ARTICLE

An International Legal Framework for Surveillance

ASHLEY DEEKS*

Edward Snowden's leaks laid bare the scope and breadth of the electronic surveillance that the U.S. National Security Agency and its foreign counterparts conduct. Suddenly, foreign surveillance is understood as personal and pervasive, capturing the communications not only of foreign leaders but also of private citizens. Yet to the chagrin of many state leaders, academics, and foreign citizens, international law has had little to say about foreign surveillance. Until recently, no court, treaty body, or government had suggested that international law, including basic privacy protections in human rights treaties, applied to purely foreign intelligence collection. This is now changing: Several UN bodies, judicial tribunals, U.S. corporations, and individuals subject to foreign surveillance are pressuring states to bring that surveillance under tighter legal control.

This Article tackles three key, interrelated puzzles associated with this sudden transformation. First, it explores why international law has had so little to say about how, when, and where governments may spy on other states' nationals. Second, it draws on international relations theory to argue that the development of new international norms regarding surveillance is both likely and essential. Third, it identifies six process-driven norms that states can and should adopt to ensure meaningful privacy restrictions on international surveillance without unduly harming their legitimate national security interests. These norms, which include limits on the use of collected data, periodic reviews of surveillance authorizations, and active oversight by neutral bodies, will increase the transparency, accountability, and legitimacy of foreign surveillance.

This procedural approach challenges the limited emerging scholarship on surveillance, which urges states to apply existing — but vague and contested — substantive human rights norms to complicated, clandestine practices. In

* Associate Professor, University of Virginia School of Law. Thanks to Daniel Abebe, Kate Andrias, Harlan Cohen, Carrie Cordero, Jen Daskal, David Kaye, Leslie Kendrick, David Kris, Peter Margulies, David Martin, Tim Meyer, Marko Milanovic, Alexandra Perina, Alan Rozenshtein, Beth Van Schaack, Rich Schragger, John Setear, Paul Stephan, Matthew Waxman, and Ben Wittes for very helpful comments.

identifying and valuing new, objectively verifiable, neutral norms, the Article offers a more viable and timely solution to the perils of foreign surveillance.

INTRODUCTION

> [F]or our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world.[1]
>
> – President Obama, January 17, 2014

One of the most significant geopolitical developments in the past several years has been the leaks by Edward Snowden regarding the breadth and depth of electronic surveillance undertaken by the U.S. National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), and other states' intelligence apparatuses. These revelations have distressed the many state leaders, elites, and foreign citizens who have been subject to this surveillance. One source of their outrage is the belief that the surveilling governments have violated basic expectations of privacy. Another problem is that one obvious source of regulation — international law — has little to say about foreign surveillance. States have tended to regulate the surveillance of their own citizens more stringently than that of foreign nationals. But as states rapidly increase their technological capabilities to collect electronic intelligence in far-flung geographies, this lack of regulation of foreign surveillance becomes more fraught.

This is the first puzzle that this Article will address: Why has international law had so little to say about how, when, and where governments may spy on other states and foreign citizens, including by electronic means? Historically, spying was heavily driven by states' efforts to collect intelligence about decision-making in foreign governments. Collecting intelligence about average citizens was less common or secondary, and few individuals saw surveillance as implicating their own rights. As a result, states sensibly concluded that the benefits to unregulated spying were high and the corresponding costs were few. Terrorist threats and the Snowden leaks changed that: Suddenly, foreign surveillance is personal and pervasive, caught in a bright and uncomfortable spotlight. The absence of international legal rules regarding surveillance has become stark and keenly felt.

International relations (IR) theory offers several ways to think about conditions under which states may decide to make international law. States turn to international law to achieve different goals, including overcoming

1. President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) [hereinafter Obama NSA Speech], *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

collective action problems, coordinating on issues that inherently require a multilateral approach, and signaling normative commitments. Whether one looks at the problem from a realist, institutionalist, liberalist, or constructivist perspective, there is reason to think as a positive matter that current conditions are ripe for states to employ international law to regulate foreign surveillance. These IR theories also shed light normatively on why states should seize this moment to regulate. Developing international norms of surveillance would offer several instrumental and expressive benefits, including the ability for states to set the agenda, relieve pressures emerging from human rights fora, and signal an underlying commitment to accountable government. This Article will argue that a unique confluence of circumstances is poised to result in novel developments in international law.

Post-Snowden pressures to regulate foreign surveillance are emerging from different corners of the international playing field. Activities in the United Nations, cases in the International Court of Justice (ICJ) and European courts, and domestic policy changes in states such as the United States are all exerting pressures on the *status quo*, but reveal a lack of consensus about what the substantive right to privacy (and therefore the international regulation of surveillance) should entail. Given that this convergence of pressures on states to rein in some of their surveillance activities has begun only recently, few — if any — scholars have marshaled and analyzed these developments as possible catalysts for change. This Article will do so, arguing that these pressures should be viewed as serious enough to cause some subset of states to recalculate upward the level of international regulation that is in their self-interest — that is, to prompt a turn to international law.

Having argued that change should come, the natural questions that follow are: What should those changes look like, and from where should states draw inspiration for these international norms? This Article will offer the first sustained discussion of the content and possible sources of those norms. Though several scholars have debated whether there is such a thing as an "international right to privacy," few have borne down on what the content of that right might look like.[2] Although some human rights groups have advocated for substantive developments around the right to privacy, discussions among states are insufficiently detailed at this

2. One recent exception is Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, HARV. INT'L L.J. (forthcoming 2015), *available at* http://ssrn.com/abstract=2418485 (discussing factors such as necessity and proportionality as substantive factors that will shape international privacy discussions). For a brief assessment of the feasibility of adopting transatlantic privacy standards for surveillance and venues in which that might occur, see Ian Brown, *The Feasibility of Transatlantic Privacy-Protective Standards for Surveillance*, 23 INT'L J.L. & INFO. TECH. 23 (2015).

stage to provide international privacy norms of real substance.[3] This is in part because even domestically, understandings of privacy are shifting as states and their citizens gain a greater understanding of the ways in which technology can intrude into hitherto private spheres.[4] At the same time, governments will continue to feel pressure to protect their citizens from harm, particularly in an age of terrorism by nonstate actors, and surely will not cease to conduct foreign surveillance. As a result, new international norms, at least in the first instance, should be procedural rather than substantive, both because a consensus about procedural norms is easier to achieve in the context of secret activity, and because a focus on procedural norms will allow states to avoid, for the time being, contentious discussions about their disparate views on fundamental aspects of personal privacy.[5] To best achieve states' goals, these procedural norms should advance three core rule of law values: transparency, accountability, and limits on governmental discretion.

In considering the inspiration for the norms that should emerge, the Article will argue that the most promising source of new international norms is domestic law. Domestic laws can and do serve as the basis for international legal developments, particularly in the face of highly politicized issues, non-reciprocal incentive structures, issue complexity, and different conceptions of the proper legal framework — all of which are

3. *See, e.g.*, *International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY & PROPORTIONATE (May 2014), https://en.necessaryandproportionate.org/ (last visited Apr. 15, 2015) [hereinafter NECESSARY & PROPORTIONATE, *Principles*] (arguing, contradictorily, that law has not kept up with modern communications surveillance and that states "must comply" with a long list of principles in order to "actually meet their international human rights obligations"); AM. CIVIL LIBERTIES UNION [ACLU], PRIVACY RIGHTS IN THE DIGITAL AGE (2014), *available at* https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf.

4. For an example of the U.S. Supreme Court wrestling with changing notions of privacy in a surveillance-heavy world, see United States v. Jones, 132 S. Ct. 945, 955, 957 (2012) (Sotomayor, J., concurring) ("[P]hysical intrusion is now unnecessary to many forms of surveillance. . . . [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." (citations omitted)). In October 2013, the U.K. parliamentary committee that oversees intelligence opened an inquiry into whether the laws that govern U.K. intelligence agencies' ability to intercept private communications were adequate and how to strike the proper balance between the individual right to privacy and the collective right to security. *See* Press Release, Intelligence & Sec. Comm. of Parliament (Oct. 17, 2013) (U.K.), *available at* https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20131017_ISC_statement_privacy_and_security_inquiry.pdf.

5. As discussed *infra* Part III.B., this Article will deem "procedural" those surveillance norms that are objectively verifiable and do not require case-by-case or discretionary value judgments about privacy or security equities in assessing compliance with the norm.

present in the surveillance debate.[6] Further, domestic surveillance laws have been test-driven in the real world and reflect concerted efforts by particular polities to balance liberty and security. As a result, the Article will draw from the domestic surveillance laws of various states to extract six procedural principles that states should adopt on the international plane. The norms that first emerge will not immediately constitute customary international law (CIL), but will serve as the grain of sand around which the pearl of CIL can form.

