweeping endorsement of extraterritoriality provided by the HRC, which receives reports from states regarding their compliance with the ICCPR and hears individual complaints against states that have signed on to the First Optional Protocol. The HRC has asserted that states are *always* bound, within their territory and in other areas subject to their jurisdiction, to both respect and ensure that individuals receive rights under the ICCPR.[53] Because this approach focuses on maximum protection of human rights, I call it the protective approach.[54] Unfortunately, the protective approach embodies a stilted view of the ICCPR's text and purpose that

---

INT'L L. 359, 391–412 (2013) (discussing the importance to policymaking of U.S. mandatory reporting to U.N. treaty bodies such as the Committee Against Torture); *cf.* Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1835 (2009) (describing international and constitutional law as coordinated games in which parties including the United States relinquish short-term benefits to realize long-term gains); Harold Hongju Koh, *Transnational Legal Process*, 75 NEB. L. REV. 181, 194–99, 203–05 (1996) (describing how the United States interacts with transnational bodies, courts, and nongovernmental organizations in a dialogue framing international norms). *But see* JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 60 (2007) (critiquing the incentive structure of nongovernmental organizations as too often skewed against U.S. positions); Kenneth Anderson, *"Accountability" As "Legitimacy": Global Governance, Global Civil Society and the United Nations*, 36 BROOK. J. INT'L L. 841, 842–44 (2011) (same); J. Andrew Kent, *A Textual and Historical Case Against a Global Constitution*, 95 GEO. L.J. 463, 510–24 (2007) (suggesting caution in accounts of interaction between international law and American constitutionalism, especially in the formation of judicially enforceable rights).

51. *See* Buergenthal, *supra* note 10, at 74.

52. *See* Optional Protocol to the International Covenant on Civil and Political Rights, art. 1, *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 302 (entered into force Mar. 23, 1976). The Optional Protocol provides less compelling evidence of a disjunctive reading, because it was drafted after the original ICCPR, is optional, and has not been ratified by the United States. *See Status of Ratification of Human Rights Instruments*, UNITED NATIONS HUM. RTS. OFF. HIGH COMMISSIONER ON HUM. RTS. (Feb. 13, 2013), http://www.ohchr.org/Documents/HRBodies/HRChart.xls.

53. CCPR General Comment 31, *supra* note 34, ¶ 10.

54. *See* Peter Margulies, *The Fog of War Reform: Change and Structure in the Law of Armed Conflict After September 11*, 95 MARQ. L. REV. 1417, 1422 (2012).

unduly discounts the concerns with manageability that Eleanor Roosevelt articulated in the early debates on the treaty's drafting.

In finding that the conditions in Article 2(1), "within the territory" and "subject to the jurisdiction," apply disjunctively to duties of the states to both respect and ensure all rights under the ICCPR, the HRC relies on the "object[] and purpose[]" of the ICCPR.[55] Indeed, in invoking the object and purpose of the ICCPR under Article 31 of the VCLT, the HRC also invokes Article 26 of the VCLT, which declares the familiar customary principle that states must interpret their treaty obligations in good faith.[56] According to the HRC, the ICCPR's object and purpose is to extend human rights as comprehensively as possible around the globe and leave as few gaps as possible in human rights protection.[57]

Unfortunately, the protective view ignores the first component that any good faith interpreter should consult: the text of the source. Article 31(1) of the VCLT requires consideration of the "ordinary meaning" of treaty terms.[58] While, as Buergenthal noted in his 1981 article, Article 2(1) could have been drafted more clearly,[59] that failure of drafting does not license interpreters to import their own policy preferences without regard to the text. The language of Article 2(1) may not require a conjunctive reading of "territory" and "jurisdiction" per the U.S. position, but, even more clearly, it does not require a disjunctive reading that imposes on states a duty to both respect *and ensure* treaty rights. A more plausible reading limits the duty to ensure to cases where an individual is both within a state's territory and subject to its jurisdiction.[60] While some have argued that the rights-promoting nature of a multilateral treaty like the ICCPR justifies less regard for the agreement's text, an inappropriately expansive reading of the text sacrifices essential virtues of a treaty: predictability, legitimacy, and connection to state consent.[61]

The HRC's view, particularly its insistence on a comprehensive reading of a state's duty to "ensure" other states' or entities' compliance with treaty rights, fares no better in accounting for the ICCPR's purpose or drafting history. The HRC failed to recognize that a treaty's purposes, like those of a constitution or statute, may be the product of crosscutting interests and

55. CCPR General Comment 31, *supra* note 34, ¶ 5.

56. This is known as the *pacta sunt servanda* principle. *See* Eliav Lieblich, *Intervention and Consent: Consensual Forcible Interventions in Internal Armed Conflicts As International Agreements*, 29 B.U. INT'L L.J. 337, 361 (2011) (describing that principle as holding that "agreements must be kept").

57. *See* CCPR General Comment 31, *supra* note 34, ¶¶ 3–4.

58. VCLT, *supra* note 38, art. 31(1).

59. Buergenthal, *supra* note 10, at 74.

60. *See* Cleveland, *supra* note 34, at 252.

61. *See* Oona A. Hathaway, *Do Human Rights Treaties Make a Difference?*, 111 YALE L.J. 1935, 1960–61 (2002) (noting that the perception that human rights treaty interpretation is "legitimate in form . . . [but] less so in practice" can undermine adherence to treaty norms). For an insightful look at questions of treaty interpretation, see David S. Jonas & Thomas N. Saunders, *The Object and Purpose of a Treaty: Three Interpretive Methods*, 43 VAND. J. TRANSNAT'L L. 565 (2010).

agendas.[62] Eleanor Roosevelt's concern about open-ended state obligations is a countervailing factor that helped shape the ICCPR's object and purpose. States like the United States that signed and ratified the ICCPR because they counted on this tempering of their obligations are in a difficult spot under the HRC's expansive rule. That difficulty has the perverse effect of tempering state appetites for ratifying future human rights treaties.[63]

C. A Modified Purposive Approach to the Threshold Issue of ICCPR Applicability

Fortunately, there is an alternative to the sweeping approach taken by the HRC, reflected in the jurisprudence of the ECHR. In addressing the threshold question of the ICCPR's applicability, the ECHR has interpreted Article 2(1) in light of both the treaty's protective purpose and the difficulty of imposing comprehensive duties on states when the state's footprint in a particular domain is fleeting.[64] This approach requires a showing of de facto jurisdiction or control over either persons or territory to trigger the state's duty to "respect" an individual's rights under the ICCPR. A state has the additional duty to "ensure" the provision of those rights only when the individuals claiming rights are both within the state's territory *and* subject to its jurisdiction.[65]

In *Al-Skeini v. United Kingdom*, the ECHR explained that the test of jurisdiction could be met either through control of an individual or a geographic area.[66] The court noted that jurisdiction follows when a state's agents "exercise[] control and authority over an individual."[67]

---

62. *Cf.* City of Chi. v. Envtl. Def. Fund, 511 U.S. 328, 339 (1994) ("It is not unusual for legislation to contain diverse purposes that must be reconciled."); William W. Buzbee, *The One-Congress Fiction in Statutory Interpretation*, 149 U. PA. L. REV. 171, 179, 190–92 (2000) (discussing ambiguities in statutory interpretation); Curtis J. Mahoney, Note, *Treaties As Contracts: Textualism, Contract Theory, and the Interpretation of Treaties*, 116 YALE L.J. 824 (2007) (arguing for reading treaties according to their text, on the theory that states parties ascertain their duties in reliance on the text's plain meaning). I do not make this point to endorse a rigid reliance on treaty text, which is often ambiguous. I argue only that inquiries into treaty purposes often yield ambiguity as well.