In effect, this Article will reject both an aggressively cynical approach to foreign surveillance and an unduly optimistic view that states will converge around robust international privacy protections in the short term. The cynics assume that whatever pressures currently exist to modify the *status quo* will diminish in short order, overtaken by subsequent geopolitical crises.[7] The optimists argue that states should develop the substantive principle of privacy contained in the International Covenant on Civil and Political Rights (ICCPR), and have robust aspirations for what that principle should contain.[8] Both of these approaches are flawed, normatively and predictively. The cynics underestimate both the enduring nature of human rights pressures on states and the benefits to states of creating new international legal rules in this area. The optimists underestimate the difficulty of agreeing on concrete, substantive norms in a multilateral setting among states with varied incentives. For this reason, states should focus first on establishing procedural limitations that reduce (though not eliminate) differences between their treatment of citizens and foreigners.

---

6. Ashley Deeks, *Domestic Humanitarian Law: Developing the Law of War in Domestic Courts*, *in* APPLYING INTERNATIONAL HUMANITARIAN LAW IN JUDICIAL AND QUASI-JUDICIAL BODIES 133 (Derek Jinks et al. eds., 2014) [hereinafter Deeks, *Domestic Humanitarian Law*].

7. *See, e.g.*, Benjamin Wittes, *Der Spiegel on U.S.-German Relations*, LAWFARE (May 6, 2014, 7:18 AM), http://www.lawfareblog.com/2014/05/der-spiegel-on-u-s-german-relations/; Eric A. Posner, Statement to the Privacy & Civil Liberties Oversight Board (Mar. 14, 2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/03/Eric-A.-Posner.pdf (noting that most countries cannot afford to break off intelligence cooperation with the United States because they rely so heavily on the stronger U.S. surveillance capabilities).

8. For a recognition that the law currently is unclear and requires development, see Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137 (2014); Laura Pitter, Comments of Human Rights Watch to the Privacy & Civil Liberties Oversight Board Hearing 8 (Mar. 19, 2014), *available at* http://www.hrw.org/sites/default/files/related_material/PCLOB%203-19-14%20Hearing%20Submission_1.pdf (implicitly recognizing lack of clarity in law when stating that "[c]oncepts of jurisdiction based on control over territory and persons . . . can and should adapt to the reality of mass digital surveillance"); NECESSARY & PROPORTIONATE, *Principles*, *supra* note 3 (stating that "logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear").

Three caveats are in order. First, not all states will be attracted to the norms discussed herein, at least in the short to medium term. Non-democratic states, such as China, and partly democratic states, such as Russia, are relatively impervious to public pressure to alter their surveillance practices. Nevertheless, states such as the United States, European Union members, Australia, New Zealand, Canada, and Japan have good reasons to conclude that the benefits of adopting such norms outweigh the costs. A second and related caveat is that states are unlikely to adopt new international norms of surveillance unilaterally, without comparable commitments from at least some other states. One possibility is that a core group of trusted allies would develop these norms initially among themselves, with the idea that other states later could adhere, both publicly and privately, to the established norms. Third, this discussion assumes an absence of another catastrophic terrorist attack along the lines of the one that took place on September 11, 2001. Most of the pressures discussed in the Article will pale in the face of such an attack, which almost certainly would push policymakers to rely even more heavily on foreign surveillance and to reject increased regulation of those surveillance activities.

The Article will proceed as follows. Part I will analyze why international law largely has failed to regulate spying. As a preliminary matter, it will define what this Article means by "spying": the surveillance by one state during peacetime of the communications of another state's officials or citizens who are located outside the surveilling state's territory, by use of electronic means that include Internet and cell phone monitoring, satellites, and drones. The Article will identify several variants in the current legal approach to spying, including the views that (1) international law neither permits nor prohibits spying; (2) international law affirmatively allows spying; and (3) certain international legal obligations may be read to regulate foreign spying but consistently are ignored. Part I will proceed to analyze why states have been unwilling or unable to enact international rules to regulate spying and why, in light of recent developments, states' calculations may begin to change.

Part II will set forth four established IR theories that purport to describe and predict state behavior, and will argue that under any of these four theories it is reasonable to expect at least some states to advert to international law to advance their interests. Part II also will describe the political, human rights-driven, and economic pressures that states are facing to regulate foreign surveillance, and will offer a taxonomy of states that bear different interests in this international regulatory process. It also will explain what the Article means by "international norms," in contrast to fully realized CIL rules.

Having identified the value to states of employing international norms to regulate foreign surveillance, Part III will take up the challenge of what these early international norms should look like. After explaining why domestic laws can serve as an important source of inspiration for international norms under certain conditions, this Part will extract common principles from surveillance laws of the United States, the United Kingdom, Canada, Australia, and Germany and will argue that states should adopt these principles internationally. These principles include: (1) notice to the public of the applicable rules; (2) limits on the reasons that states may collect or query data; (3) a requirement for periodic reviews of surveillance authorizations; (4) limits on how long the data can be held; (5) a preference for domestic action (i.e., action by the host state intelligence services) wherever reasonable; and (6) the existence of a neutral body to authorize surveillance *ex ante* or review it *ex post*. Part III will conclude by addressing various potential objections to these international norms.

I. INTERNATIONAL LAW ON SURVEILLANCE: EXPLAINING THE AGNOSTICISM

A. Defining Surveillance

The concept of peacetime espionage or spying encompasses a wide range of clandestine government activities.[9] It includes the use of human sources to obtain information of interest to the governments for which those sources work. It includes the wiretapping of the cell phones of foreign nationals suspected of terrorist activity. It includes the use of satellite imagery to detect activities at another state's nuclear facilities or mass atrocities during a civil war. And it includes efforts to obtain greater knowledge about other states' military capabilities.[10]

---

9. Espionage occurs during wartime as well. Wartime espionage traditionally was conducted by soldiers out of uniform crossing enemy lines to gather information about troop numbers, movements, or locations. The 1907 Hague Regulations define a spy (for wartime purposes) as one who, "acting clandestinely or on false pretences . . . obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party." Hague Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulations Respecting the Laws and Customs of War on Land art. 29, Oct. 18, 1907, 36 Stat. 2277; *see also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 46, June 8, 1977, 1125 U.N.T.S. 3. This Article focuses on peacetime surveillance because that is predominately the context in which recent developments have occurred.

10. *See, e.g.*, Adam Entous, Julian E. Barnes & Siobhan Gorman, *U.S. Scurries to Shore up Spying on Russia*, WALL ST. J., Mar. 24, 2014, http://www.wsj.com/articles/SB10001424052702304026304579453331966405354 (discussing U.S. surveillance of Russian troop movements).

Electronic surveillance has a decades-long history, and from its inception it was used both to facilitate war-fighting and to assist diplomats in assessing each other's plans.[11] As early as 1950, the United States undertook electronic surveillance not just against foreign governments but also against foreign nationals.[12] Nevertheless, a survey of the subjects of collection until recently seems heavily weighted toward governmental actors.[13]

Although "espionage" in the colloquial sense encompasses a wide range of collection activity, it is in the area of electronic surveillance that international law is most under pressure, and in which we are most likely to witness developments. The idea that one state sends undercover operatives overseas to spy on foreign government actions and recruit foreign officials is not of particular interest to the general public or human rights and civil liberties advocates, although it is of intense interest to governments themselves. Since human intelligence collection is more costly, time-intensive, and detectable, there is a lower likelihood that international law will begin to regulate human intelligence collection.

As a result, this Article focuses on the category of spying that consists of foreign surveillance. "Foreign surveillance" here refers to the clandestine surveillance by one state during peacetime of the communications of another state's officials or citizens, when those communications take place partly or entirely outside the surveilling state's territory, using electronic means, including cyber-monitoring, telecommunications monitoring, satellites, or drones. Foreign surveillance is comprised of two types of surveillance: "transnational surveillance" and "extraterritorial surveillance."[14] Transnational surveillance refers to the

---

11. George F. Howe, *The Early History of NSA*, CRYPTOLOGIC SPECTRUM, Spring 1974, at 11, 11–12, *available at* http://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf.

12. NAT'L SEC. COUNCIL, INTELLIGENCE DIRECTIVE NO. 9, ¶ 12(a) (1950), *available at* https://history.state.gov/historicaldocuments/frus1945-50Intel/d435 (defining "foreign communications" as "includ[ing] all telecommunications and related materials . . . of the government *and/or their nationals* or of any military, air, or naval force, . . . or of any person or persons acting or purporting to act therefor" (emphasis added)).

13. *See, e.g.*, JAMES BAMFORD, THE PUZZLE PALACE: INSIDE THE NATIONAL SECURITY AGENCY, AMERICA'S MOST SECRET INTELLIGENCE ORGANIZATION 43 (1983) (describing communications intelligence as indicating throughout WWII how many ships Japan had, where they were, and when they were lost); *id.* at 49 (describing targets as including "advanced weapon systems, troop movements, and so on"); *id.* at 283 (describing eavesdropping on Soviet government leaders); *id.* at 313 (describing British collection of Germany military traffic). *But see* Joe Kloc, *The History of NSA Spying, from Telegrams to Email*, DAILY DOT (June 17, 2013, 10:41 AM), http://www.dailydot.com/politics/nsa-prism-shamrock-history-spying-telegraphs/ (describing how the Army in 1945 reviewed all incoming international telegrams to look for encrypted intelligence and examples of Soviet spying).