63. *Cf.* Stephen C. Sieberson, *The Treaty of Lisbon and Its Impact on the European Union's Democratic Deficit*, 14 COLUM. J. EUR. L. 445, 452–53 (2008) (asserting that the unease of European states with constraints imposed by the European Union (EU) has been exacerbated by the EU's "non-majoritarian institutions" that are not accountable to the public for their decisions). I do not argue here that U.N. bodies like the HRC are fatally flawed because they are not majoritarian in nature. Rather, I argue that this aspect of U.N. bodies should prompt greater modesty in substantive positions such bodies adopt.

64. *See* Al-Skeini v. United Kingdom, App. No. 55721/07, 53 Eur. H.R. Rep. 589 (2011).

65. For a thoughtful analysis that limits a state's duty to "ensure" rights to its own territory, but pegs the duty to "respect" to direct state actions that infringe on rights anywhere around the globe, see MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY (2011), Marko Milanovic, *From Compromise to Principle: Clarifying the Concept of State Jurisdiction in Human Rights Treaties*, 8 HUM. RTS. L. REV. 411 (2008), and Milanovic, *supra* note 3.

66. *Al-Skeini*, 53 Eur. H.R. Rep. at 647–48.

67. *Id.* at 648; *see also* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶¶ 109–10 (July 9)

Alternatively, a state can exercise effective control over a geographic area, either directly, through its own armed forces, or through a "subordinate local administration."[68] In *Al-Skeini*, the court found that the United Kingdom, along with the United States, had assumed the "public powers" typically wielded by a sovereign state pursuant to the U.N. Security Council Resolution authorizing the occupation of Iraq by a multinational force after Saddam Hussein's overthrow.[69]

Importantly, the ECHR has moved away from the view that jurisdiction is an all-or-nothing inquiry. The facts of a case may demonstrate that a state had jurisdiction over a particular individual, even if the state did not have overall control of the territory where it gained control over the individual. For example, in *Ocalan v. Turkey*,[70] a case involving the handover in Kenya to Turkish officials of a suspect sought in Turkey for terrorist-related crimes, the ECHR noted that "the applicant was effectively under Turkish authority and therefore within the 'jurisdiction'" of Turkey after the handover was completed in Kenya.[71] In other words, a state need not exercise all "public powers" to meet the jurisdictional test; even exercise of "some" public powers may be sufficient.[72] Followed to its logical conclusion, permitting jurisdiction to hinge on the exercise of "some" public powers suggests that one state's jurisdiction is not necessarily exclusive of all other states: in *Ocalan*, Turkish officials in Kenya had jurisdiction over the suspect they had received from Kenyan authorities, even though Kenya clearly retained jurisdiction over its own territory, where the transfer of the suspect had occurred.[73] If this is true, jurisdiction may be divisible in a way suggested in the next subsection: jurisdiction over electronic communications may, as a de facto matter, be

---

(holding that the ICCPR applied to Israel's occupation of the West Bank). My citation of the International Court of Justice's *Wall* decision does not reflect agreement with its narrow view of the application of the right to self-defense only to "armed attacks" committed by other *states*, as opposed to nonstate actors such as terrorist groups. *See id.* ¶ 139; *cf.* Margulies, *supra* note 54, at 1473 n.253 (criticizing this aspect of the *Wall* opinion).

68. *Al-Skeini*, 53 Eur. H.R. Rep. at 648.

69. *Id.* at 650–51.

70. 2005-IV Eur. Ct. H.R. 131.

71. *Id.* at 164; *cf.* Cleveland, *supra* note 34, at 266 (discussing *Ocalan*); Jules Lobel, *Fundamental Norms, International Law, and the Extraterritorial Constitution*, 36 YALE J. INT'L L. 307, 356 (2011) (same).

72. *See* Bankovic v. Belgium, 2001-XII Eur. Ct. H.R. 333, 355. Because *Bankovic* held that North Atlantic Treaty Organization (NATO) countries were not responsible for harm incurred as a result of NATO's bombing of a Serbian-controlled broadcast station during the 1999 Kosovo campaign, commentators have viewed it as imposing a narrow test of effective control that requires some plenary control of persons or territory. The power to cause substantial consequences, including death, through direct state action, was deemed insufficient. *See* MILANOVIC, *supra* note 65, at 25, 57 (arguing that the ECHR in *Bankovic* adopted an unduly rigid conception of the reach of the ICCPR); *see also* Cleveland, *supra* note 34, at 262–64 (discussing *Bankovic*); Gerald L. Neuman, *Understanding Global Due Process*, 23 GEO. IMMIGR. L.J. 365, 376–77 (2009) (same). However, the assertion in *Bankovic* that an exercise of "all or some of the public powers" was necessary to find jurisdiction, 2001-XII Eur. Ct. H.R. at 355, should be read in tandem with subsequent decisions of the ECHR, such as *Ocalan* and *Al-Skeini*, which broadened the ICCPR's reach.

73. *Ocalan*, 2005-IV Eur. Ct. H.R. at 164–66.

shared between countries, even when only one of those states has jurisdiction over territory and persons. Dividing jurisdiction in this way establishes the ICCPR's threshold applicability to NSA surveillance abroad.

D. Virtual Control Is Also a Basis for Jurisdiction

I argue elsewhere that the growth of the virtual world of cyber and other electronic communication challenges traditional international law tests of state control, including the "effective control" test that represents the best synthesis of the ECHR's jurisprudence.[74] Notions of control that were adequate to analyze the actions in real time taken overseas by state officials or their alleged agents do not translate well into the cyber domain. Deterrence of problematic conduct in the cyber arena requires a broader test, which I call the virtual control standard. This test should also govern the showing necessary to support extraterritorial application of the ICCPR to surveillance abroad.

I argue in my forthcoming article that the effective control test does not provide adequate deterrence against states using nonstate actors to launch intrusions against other states in the cyber domain. The law of state responsibility for private actors imposes a demanding test on a state claiming that it has been victimized by another state through private actors: the responsible state must specifically direct the offending nonstate actors, or least train and equip them for the specific activity giving rise to the victim state's complaint. This demanding test makes sense for the realm of kinetic action, such as bombs or bullets. In that realm, I suggest, actions are often immediately apparent, while preparations are elaborate, creating built-in deterrents. In the *Military and Paramilitary Activities in and Against Nicaragua* case, for example, the International Court of Justice cited kinetic actions, including killings, kidnappings, and torture committed by the Nicaraguan Contra forces.[75] It also cited evidence of training that the Nicaraguan Contra forces received from the U.S. government in coercive interrogation.[76] Because of the nature of kinetic action, evidence to meet the effective control standard will be accessible to victim states. A victim state can survey visible damage to persons or property caused by a kinetic strike within its territory. Moreover, responsible states will also often confront significant obstacles of manageability, time, and distance in the use of kinetic means by nonstate agents.[77]

---

74. *See* Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 15 MELBOURNE J. INT'L L. (forthcoming 2014). *But see* INT'L GRP. OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 32–33 (Michael N. Schmitt ed., 2013) (arguing that the "effective control" test should apply to cyber warfare).

75. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 64 (June 27).

76. *Id.*

77. *See* Liz Sly, *U.S. Aid to Syrian Rebels Is Halted*, WASH. POST, Dec. 12, 2013, at A1 (discussing the problems with providing aid to rebels because of growing al Qaeda influence among rebel groups). That said, the difficulty of containing cyber attacks may also be a

As I suggest in my forthcoming article, however, the effective control test is inadequate for the cyber and communications realm.[78] Here, physical control over persons or territory is unnecessary.[79] The NSA can remotely control much of the communication of a foreign national abroad. It can eavesdrop on those communications and may be able to filter the communications received by that individual or alter the content the individual receives.[80] According to press reports, the NSA can break many forms of encryption used around the world because of "back doors" it has engineered in many software systems.[81] The NSA apparently also has the capacity to gain control of computers not directly connected to the internet, because of the implantation of tiny radio transmitters in many computers manufactured in the United States and elsewhere.[82] Consider as well that the United States has relationships with internet and telecommunications companies that facilitate surveillance. Since, at the present time, much of the world's internet traffic is routed through the United States, that virtual power is unprecedented. Moreover, the United States has the capacity to directly access undersea cables and other carriers of internet and telephonic communications.[83] The extended duration and seamlessness of U.S. control

---

prudential factor that limits their use. *See* David E. Sanger, *Syria War Stirs New U.S. Debate on Cyberattacks*, N.Y. TIMES, Feb. 25, 2014, at A1.