14. For a useful comparable taxonomy, see Craig Forcese, *Spies Without Borders: International Law*

surveillance of communications that cross state borders, including those that begin and end overseas but incidentally pass through the collecting state. Extraterritorial surveillance refers to the surveillance of communications that take place entirely overseas. For example, if Australia were to intercept a phone call between two French nationals that was routed through a German cell tower, this would be extraterritorial surveillance. In contrast, surveillance that takes place on the surveilling state's territory ("domestic surveillance") against either that state's nationals or any other individual physically present in that state is generally regulated by the ICCPR, as discussed below.[15] This Article focuses predominately on transnational and extraterritorial surveillance, arguing that states should close the gap between the ways in which they regulate the two.

This taxonomy of communications is not the only possible way to think about the issue. This Article's approach focuses on the location of the individuals who are engaged in the communications. An alternative approach could focus on the place at which the communication itself is intercepted. Under that approach, communications that incidentally pass through a state would be treated as "domestic communications" if the state intercepted them in its own territory, even though the sender and recipient of the communications are located overseas. Some of the human rights bodies currently seized with surveillance questions may begin to use the communication itself as the unit of analysis, rather than the location of the communicators. I use the individual as the unit of analysis because to date courts and treaty bodies have primarily focused on the location of the individual claiming a particular human right.[16] Nevertheless, states and human rights bodies may eventually abandon this approach because they decide it is hard to reconcile with the nature of electronic communications and their interception.

B. Three Approaches

Until recently, there was significant consensus about international law's relation to espionage. With a few exceptions discussed below, most scholars agree that international law either fails to regulate spying or affirmatively permits it.

---

and Intelligence Collection, 5 J. NAT'L SECURITY L. & POL'Y 179, 183–84 (2011).

15. One exception to this statement is the spying by a receiving state on a sending state's diplomatic mission or officials. This should be considered "surveillance" for purposes of this Article, but would not be regulated by international law, as discussed *infra* Part I.B.3. (analyzing Vienna Convention on Diplomatic Relations and ICCPR).

16. *See infra* Part I.B.3.b.

1. The Lotus *Approach*

The *Lotus* case in the Permanent Court of International Justice famously stands for the proposition that, in the absence of a positive rule, states are free to act.[17] The burden falls on the objecting states to show that the acting state has consented to — or is otherwise subject to — a restriction on its actions.[18] The Court stated that international law leaves to states "a wide measure of discretion which is only limited in certain cases by prohibitive rules" and that in the absence of such rules "every State remains free to adopt the principles which it regards as best and most suitable."[19] The *Lotus* principle thus becomes relevant when there is a gap or lacuna in the law — a situation of "*non liquet*."[20] Although the *Lotus* Court's rigid adherence to a state's consent as the sole source of its obligations has been supplanted by more modern understandings of how international law works, the underlying idea remains that if no limits are established, a state remains free to act as it wishes.[21]

Several government officials and scholars believe that the *Lotus* approach provides the best way to think about spying in international law. For them, the idea is simply that nothing in international law forbids states from spying on each other; states therefore may spy on each other — and each other's nationals — without restriction. Spying is therefore unregulated in international law.[22] Further, this group presumably would

---

17. S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 19 (Sept. 7).

18. *Id.* at 18, 31.

19. *See id.* at 18–19.

20. Michael J. Glennon, *The Fog of Law: Self-Defense, Inherence, and Incoherence in Article 51 of the United Nations Charter*, 25 HARV. J.L. & PUB. POL'Y 539, 555 n.49 (2002); Prosper Weil, *"The Court Cannot Conclude Definitely . . .":* Non Liquet *Revisited*, 36 COLUM. J. TRANSNAT'L L. 109, 109 (1997).

21. Michael Glennon, *The Road Ahead: Gaps, Leaks and Drips*, 89 INT'L L. STUD. 362, 374 (2013) [hereinafter Glennon, *The Road Ahead*] ("Whatever the conceptual difficulties with the notion of consent, it remains true that unless a restriction is established, a State remains free to act.").

22. *See, e.g.*, OFFICE OF GEN. COUNSEL, DEP'T OF DEF., AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 29 (1999), *available at* http://www.dtic.mil/get-tr-doc/pdf?AD=ADB257057 ("International communications law contains no direct and specific prohibition against the conduct of information operations by military forces, even in peacetime."); Daniel B. Silver, *Intelligence and Counterintelligence*, *in* NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005) (updated and revised by Frederick P. Hitz & J.E. Shreve Ariail) (espionage neither legal nor illegal); W. Hays Parks, *The International Law of Intelligence Collection*, *in* NATIONAL SECURITY LAW 433, 433–34 (John Norton Moore et al. eds., 1990) ("No serious proposal ever has been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each."); Gary D. Brown, *The Wrong Questions About Cyberspace*, 217 MIL. L. REV. 214 (2013) (espionage not considered to be prohibited by international law); Gary D. Brown & Andrew O. Metcalf, *Easier Said than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SECURITY L. & POL'Y 115, 116–17 (2014) ("[T]here is a long-standing (and cynically named) 'gentleman's agreement' between nations to ignore espionage in international law . . . ."); Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 321 (1996) ("International law regarding

point to the widespread practice of spying to counter any suggestion that a customary international norm had developed against spying. In this view, ideas such as non-intervention and sovereignty developed against a background understanding that states do and will spy on each other, thus establishing a carve-out for espionage within those very concepts.

2. International Law as Permissive

A slight variation to the *Lotus* approach is the notion that international law should be read affirmatively to permit spying. Several scholars have suggested that spying is a precursor to (and an integral part of) a state's right to act in self-defense.[23] That is, for a state to be able to accurately anticipate and prepare for an armed attack before it occurs, it must be lawful for that state to gather intelligence on foreign military and governmental decision-making. To deem spying unlawful in international law would be to vitiate a state's critical and well-established right of self-defense, which no state would tolerate.[24]

Other scholars interpret the widespread state practice of espionage as indicating that states affirmatively recognize a right to engage in that conduct.[25] Indeed, government officials have publicly asserted that spying

---

peacetime espionage is virtually unstated . . . ."); Reese Nguyen, *Navigating* Jus Ad Bellum *in the Age of Cyber Warfare*, 101 CALIF. L. REV. 1079, 1082 (2013) (espionage neither condoned nor condemned under international law); A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595 (2007) (espionage neither condoned nor condemned under international law); Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. REV. 217, 217 (1999) (international law does not specifically prohibit espionage); Thomas C. Wingfield, *Legal Aspects of Offensive Information Operations in Space*, 9 U.S. AIR FORCE ACAD. J. LEGAL STUD. 121, 140 (1999) (noting lack of international prohibition of espionage).

23. *See* Forcese, *supra* note 14, at 198–99; Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L L. REV. 1091, 1092 (2004). This argument supports spying on hostile or enemy states, but does not support spying on close allies.

24. U.N. Charter art. 51 (affirming a state's right to self-defense against an armed attack).

25. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 123 (1999) (describing state practice as "specifically recogniz[ing] a right to engage in [espionage] as an inherent part of foreign relations"); Quincy Wright, *Espionage and the Doctrine of Non-Intervention in Internal Affairs*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW 3, 16–17 (Roland J. Stanger ed., 1962) (noting that British jurist Lassa Oppenheim concluded that espionage is not politically or legally wrong and that there is a general practice of espionage by all states); Jeffrey H. Smith, *Symposium: State Intelligence Gathering and International Law: Keynote Address*, 28 MICH. J. INT'L L. 543, 544 (2007) ("[B]ecause espionage is such a fixture in international affairs, it is fair to say that the practice of states recognizes espionage as a legitimate function of the state, and therefore it is legal as a matter of customary international law."); Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The Intelligence Function and World Public Order*, 46 TEMPLE L.Q. 365, 394 (1973) (discussing a "deep but reluctant admission of the lawfulness of such intelligence gathering, when conducted within customary normative limits"). For recent examples of states spying on each other, see David E. Sanger, *In Spy Uproar, 'Everyone Does It' Just Won't Do*, N.Y. TIMES, Oct. 25, 2013, http://www.nytimes.com/2013/10/26/world/europe/in-spy-uproar-everyone-does-it-just-wont-do.html?_r=0.

is permissible. President Obama recently stated that "few doubt[ ] the legitimacy of spying on hostile states."[26] Though legitimacy and legality are not identical, this is a relatively bold affirmation that the United States spies, at least on non-friendly states. British Prime Minister David Cameron reportedly pointed out at a European Union summit that spying capabilities have prevented many terror attacks.[27] The former French foreign minister, Bernard Kouchner, stated, "The magnitude of the eavesdropping is what shocked us . . . . Let's be honest, we eavesdrop too. Everyone is listening to everyone else."[28]

The fact that certain states have entered into arrangements with other states to limit such spying is additional evidence that international law either permits or does not prohibit spying.[29] If international law prohibited such spying, these agreements would be unnecessary. At the very least, the existence of these arrangements proves that international law is unclear about whether it regulates espionage.

In short, some believe that international law affirmatively permits espionage, as evidenced by longstanding and widespread state practice as well as by public statements by government officials that acknowledge the practice.

3. International Law as Prohibitive

On the other side of the argument are those who suggest that international law today prohibits espionage. Some members of this school note that states do not tend to overtly claim that spying is legal — though this presumably is due in large part to the fact that spying usually violates the spied-upon state's domestic laws, which makes it more complicated to assert a "right to spy."[30] This school often points to three international legal sources that could be read to regulate spying, though those sources

---

26. Obama NSA Speech, *supra* note 1.

27. *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, DER SPIEGEL, Oct. 27, 2013, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html [hereinafter *Embassy Espionage*].

28. Geir Moulson & John-Thor Dahlburg, *Merkel Calls Obama to Complain About Surveillance*, ASSOCIATED PRESS, Oct. 23, 2013 (internal quotation marks omitted), *available at* http://bigstory.ap.org/article/nsa-spying-scandal-outrage-calculation-too. *But see* Alissa J. Rubin, *French Condemn Surveillance by N.S.A.*, N.Y. TIMES, Oct. 21, 2013, http://www.nytimes.com/2013/10/22/world/europe/new-report-of-nsa-spying-angers-france.html (noting Mexican Foreign Ministry assertion that U.S. spying on the Mexican President was "unacceptable, illegitimate and contrary to Mexican and international law").

29. *See* Paul Farrell, *History of 5-Eyes – Explainer*, GUARDIAN, Dec. 2, 2013, http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer; W. Michael Reisman, Remarks, *Covert Action*, 20 YALE J. INT'L L. 419, 421 n.3 (1995) (describing the Soviet Union's agreements with its Eastern European satellites).

30. Wright, *supra* note 25, at 12, 17.

lack crisp content or have not been consistently read by states to inhibit foreign surveillance.

a. Sovereignty and Territorial Integrity

Two seminal principles in CIL are the obligations of states to respect the (a) sovereignty and (b) territorial integrity of other states.[31] Though widely cited, the substantive content of these broad principles remains the subject of debate. Generally, respect for sovereignty requires that states not interfere with the internal affairs of other states (except with those states' consent).[32] One might argue that surveillance interferes (albeit indirectly) with the internal affairs of another state by detecting communications related to those affairs.[33] By penetrating the internal discussions of a state, the surveilling state might be thought ultimately to weaken the spied-upon state's ability to effectively protect its own interests when it seeks to act.

Respect for territorial integrity is generally construed to mean that force should not be used to alter interstate boundaries.[34] But it also means that one state may not enter another state's territory, airspace, or territorial waters without the latter's consent.[35] Thus, some argue that the principle of territorial integrity "negates the general permissibility of strategic observation in foreign territory."[36] However, technological advances now allow states to conduct espionage against other states without actually penetrating the territory or airspace of those other states. For example, data packets that originate in Europe may pass through servers in the United States before being routed back to Europe. If the United States intercepts those packets while they are transiting the United States, it is

31. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 202–05 (June 27) (discussing non-intervention); *id.* ¶¶ 212–14 (discussing sovereignty and territorial integrity).

32. This principle is closely related to the principle of non-intervention. *See* U.N. Charter art. 2, ¶ 7; Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), Annex, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970) (setting forth principle concerning duty not to intervene in matters within domestic jurisdiction of any state and principle of sovereign equality, including the idea that "[t]he territorial integrity and political independence of the State are inviolable").

33. Wright, *supra* note 25, at 1, 12 (arguing that peacetime espionage violates international laws that protect state territorial integrity and political independence).

34. Mark Zacher, *The Territorial Integrity Norm: International Boundaries and the Use of Force*, 55 INT'L ORG. 215, 215 (2001).

35. *See* JOHN KISH, INTERNATIONAL LAW AND ESPIONAGE 83 (David Turns ed., 1995). For a comprehensive discussion of sovereignty and territorial integrity norms in the espionage context, see Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1081–87 (2006).

36. KISH, *supra* note 35, at 84.

hard to argue that the United States has violated the territorial integrity of the states from which the packets originated.[37] When states conduct surveillance from within a host state, however, a stronger argument can be made that a violation of the host state's territorial integrity has occurred.[38]

Even if both of these principles can be interpreted to cast doubt on the legality of espionage, states have not acted as though they do. States generally refrain from characterizing spying by other states as internationally illegal, at least when such spying collects intelligence about core state activities such as military capabilities. Further, the widespread and long-standing practice of spying — committed by many states in different regions of the world during time periods that both precede and post-date the UN Charter — undercuts arguments that these customary principles either were intended to prohibit espionage at the time they developed or should be deemed to do so today.

b. ICCPR

The ICCPR, to which most states are party, establishes a right to privacy. Article 17(1) states, "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[39] Putting aside the important jurisdictional question discussed below, there is little doubt that this right applies to a state's domestic collection of data about a person when that collection constitutes "interference," and many would agree that correspondence includes a person's online and telephonic communications. Nor is there disagreement that the right to privacy is a qualified right, subject to lawful and non-arbitrary interference by a state. Nevertheless, disagreement exists about which standards apply when assessing whether a state's domestic surveillance is lawful and non-arbitrary. The United States, for example, believes that states may engage in surveillance that is in accordance with transparent laws and that furthers a legitimate aim.[40] Human rights groups favor a higher standard drawn

37. Julius Stone, *Legal Problems of Espionage in Conditions of Modern Conflict*, *in* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, *supra* note 25, at 29, 36 (arguing that, in the face of space exploration and reconnaissance, "territorial sovereignty in the old sense of full psychological sacrosanctity is no longer with us"); Chesterman, *supra* note 35, at 1098 (noting that non-intervention norm has failed to keep pace with technological advances that render territorial limits irrelevant).

38. *But see, e.g.*, Weber & Saravia v. Germany, 2006-XI Eur. Ct. H.R. 309, 332 ¶ 81 (describing Germany's argument that extraterritorial surveillance of German citizen was "not contrary to public international law because the monitoring of wireless telecommunications did not interfere with the territorial sovereignty of foreign States").

39. International Covenant on Civil and Political Rights art. 17(1), *adopted* Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

40. *See* U.N. Office of the High Comm'r for Human Rights, United States Response to OHCHR

from European Court of Human Rights (ECtHR) case law: The interference must be necessary in the circumstances of the case and proportional to the end sought, and the surveillance must be conducted under specific and clearly defined laws.[41] Reasonable minds can differ about whether some of the intelligence surveillance that has recently come to light is consistent with the ICCPR. The United States would presumably argue that programs such as its bulk telephony collection under PATRIOT Act Section 215 are consistent with the ICCPR.[42] Human rights groups would disagree, arguing that bulk collection inherently is an arbitrary or disproportionate interference with privacy.

Just as the content of ICCPR Article 17 is disputed in the surveillance context, so too is the scope of its application. Some scholars argue that the ICCPR establishes an extraterritorial right to privacy.[43] Although no treaty body has addressed in detail how electronic surveillance implicates the ICCPR's right to privacy,[44] at least one human rights body has concluded that in general, foreign surveillance implicates the ICCPR.[45] It also seems

---

Questionnaire on "The Right to Privacy in the Digital Age," http://www.ohchr.org/Documents/Issues/Privacy/United%20States.pdf (last visited May 18, 2015).

41. Milanovic, *supra* note 2 (manuscript at 66) (describing ECtHR and HRC four-part tests for whether there has been a privacy violation, including whether the interference pursued a legitimate aim and was proportionate to that aim).

42. *See* U.N. Office of the High Comm'r for Human Rights, *supra* note 40 (implying that domestic U.S. surveillance is consistent with its interpretation of ICCPR Article 17).

43. *See* David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SECURITY (Oct. 29, 2013, 12:48 PM), http://justsecurity.org/2668/foreigners-nsa-spying-rights/; Martin Scheinin, *Letter to the Editor from Former Member of the Human Rights Committee, Martin Scheinin*, JUST SECURITY (Mar. 10, 2014, 10:32 AM), http://justsecurity.org/8049/letter-editor-martin-scheinin/ (arguing that ICCPR Article 17 applies extraterritorially to regulate a state's surveillance of foreign nationals); Manfred Nowak, *Letter to the Editor from Manfred Nowak, What Does Extraterritorial Application of Human Rights Treaties Mean in Practice?*, JUST SECURITY (Mar. 11, 2014, 8:06 AM), http://justsecurity.org/8087/letter-editor-manfred-nowak-extraterritorial-application-human-rights-treaties-practice/ (same); Ryan Goodman, *UN Human Rights Committee Says ICCPR Applies to Extraterritorial Surveillance: But Is That So Novel?*, JUST SECURITY (Mar. 27, 2014, 8:50 AM), http://justsecurity.org/8620/human-rights-committee-iccpr-applies-extraterritorial-surveillance-novel/. *But see* Jennifer Daskal, *Extraterritorial Surveillance Under the ICCPR . . . The Treaty Allows It!*, JUST SECURITY (Mar. 7, 2014, 5:09 PM), http://justsecurity.org/7966/extraterritorial-surveillance-iccpr-its-allowed/ (arguing that ICCPR only applies to persons within the acting state's authority or effective control, which is not the case when an acting state conducts surveillance); John B. Bellinger III, Testimony Before the Privacy & Civil Liberties Oversight Board (Mar. 19, 2014), *available at* http://www.pclob.gov/Library/20140319-Testimony-Bellinger.pdf (arguing that ICCPR does not apply extraterritorially).