78. Margulies, *supra* note 74; Ashley Deeks, *Extraterritorial Right to Privacy: A Response by Luca Urech*, LAWFARE (Nov. 15, 2013, 6:54 PM), http://www.lawfareblog.com/2013/11/extraterritorial-right-to-privacy-a-response-by-luca-urech/#.Ut24nKMo6po.

79. *Cf.* David D. Clark & Susan Landau, *Untangling Attribution*, HARV. NAT'L SECURITY J. (2011), http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf (discussing aspects of cyber intrusions).

80. *See* Shane McGee, Randy V. Sabett & Anand Shah, *Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*, 8 J. BUS. & TECH. L. 1, 13 & nn.87–89 (2013) (noting that the Stuxnet virus implanted in Iranian centrifuges' systems for supervisory control and data acquisition altered the systems' reporting of the centrifuges' rate of revolution and temperature level, deceiving Iranian operators into running machines at high levels that resulted in their destruction); Jeremy Rabkin & Ariel Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea*, 14 CHI. J. INT'L L. 197, 209–10 (2013) (noting that the Stuxnet intrusion "disable[d] Iranian centrifuges while concealing its operation from Iranian technicians, by sending false signals to monitoring equipment").

81. *See* Scott Shane, *No Morsel Too Miniscule for All-Consuming N.S.A.*, N.Y. TIMES, Nov. 3, 2013, at A1. The revelations regarding the NSA's reach have sparked debate about the future of Internet governance, with some states calling for greater state control and state capacity for storage that would limit the influence of the United States, whose companies and facilities currently handle a huge portion of global internet traffic. *See generally* Melissa E. Hathaway & John E. Savage, *Stewardship of Cyberspace: Duties for Internet Service Providers*, CYBER DIALOGUE (2012), http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_hathaway-savage.pdf (discussing models of internet governance); *see also* Vincent J. Vitkowsky, *Snowden Affair and Control of the Internet*, ADVISEN (2013), https://www.advisen.com/HTTPBroker?action=jsp_request&id=articleDetailsNotLogged&resource_id=208291146.

82. *See* David E. Sanger & Thom Shanker, *N.S.A. Devises Radio Pathway into Computers*, N.Y. TIMES, Jan. 15, 2014, at A1.

83. *See In re* Gov't's Ex Parte Submission of Reauthorization Certification for 702 Program, slip op. at 5 (FISA Ct. Oct. 3, 2011) (Bates, J.), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-

in the virtual sphere constitutes an ongoing state presence that is in some ways more pervasive than states' dominance within their physical territory. A narrow standard requiring physical control does not do justice to the challenge of rapidly evolving technology in a changing world.[84] The virtual control test supplies a broader standard that meets this challenge.

Having made this argument, a caveat is in order. While the extent of U.S. surveillance capability should affect the threshold coverage of the ICCPR, it does *not* provide an answer on the ultimate legal merits of U.S. policies. The merits of NSA surveillance abroad hinge not on the capabilities of the United States but on how the substantial restraints that the United States imposes on those capabilities square with the ICCPR's arbitrariness standard for intrusions on privacy. I turn to these questions in the next section of the Article.

III. THE LEGAL MERITS OF NSA SURVEILLANCE ABROAD UNDER THE ICCPR

Having determined that the ICCPR applies as a threshold matter, we next ask whether NSA surveillance abroad is "arbitrary" or "unlawful" under Article 17. I assume in what follows that most surveillance conducted on non-U.S. persons outside the United States is lawful under the Fourth Amendment of the U.S. Constitution and U.S. statutes. Therefore, this section focuses on whether NSA surveillance is "arbitrary." I conclude that NSA surveillance is not arbitrary under Article 17, because it targets terrorists, national security threats, and espionage in a tailored fashion.

In reaching this conclusion, I rely on the principle of complementarity, which seeks to harmonize a body of international law with other international law doctrine and with the prerogatives of states. To integrate

---

with-exemptions.pdf (discussing "upstream" collection of contents of communications for which at least one party is located overseas).

84. On a superficial level, the virtual control that the United States can exercise abroad may appear less significant than the power to use deadly force on foreign territory. Arguably, the United States has a greater impact when it uses a drone to kill an agent of al Qaeda in Pakistan than when it eavesdrops on an al Qaeda agent in Germany. *Cf.* Jennifer C. Daskal, *The Geography of the Battlefield: A Framework for Detention and Targeting Outside the "Hot" Conflict Zone*, 161 U. PA. L. REV. 1165, 1191 (2013) (noting uncertainty regarding application of human rights law to extraterritorial targeted killings); Michael W. Lewis & Emily Crawford, *Drones and Distinction: How IHL Encouraged the Rise of Drones*, 44 GEO. J. INT'L L. 1127, 1142–49 (2013) (discussing the use of drones under international humanitarian law). At first blush, this argument seems to blunt the case for a virtual control standard, since *Bankovic* and the other ECHR cases cited above would not classify a country conducting a drone strike overseas as possessing sufficient "public powers" over persons or territory to justify a finding of jurisdiction. Indeed, the "public power" test seems to exclude surveillance of electronic communications by a foreign state, since such surveillance is often engaged in covertly, not publicly.

While these doubts are formidable, they should not carry the day. The effective jurisdiction test applicable to a state's physical footprint overseas was not designed to cover virtual or electronic surveillance. As suggested above, the pervasiveness of the communications capability of the United States, as well as the secrecy attending use of that power (at least prior to Edward Snowden's disclosures), argues for a broader test of jurisdiction.

all of the relevant international law doctrines, I read Article 17 in tandem with the law of armed conflict and U.N. Security Council resolutions on counterterrorism. To reconcile Article 17 with these norms and with sovereign prerogatives, I advance a model of procedural pluralism that gives states flexibility in creating protections if they honor core principles such as notice, oversight, and minimization but does not mandate the same itemized menu of safeguards required in European Union (ECHR) jurisprudence. In fact, as I note, ECHR jurisprudence permits exceptions to procedural safeguards, including exceptions designed to preserve the effectiveness of national security surveillance, that are not radically different from U.S. practice. I note, however, that certain reforms of NSA surveillance, such as a public advocate, would further strengthen compliance, affirming that NSA programs are consistent with the ICCPR. President Obama's initiatives, including a clearer articulation of the bases for U.S. surveillance abroad, buttress this case.

A. The Primacy of Complementarity

The concept of complementarity is a valuable lens for examining the lawfulness of states' conduct under the ICCPR. The principle of complementarity holds that international law norms are implemented in a complex landscape that requires actions by states and reconciliation with other rules of international law. Complementarity has two facets relevant to this piece: (1) complementarity accords a measure of deference to states in their good faith interpretation of their international obligations; and (2) complementarity also endeavors to harmonize disparate international rules and norms. A proper vision of complementarity eschews an all-or-nothing approach, in which international law trumps state policy or vice versa, and instead tailors each body of law to the needs of the other whenever possible. The same tailoring approach is appropriate for harmonizing disparate international rules. Each facet of complementarity demonstrates U.S. compliance with the ICCPR in its surveillance abroad.

1. Complementarity and State Law

Tribunals in Europe and elsewhere acknowledge the importance of complementarity between state and international law.[85] Complementarity requires engagement between international tribunals and sovereign states.[86] A measure of deference for state determinations reinforces collaboration

85. Rome Statute of the International Criminal Court pmbl. para. 10, art. 1, July 17, 1998, 2187 U.N.T.S. 90 (noting that the ICC was established as "complementary to national criminal jurisdictions").

86. *See* Jennifer Trahan, *Is Complementarity the Right Approach for the International Criminal Court's Crime of Aggression? Considering the Problem of "Overzealous" National Court Prosecutions*, 45 CORNELL INT'L L.J. 569, 578 (2012) ("[C]omplementarity 'forces the [International Criminal Court] and national legal systems to engage with one another.'" (citing Pål Wrange, *The Crime of Aggression and Complementarity*, *in* INTERNATIONAL CRIMINAL JUSTICE: LAW AND PRACTICE FROM THE ROME STATUTE TO ITS REVIEW 591, 592 (R. Bellelli ed., 2010))).

with international institutions. Jettisoning complementarity would jeopardize that link. Indeed, states joined the International Criminal Court (ICC) in reliance on that tribunal's recognition of the complementarity principle.[87] Observance of the complementarity principle mitigated the risk to sovereignty that the ICC posed. Construing the margin of appreciation, complementarity requires tribunals to accord some deference to a state's decisions about war crimes prosecution of that state's own officials.[88] Similarly, the ECHR has granted a measure of deference, which it describes as a "margin of appreciation," to a state's interpretation of its duties under the European Convention.[89] For example, the ECHR has deferred to a state's need to curb free expression to promote child safety[90] and curb extremist violence.[91] Analysis of U.S. overseas surveillance programs should trigger a similar quantum of deference.

2. Complementarity and International Norms

Complementarity is also a core principle in reconciling conflicts among different international law norms. International law is a vast canvas whose strands sometimes pull in different directions. Interpreting a particular provision should entail the least disruption with the entire enterprise. Moreover, certain provisions, principles, or entire bodies of law within the whole may be more recent or more specifically tailored to particular situations.[92] More specific provisions should inform the interpretation of other international norms.

Such provisions include U.N. Security Council resolutions enacted after September 11 to address the threat of terrorism. For example, Resolution 1373[93] requires that states "[t]ake the necessary steps to prevent the commission of terrorist acts, including [the] provision of early warning to other States by exchange of information."[94] The United States and other

87. *See id.* at 578–79.

88. *See id.* at 579–80.

89. Handyside v. United Kingdom, 24 Eur. Ct. H.R. (ser. A) at 16, 17 (1976); *see also* Robert D. Sloane, *Human Rights for Hedgehogs?: Global Value Pluralism, International Law, and Some Reservations of the Fox*, 90 B.U. L. REV. 975, 983 (2010) (explaining that the margin of appreciation provides flexibility for sovereign states to "implement or interpret human rights in ways that may be sensitive or responsive to prevailing social, cultural, and other norms within their polities"); *cf.* Robert M. Chesney, *Disaggregating Deference: The Judicial Power and Executive Treaty Interpretations*, 92 IOWA L. REV. 1723, 1766–70 (2007) (discussing U.S. domestic law approaches to deference).

90. *See generally Handyside*, 24 Eur. Ct. H.R. (ser. A).

91. Zana v. Turkey, 1997-VII Eur. Ct. H.R. 2533 (upholding the conviction of an official who, after attacks on civilians by a terrorist group, described the group as a "national liberation movement"). I cite these free expression cases not to recommend changes in the U.S. Constitution's First Amendment, which grants speech greater protection, but solely to illustrate how complementarity works in European tribunals.

92. *See* CCPR General Comment No. 31, *supra* note 34, ¶ 11 (stating, in discussing the role of the law of armed conflict in interpreting the ICCPR, that "more specific rules of international humanitarian law may be specially relevant for the . . . interpretation of Covenant rights [and] both spheres of law are complementary, not mutually exclusive").

93. *See* S.C. Res. 1373, ¶ 2(b), U.N. Doc. S/RES/1373 (Sept. 28, 2001).

94. *Id.*

states that engage in counterterrorist measures can enhance their ability to fulfill this obligation by conducting surveillance on suspected terrorists and sharing the information thereby acquired. Similarly, subsection 2(d) of the resolution mandates that states "[p]revent those who finance, plan, facilitate or commit terrorist acts from using [states'] territories for those purposes against other States or their citizens."[95] While this duty applies most clearly to a state conducting surveillance on persons within its borders, in today's mobile and interconnected world, such persons may have regular contacts with persons abroad. In addition, subsection 3(a) urges states to share "operational information . . . regarding actions or movements of terrorist persons or networks" and, inter alia, "use of communications technologies by terrorist groups."[96] A reading of the ICCPR that inhibits achievement of these goals by imposing burdensome limits on surveillance would not effectively harmonize the ICCPR with the international post-9/11 counterterrorism framework imposed by the U.N. Security Council.

The law of armed conflict[97] also requires a more flexible interpretation of the ICCPR in the surveillance arena. The International Court of Justice has held that the law of armed conflict constitutes *lex specialis* that, by virtue of its more specific provisions, should inform human rights law in armed conflicts.[98] Reconnaissance and surveillance of another party to an armed conflict is an accepted incident of war.[99] The law of armed conflict does not preclude espionage, and permits a wide range of observation of enemy forces.[100] This observation can be clandestine or open. A noninternational armed conflict, like the conflict between the United States and al Qaeda and associated forces, does not diminish a state's prerogative to engage in such observation of its adversaries.[101] A rigid application of the ICCPR that

95. *Id.* ¶ 2(d).

96. *Id.* ¶ 3(a).

97. *See generally* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT (2d ed. 2010); MICHAEL N. SCHMITT ET AL., INT'L INST. OF HUMANITARIAN LAW, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT (2006), *available at* http://www.iihl.org/iihl/Documents/The%20Manual%20on%20the%20Law%20of%20NIAC.pdf.

98. *See* Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 262 (July 8); Neuman, *supra* note 72, at 387 (defending "modifying the content of . . . treaty norms . . . by importing relevant rules (if any exist) from the law of armed conflict, by means of *lex specialis* or similar arguments").

99. Michael N. Schmitt, *Unmanned Combat Aircraft Systems and International Humanitarian Law: Simplifying the Oft Benighted Debate*, 30 B.U. INT'L L.J. 595, 597–601 (2012) (discussing surveillance and reconnaissance in the context of the use of drones).

100. *See* Richard R. Baxter, *So-Called 'Unprivileged Belligerency': Spies, Guerillas, and Saboteurs*, 28 BRIT. Y.B. INT'L L. 323, 328–33 (1951) (questioning whether espionage is a violation of the law of nations); *cf.* John C. Dehn, *The* Hamdan *Case and the Application of a Municipal Offence: The Common Law Origins of 'Murder in Violation of the Law of War,'* 7 J. INT'L CRIM. JUST. 63, 68 n.26, 73–79 (2009) (noting and elaborating upon Baxter's view).

101. *See* Hamdan v. Rumsfeld, 548 U.S. 557, 562 (2006) (holding that the conflict with al Qaeda is "not of an international character" for purposes of the Geneva Conventions' Common Article 3); *cf.* Geoffrey Corn & Eric Talbot Jensen, *Transnational Armed Conflict: A "Principled" Approach to the Regulation of Counter-Terror Combat Operations*, 42 ISR. L. REV. 46, 53, 68–69 (2009) (arguing that the noninternational armed conflict model was

precludes such observation would fundamentally reshape the law of armed conflict. That disregard for another corpus of international law would not do justice to the principle of complementarity.