44. Milanovic, *supra* note 2 (manuscript at 38).

45. *See* Human Rights Comm., Concluding Observations on the Fourth Periodic Rep. of the United States, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014) [hereinafter HRC Concluding Observations]. *Cf.* 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 (2014) (discussing trends in jurisprudence of human rights courts and bodies related to extraterritorial application of

likely that the ECtHR, interpreting a comparable privacy provision in the European Convention on Human Rights (ECHR), will decide that extraterritorial surveillance implicates that right.[46] Further, the General Assembly recently approved a resolution that appears to adopt the ICCPR's view.[47] However, it remains unsettled precisely when and how the treaty would apply to foreign electronic surveillance.

ICCPR Article 2(1) states, "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant . . . ."[48] The United States has long interpreted the ICCPR not to apply extraterritorially, because the U.S. government reads Article 2 as limiting the treaty to activity within U.S. territory.[49] This is a minority view. Many other states, as well as the Human Rights Committee (the ICCPR treaty body), assert that the ICCPR applies either when a person is within the territory of a state party or is subject to a state's jurisdiction (as when a state detains a non-national or exercises territorial control abroad).[50] The Commentary to the ICCPR does indicate, however, that when states were negotiating Article 17, they understood the prohibition on "unlawful" or "arbitrary" interference to refer to acts that conflicted with the state's domestic legal system (which tends to run with the state's territory).[51] There is no indication in the *travaux preparatoires* that states anticipated that the prohibition on arbitrary or unlawful interference with privacy or correspondence would extend to foreign nationals outside the territory of the state party. That may be explained by the state of technology at the time, however; signals intelligence was hardly as ubiquitous in 1966 as it is today.

---

human rights).

46. Milanovic, *supra* note 2 (manuscript at 4).

47. The Right to Privacy in the Digital Age, G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Jan. 21, 2014); *see also infra* note 166 (discussing U.N. Resolution 68/167).

48. ICCPR, *supra* note 39, art. 2(1).

49. *See* HRC Concluding Observations, *supra* note 45; 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/.

50. *E.g.*, Human Rights Comm., 80th Sess., General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 10, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004) (asserting that ICCPR requires states to "respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party").

51. MANFRED NOWAK, U.N. COVENANT ON CIVIL AND POLITICAL RIGHTS: CCPR COMMENTARY 382 (2d ed. 2005) ("Thus, the Covenant refers primarily to the national legal system . . . . Interference with privacy or an attack on honour by the State or the private sector consequently represents a violation of Art. 17 when it conflicts with the national legal system (laws, ordinances, judicial directives).").

Indeed, in July 2013, Germany publicly expressed interest in amending the ICCPR or concluding a protocol to that treaty.[52] Germany's goal was to clarify that the right to privacy contained in the ICCPR extends to electronic privacy. The German Justice Ministry reportedly went so far as to draw up treaty language that would regulate intelligence agencies' access to electronic data.[53] The fact that Germany thought — as recently as mid-2013 — that it was not obvious that the ICCPR regulates electronic surveillance (whether or not collected in bulk and whether or not extraterritorial) suggests that other states may not currently read Article 17 that way either.

Even if one reads Article 2 disjunctively, what counts as being subject to a state's jurisdiction is the subject of significant debate. Many states, scholars, and human rights bodies that read the geographic scope of the ICCPR expansively concede that a state party has obligations only to those individuals in territory under that state's "effective control" (the spatial model of jurisdiction) or who are subject to that state's legal jurisdiction (the personal model of jurisdiction).[54] Some states have accepted the "effective control" test (particularly those who are bound by the ECHR, which the ECtHR has found to apply extraterritorially in certain cases).[55] But even states such as Australia, Germany, and the United Kingdom, the practice of which human rights groups cite as evidence that virtually all states accept the extraterritorial application of the ICCPR, have accepted the treaty's application in narrow circumstances that fall short of an expansive "effective control" test.[56]

---

52. Ryan Gallagher, *After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty*, SLATE: FUTURE TENSE (Sept. 26, 2013, 2:16 PM), http://www.slate.com/blogs/future_tense/2013/09/26/article_17_surveillance_update_countries_want_digital_privacy_in_the_iccpr.html (describing Germany's protocol efforts); Matthias Bölinger, *Berlin Calls for Global Data Protection Rules*, DEUTSCHE WELLE (July 16, 2013), http://www.dw.de/berlin-calls-for-global-data-protection-rules/a-16952477.

53. Bölinger, *supra* note 52.

54. Milanovic, *supra* note 2 (manuscript at 37–46).

55. Harold Hongju Koh, Memorandum Opinion on the Geographic Scope of the Covenant on Civil and Political Rights 43 (Oct. 19, 2010), *available at* http://www.nytimes.com/interactive/2014/03/07/world/state-department-iccpr.html (stating that Netherlands recognizes applicability of ICCPR abroad where the country exercises "full and effective control" (internal quotation marks omitted)).

56. *Id.* at 37–42. The memo discusses the positions of Israel (rejecting the extraterritorial application of the ICCPR); Australia (stating that a high standard needs to be met before a State could be considered to be in effective control of territory abroad); Belgium (stating that it ensures the rights of all persons under its jurisdiction when members of its armed forces are deployed abroad); Germany (same); and the United Kingdom (stating that the ICCPR can have extraterritorial effect only in "very exceptional cases," such as military detention). Of course, states such as Germany and the United Kingdom are bound by the ECHR and the decisions of the ECtHR. That Court is increasingly moving away from a territorial control model of extraterritorial application, and is focused more intently on a state's ability to respect particular rights. *See* Van Schaack, *supra* note 45,

When using the personal model of jurisdiction, courts have asked whether a person is within a state's "control and authority,"[57] though they have attempted to constrain that broad test by considering whether the state was acting in the exercise of public powers in the area in which the act occurred.[58] Other scholars believe that a state has obligations to respect the rights of individuals in an even broader set of circumstances: when a state has "*authority* . . . over a person *or a context*."[59] In support, they cite two Human Rights Committee (HRC) cases in which the state was found to have violated an individual's rights when it controlled either a payment to the individual or the individual's ability to leave a foreign country.[60] In the latter case, control over a person's ability to leave one state and enter a different state has elements of physical control that are consistent with common understandings of what it means to have control over a person. Even if this has been the approach of the HRC in a few cases, there does not appear to be widespread state acceptance of the concept of "authority over a person or a context" as the correct legal interpretation of the ICCPR.[61] In any case, two non-binding holdings by a treaty body do not, standing alone, elevate to a rule of law "authority over a person or context" as the relevant jurisdictional provision of the ICCPR.

No court or human rights body has dealt expressly with how to apply any of these jurisdictional approaches to surveillance. If a court or treaty

---

at 52 ("The current state of the law would thus dictate that human rights obligations exist wherever a State exercises *de facto* authority or control over territory, individuals, or a transaction and has the power to respect and ensure the enjoyment of rights and freedoms.").

57. *E.g.*, Al-Skeini v. United Kingdom, 2011-IV Eur. Ct. H.R. 99 ¶ 137.

58. Milanovic, *supra* note 2 (manuscript at 45–46).

59. Scheinin, *supra* note 43 (emphasis added) (quoting Koh, *supra* note 55) (internal quotation marks omitted); Koh, *supra* note 55. The ACLU construes "effective control" to include virtual power or control. ACLU, *supra* note 3, at 5. At least one scholar has argued that the ICCPR "expressly guarantees a right of privacy to all human beings." David Cole, *More on the Rights of Others — Ben Wittes' Failure of Imagination*, JUST SECURITY (Nov. 12, 2013, 4:44 PM), http://justsecurity.org/3128/rights-ben-wittes-failure-imagination/.

60. Rep. of the Human Rights Comm., Views of the Human Rights Committee Under Article 5, Paragraph 4, of the Optional Protocol to the International Covenant on Civil and Political Rights, Annex X, Commc'n No. 196/1985; GAOR, 44th Sess., Supp. No. 40 (1989) (Gueye v. France) (payments); Rep. of the Human Rights Comm., Views of the Human Rights Committee Under Article 5 (4) of the Optional Protocol to the International Covenant on Civil and Political Rights Concerning Communication No. R.13/57, Annex XIII; GAOR, 37th Sess., Supp. No. 40 (1982) (Vidal Martins v. Uruguay) (passport withholding).