While, as we shall see, the ECHR jurisprudence on surveillance is not wholly inconsistent with complementarity, especially as regards state law, other European tribunal decisions on counterterrorism are less promising on harmonizing international norms. In *Al-Jedda v. United Kingdom*,[102] *Kadi v. European Court of Justice*,[103] and *A. and Others v. United Kingdom*,[104] European courts failed to adequately harmonize individual rights guarantees with global counterterrorism measures. In *Al-Jedda*, the ECHR rigidly defined detention authority in an armed conflict, limiting it to peacetime modes such as quarantine or detention prior to a criminal trial.[105] The ECHR declined to read in to the European Convention an acknowledgment that the law of armed conflict requires broader detention authority.[106] In failing to give Britain detention authority required to effectuate a U.N. Security Council resolution authorizing occupation in post–Saddam Hussein Iraq, the ECHR also failed to show appropriate respect for the role of the Security Council in ensuring world order. In *A. and Others*, the ECHR was unduly rigid in applying a proportionality analysis to Britain's derogation from the European Convention's detention rules, where Britain sought to detain a foreign national whom it suspected of terrorism but could not deport because of concerns that the detainee would be subject to mistreatment if returned to his country of origin.[107] In *Kadi v. European Court of Justice*, the European Court of Justice applied procedural safeguards rigidly. The court thus failed to respect Security Council resolutions that curbed financial assistance to terrorist groups[108] and the U.N. ombudsperson regime that had provided relief to those wrongly targeted by counterterrorism sanctions.[109]

originally designed to cover internal rebellions or civil wars, and that conflict with a transnational terrorist organization like al Qaeda requires a different paradigm); Michael W. Lewis, *Drones and the Boundaries of the Battlefield*, 47 TEX. INT'L L.J. 293, 306–08 (2012) (cautioning against conflation of civil wars and conflicts with transnational armed groups).

102. App. No. 27021/08, 53 Eur. H.R. Rep. 23 (2011).

103. Joined Cases C-584/10 P, C-593/10 P & C-595/10 P, INFOCURIA—CASE-LAW CT. JUST. (July 18, 2013), http://curia.europa.eu/juris/document/document.jsf?text=&docid=139745&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=1914364.

104. 2009-II Eur. Ct. H.R. 137.

105. *Al-Jedda*, 53 Eur. H.R. Rep. at 843–48.

106. *Id.*; *cf.* James Farrant, *Is the Extra-Territorial Application of the Human Rights Act Legally Justified?*, 9 INT'L CRIM. L. REV. 833, 833–54 (2009) (critiquing an earlier opinion in the case).

107. *A. & Others*, 2009-II Eur. Ct. H.R. at 222–24.

108. *See, e.g.*, S.C. Res. 1989, U.N. Doc. S/RES/1989 (July 1, 2011).

109. For discussion of the ombudsperson system, see SUE E. ECKERT & THOMAS J. BIERSTEKER, WATSON INST. FOR INT'L STUDIES, BROWN UNIV., DUE PROCESS AND TARGETED SANCTIONS: AN UPDATE OF THE "WATSON REPORT" 6 (2012), *available at* http://www.watsoninstitute.org/pub/Watson%20Report%20Update%2012_12.pdf.

3. Complementarity and Procedural Plurality

To honor complementarity, we should embrace a pluralist account[110] of appropriate procedural safeguards. Pluralism has gone hand in hand with complementarity in the work of a significant number of tribunals and scholars. Often pluralism comes into play when assessing the appropriateness of different state remedial frameworks in the wake of persecution and atrocities. We can apply a similar perspective to the procedural safeguards that should accompany surveillance.

An important strand in law and commentary on remedial frameworks holds that no one model fits all situations in coping with the aftermath of mass human rights violations, such as South Africa's apartheid. South Africa famously endorsed a truth and reconciliation model that stressed dialogue and transparency regarding past wrongs over formal legal accountability.[111] In many settings in the developing world, formal legal accountability came to be seen as a model too rigid to foster transitions from oppression. The plurality of the formal and informal models that were used suggests that, beyond baseline requirements, states should have choices in the frameworks they adopt. An absolute amnesty for wrongdoers was out of bounds.[112] However, once states rejected this course of action, a range of frameworks were acceptable, including truth and reconciliation and exemplary punishment of leaders in abuses, together with de facto amnesty for many followers in the interest of forging political peace.

We can apply this model to procedural safeguards accompanying certain intrusive governmental action, including surveillance. On this view, one would ask if a given framework provided a sound foundation: notice about grounds for surveillance, oversight of surveillance programs, and deterrence of arbitrary official conduct, including targeting of political opponents or disfavored ethnic, racial, or religious groups. A state could choose from a number of procedural options that would accomplish these goals, without being locked into specific measures that might not fit with that state's history or traditions. Procedural pluralism would also minimize conflicts with other international rules, such as the law of armed conflict and Security Council resolutions mandating counterterrorism efforts. With procedural pluralism as a backdrop, we can turn to European precedents on surveillance policy.

---

110. *See* PAUL SCHIFF BERMAN, GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS (2012); Paul Schiff Berman, *Global Legal Pluralism*, 80 S. CAL. L. REV. 1155 (2007).

111. *Azanian People's Org. v. President of the Republic of S. Afr*. 1996 (4) SA 671 (CC) (S. Afr.); *cf.* MARK A. DRUMBL, ATROCITY, PUNISHMENT, AND INTERNATIONAL LAW 148 (2007) (praising restorative-justice mechanisms that promote a "'forgiveness process characterized by truth telling, redefinition of the identity of the former belligerents, partial justice, and a call for a new relationship'" (quoting WILLIAM J. LONG & PETER BRECKE, WAR AND RECONCILIATION: REASON AND EMOTION IN CONFLICT RESOLUTION 3 (2003))); Newton, *supra* note 12, at 13 ("'[J]ustice' is most legitimate and . . . effective when it is most responsive to the demands of the local population.").

112. *See* Diane F. Orentlicher, *Settling Accounts: The Duty To Prosecute Human Rights Violations of a Prior Regime*, 100 YALE L.J. 2537, 2604–06 (1991).

B. European Case Law on Security Surveillance

While European surveillance law may appear, on first encounter, to require more privacy protections than U.S. law,[113] several caveats are in order. First, as we shall see, European courts do not require judicial authorization of surveillance,[114] which in some form is central to most U.S. surveillance programs, including those concerning the content of overseas communications. Second, the ECHR has not indicated hostility to bulk collection of internet or telecommunications data; indeed, some years ago it approved a German program that queried a massive database of communications content.[115] Third, the ECHR, recognizing that national security threats may be "difficult to define in advance,"[116] has not required that a statute specify detailed criteria justifying surveillance. Fourth, the ECHR has recognized that a state can assemble a database including communications by foreign nationals located outside of that state.[117] Fifth, even when the ECHR has imposed procedural requirements that exceed those that U.S. courts have imposed, those safeguards stem in large part from interpretation not of the ICCPR, but of the European Convention on Human Rights,[118] which does not bind the United States. Sixth, the United States and Europe both follow minimization requirements for foreign communications, although those requirements are not spelled out as clearly in U.S. law.

While there are differences between European and U.S. law, these differences often concern tone and emphasis, not substance. The ECHR has subjected European states to requirements, such as notification of the targets of surveillance and recourse for those wrongly targeted, that are usually not available in the United States for national security surveillance. Even in Europe, however, courts have permitted exceptions that substantially ease compliance for governments engaged in surveillance.

---

113. *See* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 633–34 (2007). This article predated the Snowden revelations and was based on earlier reports of U.S. surveillance.

114. *See* Kennedy v. United Kingdom, App. No. 26839/05, 52 Eur. H.R. Rep. 207 (2010); *cf.* Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶ 54, Human Rights Council, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) (by Frank La Rue) (noting that, in Britain, the Secretary of State authorizes surveillance).

115. *See* Weber v. Germany, 2006-XI Eur. Ct. H.R. 309.

116. *See Kennedy*, 52 Eur. H.R. Rep. at 256.

117. *See Weber*, 2006-XI Eur. Ct. H.R. at 332–34.

118. *See* Convention for the Protection of Human Rights and Fundamental Freedoms art. 8(1), Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter Convention for the Protection of Human Rights] ("Everyone has the right to respect for his private and family life, his home and his correspondence."); *id.* art. 8(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 well-being 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.").

1. Overlap Between the U.S. and European Models

The caveats above push back against the conventional narrative that Europe provides greater privacy protections.[119] Consider the judicial role in surveillance. In the United States, the Fourth Amendment or federal legislation requires some judicial role in the authorization of the acquisition of the content of communications, or even in the ongoing collection of phone records. In contrast, although European courts stress the need for some independent review of surveillance requests, courts need not be the agency performing this role. In *Weber v. Germany*,[120] for example, the ECHR approved a framework that entrusted review to a body called the G 10 Commission.[121] While the G 10 Commission must by law include a senior judicial official, it is not a court.[122] Federal courts have a wide range of remedies at their disposal in the United States, and federal judges enjoy the protection of lifetime tenure.[123] The German G 10 Commission may not have similarly effective tools and lacks the same protections.[124]

In *Weber*, the ECHR also approved a surveillance program that gathered the contents of communications by foreign nationals abroad. The ECHR referred to Germany's program as "strategic monitoring."[125] German officials assembled this vast database without any "particularized suspicion of wrongdoing."[126] They then used search terms to query the data.[127] The U.S. section 702 program uses methods that are substantially similar to the German approach.[128]

Crucially, the ECHR has recognized that detailed statutory criteria governing surveillance would be counterproductive. While noting the importance of "forseeability" among the public that surveillance is possible and the perils of "unfettered" discretion,[129] the ECHR has held that

119. For the classic treatment of such comparisons, see James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004) (arguing that the United States values privacy as a means for securing liberty, while Europeans value dignity, defined as not subjecting individuals to unwanted public gaze). *But see* Bignami, *supra* note 113 (arguing that the European approach also protects liberty).

120. 2006-XI Eur. Ct. H.R. 309.

121. *Id.* at 318, 319, 327.

122. *Id.* at 320.

123. U.S. CONST. art. III, § 1.

124. Judges on the German Federal Constitutional Court serve twelve-year terms. *See* Susanne Baer, *The Difference a Justice May Make: Remarks at the Symposium for Justice Ruth Bader Ginsburg*, 25 COLUM. J. GENDER & L. 92, 93 (2013).

125. *Weber*, 2006-XI Eur. Ct. H.R. at 315.

126. *See* Bignami, *supra* note 113, at 640; Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 751, 778–82 (2003).

127. *Weber*, 2006-XI Eur. Ct. H.R. at 316 (explaining that the German government would monitor telecommunications "with the aid of catchwords which remained secret").

128. *See In re* Gov't's Ex Parte Submission of Reauthorization Certification for 702 Program, slip op. at 15–16, 22–23 (FISA Ct. Oct. 3, 2011) (Bates, J.), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf; *see also supra* notes 23–25 and accompanying text.

129. Kennedy v. United Kingdom, App. No. 26839/05, 52 Eur. H.R. Rep. 207, 253–54 (2010).

surveillance based on "national security" concerns is appropriate.[130] Ruling that the term, "national security," is not unduly vague, the ECHR found that the term has been "frequently employed in both national and international legislation," and that protecting national security is "one of the legitimate aims" of the underlying statute.[131] More detailed criteria, the court cautioned, would lead to national security threats "adapt[ing their] conduct" to stay just outside the statute's reach.[132] Pursuant to the directive issued simultaneously with President Obama's January 2014 speech, the NSA must also limit itself in exactly the same way that European courts require, focusing on national security and crime.[133] U.S. policy squarely precludes surveillance abroad for other purposes, such as suppressing speech critical of the United States, discriminating against racial, religious, or ethnic groups, or gaining a competitive advantage for U.S. companies.[134]

The ECHR has also recognized that states need greater leeway in surveillance of foreign nationals located abroad. The ECHR has held that surveillance by one state generally does not impinge on the sovereignty of another state in which the target of the surveillance is located.[135] No interference with sovereignty occurs, the ECHR has asserted, as long as the state conducting surveillance does not gain access to "fixed telephone lines" or other physical communications instrumentalities without the territorial state's consent.[136] Moreover, greater flexibility in conducting surveillance on foreign nationals abroad makes policy sense given the transnational nature of the terrorist threat and the difficulty of coordinating with other states in addressing that threat. States are at risk for terrorist attacks that are planned elsewhere. However, a state that is a likely target may not learn about that preparation in a timely manner, if it must rely solely on the cooperation of the state in which the planners are currently located.[137] Surveillance across borders that is appropriately tailored to national security threats helps connect the dots.

Moreover, ECHR opinions interpret the privacy protections in Article 8 of the European Convention on Human Rights, which is not limited by its terms to barring the "arbitrary" intrusions prohibited by Article 17 of the

130. *Id.* at 255.
131. *Id.* at 256.
132. *Id.* at 253–54.
133. *See* PPD-28, *supra* note 5, at 3–4.
134. *See id.*; *cf.* United States v. Duggan, 743 F.2d 59, 69–71 (2d Cir. 1984) (upholding surveillance under FISA of alleged agents of the Irish Republican Army, citing to the statutory term "foreign intelligence information" as including information about "terrorism," "national security," and "the conduct of the foreign affairs of the United States," and stating that such terms were not impermissibly vague). Section 702 does not authorize surveillance based on such grounds, and no reports tying the NSA to surveillance based on such grounds have surfaced, even after the worldwide scrutiny occasioned by Snowden's revelations.
135. Weber v. Germany, 2006-XI Eur. Ct. H.R. 309, 332–34.
136. *Id.*
137. *See* Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2726 (2010) (noting the need for "cooperative efforts" and "international cooperation" in counterterrorism); *cf.* Peter Margulies, *Advising Terrorism: Material Support, Safe Harbors, and Freedom of Speech*, 63 HASTINGS L.J. 455 (2012) (discussing information asymmetries that justify flexibility in counterterrorism capabilities).

ICCPR. True, European states that collaborate with the United States on surveillance still have to observe the provisions of the European Convention. The United States, however, is not directly bound by those provisions. Moreover, Article 8 of the European Convention contains broad exceptions for national security, law enforcement, and other governmental purposes.[138]

In addition, both the United States and Europe follow minimization requirements for handling personal data acquired through surveillance. In the United States, legislation requires minimization of data about U.S. persons,[139] while minimization of data regarding foreign nationals located abroad is largely the province of internal agency rules. In the United States, according to Robert Litt, the General Counsel of the Office of the Director of National Intelligence, conversations that are not relevant are "destroyed after a maximum of five years."[140] In Europe, legislation often expressly provides for minimization within a shorter period for data collected from persons located both within and outside a state's territory.[141] However, minimization requirements are substantial in both the United States and Europe.

2. Differences Between the United States and Europe in the Privacy Space

European courts have imposed two requirements, notification and recourse, that U.S. law construes more narrowly in the national security arena. Even here, however, European courts have acknowledged exceptions to the requirements that bring the European model and the American one much closer together. Consider notification first. A central principle of privacy law in both the United States and Europe is notification to individuals whose "personally identifiable information" (PII) has been obtained by another individual or entity or has been disclosed without the individual's authorization. This principle is a component of the U.S. Privacy Act,[142] which has for decades served as a model for global privacy efforts. Notification serves a number of purposes. For example, it allows the individual to take appropriate remedial measures and helps deter unauthorized disclosures. No entity, such as a healthcare provider, entrusted with an individual's PII, wants to admit that it has not taken good care of this vital information.

---

138. *See* Convention for the Protection of Human Rights, *supra* note 118, art. 8(2).

139. 50 U.S.C. § 1881a (Supp. V 2011).