61. Further, as John Bellinger points out, these HRC cases preceded the HRC's adoption of General Comment 31 by fifteen years. The HRC thus in General Comment 31 chose to limit its interpretation of Article 2 to the concept of "effective control," notwithstanding its possibly broader interpretation of that provision many years earlier. John Bellinger, *A Reply to Ryan Goodman on the Application of the ICCPR to NSA Surveillance*, LAWFARE (Mar. 30, 2014, 3:05 PM), http://www.lawfareblog.com/2014/03/a-reply-to-ryan-goodman-on-the-application-of-the-iccpr-to-nsa-surveillance/.

body were to adopt an "effective control" test to govern the extraterritorial application of the right to privacy (under the ICCPR or ECHR), it likely would conclude that the state conducting foreign surveillance lacks effective control over the territory in which it is conducting surveillance. Even if a court or treaty body adopted a personal model of jurisdiction, it is not clear that intercepting someone's phone calls or email renders that person within the surveilling state's control and authority,[62] particularly because surveillance often is entirely passive and the surveilling state cannot — on its own — impose physical or legal consequences on the person being surveilled. It therefore is difficult to predict how these actors (and states themselves) will approach the question.

Council of Europe member states (i.e., most states in Europe) have different and arguably more extensive human rights treaty obligations, but these obligations, too, are subject to jurisdictional limits. The ECHR requires states parties to "secure to everyone within their jurisdiction the rights and freedoms" in the Convention.[63] Those rights include the respect for private and family life, home, and correspondence, subject to certain exceptions (such as national security, public safety, and the economic well-being of the country).[64] While there is extensive and internally contradictory case law in the ECtHR about what "within [a state's] jurisdiction" means, a common thread is the "control and authority test" — which requires that the individual complaining of an ECHR violation was under the control and authority of the state that allegedly violated his rights.[65] Many (though not all) of these cases involved detention — cases in which a state exercised some level of physical authority and control over the individual who claimed the rights violation.[66]

---

62. *See, e.g.*, Pitter, *supra* note 8, at 8 (implicitly recognizing lack of clarity in law when stating that "[c]oncepts of jurisdiction based on control over territory and persons . . . can and should adapt to the reality of mass digital surveillance"); NECESSARY & PROPORTIONATE, *Principles*, *supra* note 3 (stating that "logistical barriers to surveillance have decreased and the application of legal principles in new technological contexts has become unclear"). Even assuming that ICCPR Article 17 applies extraterritorially, and places obligations on states that conduct surveillance on foreign nationals (even though those states do not exercise "effective control" over those nationals), Article 17 only requires that the state's surveillance not be arbitrary or unlawful.

63. Convention for the Protection of Human Rights and Fundamental Freedoms art. 1, *done* Nov. 4, 1950, 213 U.N.T.S. 221.

64. *Id.* art. 8.

65. *See* Fact Sheet, European Court of Human Rights, Extra-Territorial Jurisdiction of States Parties to the European Convention on Human Rights (Nov. 2014), *available at* http://www.echr.coe.int/Documents/FS_Extra-territorial_jurisdiction_ENG.pdf (summarizing extraterritorial jurisdiction cases).

66. *See, e.g.*, Al-Jedda v. United Kingdom, 2011-IV Eur. Ct. H.R. 305 (case involving U.K. custody of detainee in Iraq in which the ECtHR found that the ECHR applied).

Intercepting telephone calls and reading someone's email is a far cry from the type of state control required by the control and authority test. Several cases related to the United Kingdom's Government Communications Headquarters and U.S. National Security Agency surveillance are pending before the ECtHR.[67] In addressing these cases, the Court likely will attempt to translate the "effective control" test into the electronic surveillance realm and may well alter the current understanding of the level of control a state must have over a person before his rights under the ECHR are triggered.

As noted above, the ICCPR quite clearly applies when a state is conducting domestic surveillance, whether or not those subject to surveillance are nationals of the state.[68] Those individuals are within a state's territory and subject to its jurisdiction under ICCPR Article 2. However, because it is not yet accepted that the ICCPR applies to situations in which a state is simply monitoring the electronic data of someone abroad, the ICCPR — as states seem to understand the treaty today — does not necessarily reach cases in which a state surveils foreign communications that pass through its territory.[69] For this reason, this Article is concerned not only with purely extraterritorial surveillance (cases in which State A surveils communications that happen entirely in State B), but also with transnational surveillance: communications sent by someone in State B (directed to someone in State C) that incidentally transit State A, as well as communications sent by someone in State B that are received in State A, but where the person in State B is the ultimate target of the surveillance.[70]

---

67. Press Release, Amnesty Int'l, Amnesty International Takes UK Government to European Court of Human Rights over Mass Surveillance (Apr. 10, 2015), *available at* https://www.amnesty.org/press-releases/2015/04/amnesty-international-takes-uk-government-to-european-court-of-human-rights-over-mass-surveillance/; Big Brother Watch v. United Kingdom, App. No. 58170/13, Eur. Ct. H.R. (2013). In the *Big Brother* case, the applicants allege at least two violations of the ECHR: the reception by GCHQ of data collected by NSA through its PRISM and upstream collection programs; and the conduct of GCHQ's Tempora program, whereby the United Kingdom collected transnational metadata and content of emails and website histories. *Id.* at 2–3.

68. It is not entirely clear that ICCPR Article 17 would regulate the state's collection and use of bulk metadata, because of the limited information that such surveillance provides. For purposes of this Article, though, I assume that the collection of both metadata and content potentially implicate Article 17. *See* ACLU, *supra* note 3, at 10.

69. ECtHR case law suggests that the ECHR might apply in such a case, however. In *Soering v. United Kingdom*, the Court held that the United Kingdom could not extradite a person to a state in which he might face treatment that would violate the ECHR. Soering v. United Kingdom, 161 Eur. Ct. H.R. (ser. A) at 35–36 ¶ 91 (1989). The implication of this case is that a state action taken within that state's territory that has an extraterritorial effect sometimes can implicate the state's ECHR obligations.

70. Communications sent by someone in State B to someone in State A generally will trigger ICCPR obligations in relation to the person in State A because that person is located in State A's territory.

In sum, we may be seeing a subtle shift in the widespread consensus that the ICCPR does not regulate espionage and, specifically, foreign electronic surveillance. Until recently, the question simply was not one that states were forced to confront. States now face novel questions about how the ICCPR applies to foreign electronic surveillance. The answers are nascent at best.

c. Vienna Convention on Diplomatic Relations

Article 41 of the Vienna Convention on Diplomatic Relations (VCDR) requires all persons receiving diplomatic immunity to "respect the laws and regulations of the receiving State."[71] One possible interpretation of this provision is that states parties have agreed that their diplomats will not spy in the receiving state, as that would violate the receiving state's domestic laws. At the same time, the Convention is highly protective of those with diplomatic status. Although a diplomat suspected of spying on the receiving state may be declared *persona non grata* and expelled,[72] the receiving state may not prosecute the diplomat for spying, given his immunity from criminal and civil process.[73] In practice, sending states commonly use diplomatic missions as bases from which to spy on receiving states, a fact that is known to the receiving states.[74] Recent news reports are rife with descriptions of spying conducted from within diplomatic posts.[75]

Approaching the question from the reverse angle, one could argue that the VCDR prohibits receiving states from spying on the facilities of sending states in the receiving state's territory. Articles 22 and 24 provide that the premises of diplomatic missions and the mission's documents and archives, respectively, are inviolable.[76] From that, one might argue that it is unlawful to penetrate that mission, even using electronic means. However,

71. Vienna Convention on Diplomatic Relations art. 41(1), *opened for signature* Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95 [hereinafter VCDR].

72. *Id.* art. 9.

73. *Id.* arts. 29, 31.

74. Radsan, *supra* note 22, at 621–22 ("The receiving country's intelligence and security services routinely assume, unless confirmed otherwise, that everyone on the list, no matter the formal designation, is an intelligence officer. As a part of standard tradecraft, they will check his background and conduct surveillance.").

75. Jens Glüsing et al., *Fresh Leak on US Spying: NSA Accessed Mexican President's Email*, DER SPIEGEL, Oct. 20, 2013, http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html (describing spying out of U.S. Embassies in Mexico City and Brasilia); *Embassy Espionage*, *supra* note 27 (describing spying out of U.S. Embassy in Berlin); George Roberts, *Indonesia Summons Australian Ambassador to Jakarta Greg Moriarty over Spying Reports*, AUSTRALIAN BROAD. CORP. (Nov. 1, 2013, 1:19 PM), http://www.abc.net.au/news/2013-11-01/indonesia-australian-embassy-spying-spies-espionage-jakarta/5062626.