140. *See In re* Gov't's Ex Parte Submission of Reauthorization Certification for 702 Program, slip op. at 24 (FISA Ct. Oct. 3, 2011) (Bates, J.), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf; Robert S. Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence, Privacy, Technology & National Security: An Overview of Intelligence Collection (July 18, 2013), *available at* http://icontherecord.tumblr.com/post/57724442606/privacy-technology-national-security-an.

141. *Weber*, 2006-XI Eur. Ct. H.R. at 337.

142. *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a note (2012)).

In the law enforcement and national security contexts, however, both Europe and the United States recognize that notification can be problematic. Imagine federal law enforcement officials in the United States obtaining a warrant to tap the phone of the fictional mobster Tony Soprano (or an actual organized crime figure) and then dutifully informing Tony that he is the subject of surveillance. Any subject of surveillance so notified would become far more guarded in his communications, thus undermining the purpose of the surveillance. The United States has responded to this concern with categorical exemptions from the Privacy Act for national security and much law enforcement activity.[143]

Europe also has exceptions to the notification requirement in national security cases. These exceptions operate in a case-by-case fashion, but in practice are quite broad. The ECHR has recognized that "notification might reveal the working methods and fields of operation of the Intelligence Service," and that "the very absence of knowledge of surveillance . . . ensures the efficacy" of the surveillance operation.[144] Accordingly, an agency conducting surveillance for national security need not notify individuals if it believes that notification will compromise the underlying goals of the investigation.[145] Moreover, in Germany, officials can cite national security as an exemption to the otherwise central imperative to give individuals access to personal information accumulated about them by the government.[146]

One feature of European jurisprudence is a requirement that an individual who has been notified or has otherwise come to suspect that he is the subject of surveillance must have recourse to an independent agency to investigate. In *Kennedy v. United Kingdom*,[147] the petitioner had been convicted of manslaughter in a controversial case featuring some missing and contradictory police evidence. He had subsequently become active in an organization that questioned police practices, and he alleged that the government was intercepting his phone calls.[148] Pursuant to statute, the petitioner filed complaints with the Investigatory Powers Tribunal (IPT), which was empowered under British law to investigate such complaints.[149]

143. *Id.* § 552a(j).

144. *Weber*, 2006-XI Eur. Ct. H.R. at 345; *cf.* Schwartz, *supra* note 126, at 776 (observing that, under European law, secrecy is appropriate if "interests of the State justified secrecy").

145. *Weber*, 2006-XI Eur. Ct. H.R. at 345. *But see* Rapporteur, *Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs*, 7, 11, European Parliament Comm. on Civil Liberties, Justice & Home Affairs, 2013/2188(INI) (Jan. 8, 2014) (by Claude Moraes), *available at* http://www.statewatch.org/news/2014/jan/ep-draft-nsa-surveillance-report.pdf (acknowledging analogous exceptions before President Obama's speech in January 2014, but arguing that NSA surveillance was not "necessary and proportionate" to those exceptions, and could be "used for reasons other than national security and the . . . fight against terrorism, for example economic and industrial espionage or profiling on political grounds").

146. *Weber*, 2006-XI Eur. Ct. H.R. at 345.

147. Kennedy v. United Kingdom, App. No. 26839/05, 52 Eur. Ct. H.R. 207 (2010).

148. *See id.* at 215.

149. *See id.* at 215–16.

The IPT can investigate claims of wrongful surveillance and award relief, including vacating warrants and ordering the destruction of illegally obtained records.[150] When the IPT finds that a complaint is not meritorious, it merely informs the complainant that "no determination has been made in his favour."[151] Courts have upheld the statutory language requiring such Delphic replies, aware of the potential for individuals to game the system if a response provides more information about surveillance practices. In France, recourse is more indirect, with a watchdog agency making inquiries about individual cases.[152]

The United States currently lacks an independent agency that provides such recourse. Instead, the United States has privacy officials who are integrated into virtually every executive department, including the Department of Homeland Security.[153] The United States also has a Privacy and Civil Liberties Oversight Board, although that body has no power to order relief.[154] President Obama's announcement in January 2014 of the creation of new White House and State Department positions dealing with privacy will enhance this voice. However, the lack of a dedicated independent agency may impede the recourse that European law requires. While individuals in the United States can contact privacy officials in various government agencies and may have standing to challenge surveillance in federal courts, each of these avenues is limited.[155]

3. Procedural Pluralism and Comparative Surveillance

Despite these differences between the United States and Europe, procedural pluralism makes a compelling argument for U.S. compliance with the ICCPR. The United States, particularly after President Obama's speech and directive, provides notice of the grounds for surveillance comparable to Europe. It provides oversight through courts, unlike most of

150. *Id.* at 232.

151. *Id.*

152. *See* Bignami, *supra* note 113, at 657–58.

153. *See* 6 U.S.C. § 142 (2012) (establishing a privacy officer for the Department of Homeland Security).

154. *See* Jay Stanley, *What Powers Does the Civil Liberties Oversight Board Have?*, ACLU (Nov. 4, 2013), https://www.aclu.org/blog/national-security-technology-and-liberty/what-powers-does-civil-liberties-oversight-board-have.

155. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147–50, 1155 (2013) (holding that the plaintiffs, who could not conclusively demonstrate that they had been subject to surveillance, lacked standing to challenge the constitutionality of the FISA Amendments Act); *cf.* ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 U.S. Dist. LEXIS 180863, at *22–30, 41 (S.D.N.Y. Dec. 27, 2013) (finding that in the wake of the Snowden disclosures, the plaintiffs could make a definitive showing that they had been subject to surveillance and thus had standing to challenge the surveillance program); *see also* Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 928 (D.C. Cir. 2003) (holding that the exception in the U.S. Freedom of Information Act (FOIA) allowed the government to refuse to disclose information about September 11 immigration detainees); Margaret B. Kwoka, *Deferring to Secrecy*, 54 B.C. L. REV. 185, 218–19 (2013) (viewing the D.C. Circuit's decision in *Ctr. for Nat'l Sec. Studies* as an expansion of government secrecy); David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005) (critiquing the D.C. Circuit's rationale for the *Ctr. for Nat'l Sec. Studies* decision).

Europe. Moreover, the president's directive narrows officials' discretion, precluding surveillance conducted to suppress speech, target minorities, or favor private business. Because the United States meets these criteria, it should have leeway to tailor safeguards without buying into other items, such as notification and recourse, that are less familiar in the context of U.S. security surveillance and subject to broad exceptions under European law. While, as I suggest later in this section, further reforms might reinforce the case, the argument from procedural pluralism is already quite solid.

C. Foreign Surveillance and Free Expression

The NSA programs also do not violate the ICCPR Article 19 prohibition on inhibiting free expression. Those protections, like the safeguards in the European Convention, are already substantially less robust than the free speech protections in the U.S. Constitution. The ICCPR's protections are qualified, allowing restrictions on the content of speech when such restrictions are necessary for national security.[156] In *Weber*, the ECHR ruled that the broad German content-collection program did not infringe free expression, because its purpose and implementation demonstrated that it was not "aimed at monitoring journalists," although the court did not rule out the possibility of incidental effects in this area.[157] U.S. surveillance abroad that is carefully tailored to national security goals should not run afoul of the ICCPR's protections. President Obama's January 2014 criteria meet these specifications.

Under the ICCPR, U.S. officials could determine that certain speech, such as speech that calls for violence against the United States or its allies, should trigger surveillance of the speaker's communications. Speech of this sort could signal the speaker's intent to actively participate in plots to engage in actual violence. While surveillance based on the speaker's stated views, without further evidence of participation in violence, might well be problematic under the U.S. Constitution, it would not violate the ICCPR.[158] One suggestion for reform of NSA surveillance offered by the President's Review Group urged the government not to target non-U.S. persons abroad "solely" because of speech or religion.[159] However, the ICCPR would not bar such surveillance, assuming that the relevant speech urged violence.[160]

---

156. *See* ICCPR, *supra* note 2, art. 19(3)(b) (providing for an exception to free expression where necessary for the "protection of national security or of public order . . . or of public health or morals"); Zana v. Turkey, 1997-VII Eur. Ct. H.R. 2533 (interpreting a similar provision in the European Convention to permit a state to bar speech praising a terrorist group). *But see* Molly Land, *Toward an International Law of the Internet*, 54 HARV. INT'L L.J. 393 (2013) (arguing that Article 19 provides robust protection of free expression by both government and private actors).