76. VCDR, *supra* note 71, arts. 22, 24.

now-Justice Antonin Scalia, when working at the U.S. Department of Justice's (DOJ) Office of Legal Counsel, drafted a memorandum on this issue, concluding that the practice of spying on foreign missions was so widespread that the "inviolability" provision of the VCDR should not be read to prohibit such activities.[77] The same analysis could apply to the question of spying by the sending state using the mission as a base: It is so widespread that it is inappropriate to interpret VCDR Article 41 as prohibiting such activity. States manifestly have not interpreted the VCDR that way. Further, even though spying was widespread at the time states negotiated the VCDR, states did not explicitly address spying in the treaty.

******

In short, several treaties conceivably could be read to reflect efforts by states to limit espionage. However, the practice by states both before and after the treaties' adoption (which reflects widespread espionage), the dearth of claims about treaty or CIL violations, and the recent efforts to amend the ICCPR to include digital privacy all strongly suggest that states traditionally have not viewed existing treaties (or CIL) as regulating electronic surveillance in a meaningful way.

C. Reasons for International Law Agnosticism

This Subpart considers why states have been unwilling or unable to enact international rules to regulate spying. Understanding why there is little existing international law on the subject allows us to identify whether recent changes to the landscape should affect states' calculations about whether to try to establish norms in this area.

Spying has proven hard to regulate for at least five reasons. First, the act of spying tends to implicate a state's core national security interests.[78] States are heavily invested in obtaining critical information about other governments while protecting their own secrets against foreign

77. Scott, *supra* note 22 (quoting Antonin Scalia, Assistant Attorney Gen., Office of Legal Counsel, Memorandum for the Attorney General on the Vienna Convention (Dec. 24, 1975)); *see also* Forcese, *supra* note 14, at 197 ("[In 1978,] Congress reportedly expressed unease that electronic surveillance directed at diplomatic premises would violate the Convention. The Administration overcame this concern by supplying a list of states that surveilled U.S. diplomatic premises abroad, suggesting that such a widely accepted practice, while not authorized by the Convention, did not violate it."). Congress in enacting the Foreign Intelligence Surveillance Act also made clear that the Act would trump the VCDR, at least on a domestic level. *See* H.R. REP. NO. 95-1720, pt. I, at 24–25 (1978) (Conf. Rep.), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4053–54.

78. Loch K. Johnson, *Think Again: Spies*, FOREIGN POL'Y (Nov. 19, 2009), http://foreignpolicy.com/2009/11/19/think-again-spies/ ("[S]pies are in some ways the ultimate agents of national interest.").

espionage.[79] Most fundamentally, effective intelligence collection can alert a state that another state is planning to attack it, or is engaged in activities that evidence hostile intent. Given the prevalence of terrorism by non-state actors today, another key function of intelligence collection is to obtain advance notice of planned terrorist attacks originating overseas, whether against a state's embassies or its homeland. Additional uses of intelligence include the ability to detect violations of sanctions regimes and proliferation of weapons of mass destruction. A more pedestrian use of espionage is to obtain information about foreign leaders' intentions, which can allow states to operate more effectively in bilateral and multilateral discussions with other states. States therefore have been loath to reduce their own flexibility to protect themselves by any means that are not obviously unlawful.

Second, espionage by definition is intended to occur without detection. The level of secrecy that attaches to such acts suggests that it would be quite difficult for one state to detect a violation of an agreement that reciprocally limits spying. Where it is very difficult to determine whether a treaty partner is complying with its commitments, a state will be less likely to enter into such commitments in the first place.[80] Surveillance implicates attribution problems as well, as has been well-described in the cyber context.[81] Even if a state is aware that an entity is engaged in surveillance against it, it may be very difficult for that state to determine which state — or private actor — is undertaking that surveillance. This problem is most acute in the collection of cyber and telephony data, and slightly less acute in the drone context, given that drones are visible and audible, are operated by a limited number of states, and may even crash while on missions.[82]

Third, states hold their spying capacities as closely guarded secrets. It is difficult for states seriously to discuss ways to limit spying on other states without revealing certain information about their own capabilities. It also is fraught for a state to discuss its knowledge of other states' spying, since

79. The fact that states tend to punish spies harshly under their domestic laws illustrates how valuable states perceive their own secrets to be and suggests why they view foreign secrets as valuable.

80. Kenneth W. Abbott, *"Trust But Verify": The Production of Information in Arms Control Treaties and Other International Agreements*, 26 CORNELL INT'L L.J. 1, 33 (1993) (noting that most international arms control agreements explicitly authorize the use of monitoring devices to verify compliance); David A. Koplow, *Back to the Future and Up to the Sky: Legal Implications of "Open Skies" Inspection for Arms Control*, 79 CALIF. L. REV. 421, 493 (1991) (stating that most states, when negotiating arms control treaties, insist on tight link between substantive commitments and verification provisions).

81. Glennon, *The Road Ahead*, *supra* note 21, at 380–83 (describing difficulties of attribution in cyber context).

82. Craig Whitlock, *When Drones Fall from the Sky*, WASH. POST, June 20, 2014, http://www.washingtonpost.com/sf/investigative/2014/06/20/when-drones-fall-from-the-sky/.

doing so can reveal the first state's sources and methods of (counter-) surveillance. States are very hesitant to reveal their toolkits publicly, for fear of losing an advantage over other states. As a result, it is unsurprising that bilateral or multilateral discussions about spying historically have been rare (other than among close allies and in secret).

Fourth, different states have very different surveillance capabilities. Some, such as France, the United Kingdom, Russia, China, Israel, and the United States, have extensive abilities to conduct electronic surveillance of other states. Other groups of states have very limited capabilities to do so. Those with limited capacities to surveil and defend against surveillance often will find it to their advantage to promote international rules that would seek to limit surveillance, as they would incur few costs and significant benefits if such a rule existed. Indeed, there has been a groundswell against the activities of the United States, a state with particularly strong surveillance capacities. Those with extensive capacities will tend to be the "spies," and therefore (to date) have had strong interests in resisting excessive regulation of surveillance. Those latter states also tend to have significant political and economic power on the international stage, and therefore generally are in a strong position to control the direction of actions in the United Nations and elsewhere.

Fifth, spying was more costly when it required a greater on-the-ground presence in another state. States by necessity had to direct their focus to the most problematic issues and individuals. Often those issues were state-centric: What type of weapons were our enemies developing? What were their political or military ambitions? Answers to those questions usually lay with the foreign state's officials, not private citizens. "Bulk" human intelligence collection did (and does) not exist, so collecting on private citizens took a back seat. As a result, public pressure to curtail spying previously was minimal, because spying was not seen to affect the average citizen.

If each of these propositions continued to hold true today, we should not expect any changes to international surveillance norms. However, new developments and pressures related to surveillance have undercut or altered the calculations that underlie these propositions.

D. A Shift from Agnosticism

The Snowden revelations affect each of the five reasons that explain why international law has done little to regulate foreign surveillance. First, although states surely continue to view espionage as critical to their core interests, many believe that state surveillance has expanded beyond those central national security interests. An NSA spokeswoman herself stated that the NSA's job is to "identify threats within the large and complex

system of modern global communications."[83] That system is an area in which "ordinary people share fiber-optic cables with legitimate intelligence targets."[84] By virtue of the NSA's techniques of accumulating large amounts of data of "ordinary people," many worry that the NSA has the capacity — if not the will or legal authority — to examine that data for inappropriate purposes. And most of that data — considered piecemeal — implicates no U.S. security interests.[85] For example, a recent leak revealed that the United States is collecting all telephone metadata and call contents in the Bahamas. The reported reason is to focus on "international narcotics traffickers and special-interest alien smugglers."[86] While a potential criminal threat, few would argue that alien smuggling directly implicates a core U.S. national security interest.[87] States therefore now face serious critiques that the type of information they are collecting exceeds what is necessary to protect their true security interests.

Second, there is a new focus on and understanding of the contents of states' domestic surveillance laws, and the way in which those laws regulate foreign surveillance. Concerns about whether one state will comply with arrangements it makes with other states to limit spying will diminish if and as states adopt domestic laws and policies that overtly regulate foreign surveillance. There is good reason to expect that states will comply with their domestic laws. If the laws of those states are in line with the (likely less specific) international norms that develop, it is reasonable to expect those states to act consistent with both bodies of law. Compliance with international norms becomes more likely.

---

83. Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches "Into the Past" to Retrieve, Replay Phone Calls*, WASH. POST, Mar. 18, 2014, http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (internal quotation marks omitted).

84. *Id.*; *see also* James Glanz, *Leaked File Details U.S. Phone Monitoring Abroad*, N.Y. TIMES, Mar. 18, 2014, http://www.nytimes.com/2014/03/19/us/leaked-file-details-us-phone-monitoring-abroad.html?_r=0 (describing NSA public statement noting "the fact that routine communications and communications of national security interest increasingly transit the same networks" (internal quotation marks omitted)).