157. Weber v. Germany, 2006-XI Eur. Ct. H.R. 307, 349.

158. *See Zana*, 1997-VII Eur. Ct. H.R. 2533.

159. *See* PRESIDENT'S REVIEW GRP., *supra* note 1, at 151 (Recommendation 13).

160. The President's Review Group appears to acknowledge this in reserving for the United States the ability to conduct surveillance on any subject abroad who "poses a threat to US national security." *Id.* at 157 n.153.

Moreover, the First Amendment would not bar U.S. surveillance based on extreme political views conducted on a non-U.S. person located abroad. My point here is not to second guess the robust protections provided by the First Amendment to persons inside the United States. Rather, I aim only to clarify that the government is not and should not be constrained by either the First Amendment or the ICCPR in surveillance of non-U.S. persons abroad, as long as it does not aim to deter speech critical of U.S. policies.

D. Proposals for Further Reform

While I have concluded that U.S. surveillance policy does not violate the ICCPR, further reforms could highlight this point and silence persistent doubts here and abroad. These reforms could also remove any barriers to cooperation between the United States and foreign states, such as those in Europe, which are subject to the European Convention on Human Rights. This section identifies reforms that would add a public advocate to FISC proceedings, enhance FISC review of the criteria used for overseas surveillance, establish a U.S. privacy agency that would handle complaints from individuals here and overseas, and require greater minimization of non-U.S. person communications. These reforms would signal U.S. support of evolving global norms of digital privacy.

Although President Obama's speech in January 2014 proposed a panel of independent lawyers who could participate in important FISC cases,[161] further institutionalization of this role would be useful. A public advocate would scrutinize and, when necessary, challenge the NSA's targeting criteria on a regular basis.[162] Challenges would be brought in the FISC, after the NSA's implementation of criteria. The NSA would be able to adapt the criteria on an exigent basis, subject to ex post review by the FISC at the public advocate's behest. A public advocate and enhanced FISC review would serve three valuable functions: (1) ensure that the FISC received the best arguments on both sides; (2) serve as a valuable ex ante check on the government, encouraging the government to adopt those criteria that could withstand subsequent scrutiny; and (3) promote domestic and global confidence in the legitimacy of processes governing NSA surveillance.

A U.S. cabinet level privacy agency would also bolster the legitimacy of surveillance. The agency could provide more regular recourse to subjects of surveillance, as the ECHR requires. That change would ease the barriers to continued U.S.-Europe cooperation on counterterrorism. A national agency would also work hand in hand with privacy officers in executive departments. It would increase the leverage of those officials, who could advocate vigorously in internal debates, knowing that their views would also have a champion in a free-standing executive department independent

161. *See* Wittes, *supra* note 5.

162. For more detail on such proposals, see Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate,"* JUST SECURITY (Nov. 4, 2013, 1:34 PM), http://justsecurity.org/2013/11/04/fisa-special-advocate-constitution/.

of the national security bureaucracy. There are downsides to this proposal, of course. A new agency would add expense, and create some redundancy in government functions. Moreover, current models that provide recourse, such as the approach currently taken by the Department of Homeland Security,[163] have been criticized as unduly burdensome.[164] However, preserving cooperation with Europe and enhancing the overall legitimacy of U.S. surveillance provides a compelling justification.

Each of these instrumentalities—a public advocate at the FISC and a new privacy agency—could also work to strengthen minimization requirements for foreign communications. The NSA says that it disposes of all irrelevant communications within five years. There may be ways to shorten this time and require even more rigorous controls on sharing of information that lacks a clear link to terrorism or other foreign intelligence matters. More exacting minimization would also promote U.S.-European information sharing and enhance global legitimacy.

CONCLUSION

While critics of U.S. surveillance abroad denounce the United States for disregarding international law on privacy, that conclusion is far too facile. Unpacking the status of U.S. surveillance under international law requires a multistep analysis. This analysis asks first whether U.S. surveillance abroad is, as a threshold matter, covered by the ICCPR. It then asks whether U.S. surveillance violates the ICCPR's Article 17, which bars "arbitrary or unlawful interference" with privacy.[165] This Article concludes that the United States is subject as a threshold matter to the ICCPR. However, U.S. surveillance abroad complies with Article 17.

On the threshold question, this Article concludes that Article 2(1) of the ICCPR is best read disjunctively on a state's duty to "respect" treaty rights. The duty to respect ICCPR rights accrues both "within [U.S.] territory" *and* in any domain "subject to its jurisdiction."[166] The purpose of the provision and its drafting history, including key remarks by U.S. chief delegate Eleanor Roosevelt, demonstrate that the ICCPR applies to the armed forces of a state wherever those forces exercise effective control over areas or individuals. However, the duty to "ensure" that others respect ICCPR rights only accrues within a state's own territory.

The Article then suggests that the effective control test is too narrow to apply to the domain of electronic and digital communications. Because of the ease of exerting remote control over such communications, a virtual control standard is more appropriate and in keeping with Article 2(1). The

163. *See* Hugo Teufel III, *An Explanation of the DHS Privacy Policy Behind Review Group Recommendation # 14*, LAWFARE (Jan. 8, 2014, 11:47 AM), http://www.lawfareblog.com/2014/01/an-explanation-of-the-dhs-privacy-policy-behind-review-group-recommendation-14/#.UuCLPqMo6po.

164. *See* Michael Leiter, *Too Much and Too Little*, LAWFARE (Dec. 26, 2013, 10:39 AM), http://www.lawfareblog.com/2013/12/too-much-and-too-little/#.UuCOA6Mo6po.

165. ICCPR, *supra* note 2, art. 17.

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

extraordinary capabilities of the United States in this arena meet the virtual control standard because of U.S. intelligence agencies' ability to monitor, filter, and, in some cases, modify the content of communications received and sent by and about subjects abroad.

While the ICCPR applies to U.S. surveillance abroad as a threshold matter, U.S. surveillance is not "arbitrary" under Article 17 of the ICCPR. This argument incorporates procedural pluralism into the complementarity due both state law and other international norms. Under the procedural pluralism framework, U.S. officials can choose among a range of procedural safeguards as long as the United States provides public notice of the criteria for surveillance and independent oversight. European law is not inconsistent with this approach: the ECHR has approved European state surveillance even absent the judicial role typical of U.S. surveillance and does not require notifying targets of surveillance when notification would jeopardize an investigation. Moreover, the ECHR interprets the European Convention, which is not limited to the ICCPR's bar on arbitrary governmental action.

As President Obama's speech and policy directive of January 17, 2014, demonstrate, the United States observes both the public notice and oversight values. The U.S. focus on national security as a basis for surveillance abroad parallels the criteria used by European countries. Moreover, the United States has more judicial involvement than European states. President Obama's initiatives provide greater clarity about existing U.S. practice, and supplement that practice in a number of respects, including provision for a panel of independent advocates to provide input to the FISC in important cases.

This Article's argument is not a basis for U.S. complacency. The United States should continue to do more to reconcile security with evolving global privacy norms. In particular, U.S. officials should strongly consider more rigorous minimization requirements for the communications of foreign nationals outside U.S. territory. U.S. officials may also wish to create an independent privacy agency and an institutional role for a public advocate at the FISC. These changes are not required under the ICCPR, but they would signal U.S. willingness to shoulder the burden of global leadership in balancing security and privacy. Absent that U.S. effort, other states may exploit the resulting vacuum, spawning results that serve neither security nor privacy rights.