85. If one believes, as the U.S. government does, that the data collectively supports a security goal because it allows the government to more easily find needles when it has the whole haystack to search through, one will resist the argument that data collected from "ordinary people" does not contribute to national security.

86. Ryan Devereaux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, INTERCEPT (May 19, 2014), https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (internal quotation marks omitted) (describing massive telephonic surveillance program focused on "international narcotics traffickers and special-interest alien smugglers").

87. Another example is Australia's decision to conduct electronic surveillance against Timor-Leste's cabinet as Timor-Leste considered its negotiating strategy on a maritime treaty. Timor-Leste brought a case in the ICJ as a result. *See infra* text accompanying notes 176–77.

Relatedly, as discussed below, states will be faced with new decisions by human rights courts and treaty bodies that seek to extend the right to privacy extraterritorially. The jurisprudential trends are such that it seems likely one or more of these entities will conclude, when faced with a case involving extraterritorial surveillance, that the surveilling state has the capacity to violate a foreign national's privacy rights overseas. As Beth Van Schaack argues, "[A] longitudinal review of the cases reveals a distinct trend toward an understanding that States' human rights obligations follow their agents and instrumentalities offshore whenever they are in a position to respect — or to violate — the rights of individuals they confront abroad."[88] If that trend continues, these bodies will conclude that the surveilling state has an obligation to respect the right to privacy extraterritorially.[89] These bodies might also conclude that mass surveillance, as distinct from targeted surveillance, violates ICCPR Article 17 because it is "arbitrary," unless a state can show probable cause or a threat of imminent harm. Some of these decisions will bind the defendant states and force them to alter their domestic laws. Others will simply be hortatory. But history illustrates that even hortatory statements by these bodies ultimately impact the way states view their international and domestic obligations.

Third, although states still desire to maintain secrecy about their surveillance capacities, the recent revelations about collection by NSA, GCHQ, and the Australian Signals Directorate, among other intelligence services, have rendered less salient that desire, at least within those states whose capabilities are now known.[90] These capabilities include the ability to access the emails and phone records of various foreign leaders;[91] to record all phone calls that occurred within a particular foreign state and replay those calls up to thirty days after they occur;[92] to engage in an "upstream" collection of communications passing through fiber optic

88. Van Schaack, *supra* note 45, at 32.

89. *Id.* at 31–52 (describing evolving jurisprudence in human rights bodies and courts toward extension of ICCPR and ECHR extraterritorially). States might respond to a shift toward increasingly extraterritorial application of these treaties by seeking to diminish the substantive scope of the right to privacy, though tribunals do not seem to be willing to apply different versions of a right depending on where the right arises.

90. Robert Litt, Gen. Counsel, Office of Dir. of Nat'l Intelligence, Remarks at American University Washington College of Law Freedom of Information Day Celebration (Mar. 17, 2014) (transcript available at IC ON THE RECORD, http://icontherecord.tumblr.com/post/79998577649/as-prepared-for-delivery-remarks-of-odni-general) ("Going forward, I believe that the Intelligence Community is going to need to be much more forward-leaning in what we tell the American people about what we do.").

91. Glüsing et al., *supra* note 75 (Calderon and Rousseff); *Embassy Espionage*, *supra* note 27 (Merkel).

92. Gellman & Soltani, *supra* note 83.

cables that are en route to but have not yet arrived at U.S. and European servers;[93] and to acquire the content of electronic communications from U.S. Internet service providers (ISPs).[94] As Admiral Michael Rogers, NSA Director and Commander of U.S. Cyber Command, submitted to Congress during his confirmation proceedings, "[T]he recent disclosures of a large portion of our intelligence and military operational history may provide us with opportunity to engage both the American public and our international partners in discussion of the . . . norms of accepted and unacceptable behavior in cyberspace."[95] States may behave opportunistically and instrumentally, deciding that they now have less to lose in public discussions about foreign surveillance, and thus are in a better position than their more secretive peers to shape emerging norms.

Fourth, while states clearly still possess disparate surveillance capacities — something that has become even more apparent in the wake of the Snowden leaks — the traditional incentive structure has flipped for certain states. In past periods, those states with the most extensive surveillance techniques were the states least inclined to establish international norms. Now, those (Western) states with the most advanced techniques — and even some Western democracies with only mid-range capabilities — are the ones whose capabilities have come to light and who now — partly because they face the greatest political pressure — have the strongest incentives to establish norms that strike a new balance between privacy and national security.

Fifth, unlike traditional human intelligence collection, bulk electronic surveillance collection is relatively cheap in relation to the volume of information gleaned, and can penetrate many arenas.[96] As a recent report

---

93. Craig Timberg, *NSA Slide Shows Surveillance of Undersea Cables*, WASH. POST, July 10, 2013, http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (describing "upstream" collection); Ewen MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, GUARDIAN, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (describing GCHQ's Tempora program, a large-scale Internet collection program that reportedly captures large amounts of Internet traffic flowing from Europe to the United States, draws data from about 1,500 fiber optic cables, and stores it for up to thirty days).

94. Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

95. S. COMM. ON ARMED SERVS., 113TH CONG., ADVANCE QUESTIONS FOR VICE ADMIRAL MICHAEL S. ROGERS, USN: NOMINEE FOR COMMANDER, UNITED STATES CYBER COMMAND, *available at* http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf (last visited May 19, 2015).

96. Johnson, *supra* note 78 ("Even during the Cold War, major powers resorted to surveillance

put it, "The explosion of digital communications content[,] . . . the falling cost of storing and mining large sets of data, and the provision of personal content through third party service providers make Communications Surveillance by States possible at an unprecedented scale."[97] This type of surveillance implicates the communications of average citizens, not just a narrow range of critical targets.[98] This has produced a public outcry about surveillance previously unseen in the espionage context.[99] Sustained public pressure on governments from citizens and corporations from multiple countries provides an impetus for change on both the domestic and international fronts, even as states continue to value "big data" both for its intelligence values and for other opportunities it offers to improve lives.[100] States also may realize that widespread surveillance, and the suspicions engendered therefrom, may cause the Internet to fragment in ways that will disadvantage their economies.[101]

The Snowden revelations illustrate why the reasons for a *laissez-faire* approach to foreign surveillance are weakening. Not only are the reasons not to regulate becoming less persuasive, however; the reasons affirmatively to regulate foreign surveillance have strengthened. The next Part argues that we are at an important crossroads, one in which international norms should play a key role.

II. FOREIGN SURVEILLANCE'S INTERNATIONAL MOMENT?

A. Theories of International Law Creation

In light of the looming shift away from international agnosticism about foreign surveillance, how should we think about the relationship between changing (international and domestic) political landscapes and the power and purposes of international law? One rich source of analysis is

technology that now seems like something out of a Laurel and Hardy movie.").

97. NECESSARY & PROPORTIONATE, *Principles*, *supra* note 3.

98. *See* SELECT COMMITTEE ON THE CONSTITUTION, SURVEILLANCE: CITIZENS AND THE STATE, 2008-9, H.L. 18-II, at 172 ¶ 5 (U.K.) (Memorandum by Prof. dr. Bert-Jaap Koops, Professor of Regulation & Tech., Tilberg Inst. for Law, Tech., & Soc'y) ("[T]he 'footprint' of criminal law and intelligence is slowly widening to cover more circles of society.").

99. For the broader idea that traditional international law operated at a step removed from private individuals, see Paul B. Stephan, *The New International Law — Legitimacy, Accountability, Authority, and Freedom in the New Global Order*, 70 U. COLO. L. REV. 1555, 1563 (1999).

100. *See* John Podesta, Findings of the Big Data and Privacy Working Group Review, WHITE HOUSE BLOG (May 1, 2014, 1:15 PM), http://www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review.

101. Gordon M. Goldstein, *The End of the Internet?*, ATLANTIC, July–Aug. 2014, http://www.theatlantic.com/magazine/archive/2014/07/the-end-of-the-internet/372301/.

international relations (IR) theory. Many international legal scholars have drawn from IR theory in an effort to provide plausible, coherent accounts — including predictive accounts — of how and why states employ international law. Although the international law literature in this vein has not developed a satisfying theory of the precise conditions under which states specifically decide to turn to international law to address discrete problems, the literature usefully addresses conditions of international law-making generally.[102]

1. Four Theories

There are several main schools of thought in international relations, each of which makes different underlying assumptions about the nature of states, how states interact with each other, and the relevance (or not) of domestic political structures.[103] Each school is by necessity somewhat of a caricature; various scholars relax certain assumptions at the margins, and some blend different schools to develop what they view as more realistic theories of how states act.[104] For ease of description, I group each school under a single heading, recognizing that different scholars within each school are likely to diverge on particular aspects of the theories and that in some cases different schools of thought may produce complementary, rather than competitive, insights about state uses of international law.

Realism assumes that states are the primary actors in the international system, that the (dis)organizing principle of state relations is anarchy, that each state has fixed, identifiable interests, and that a state's dominant preference is to ensure its own survival, which it does by maximizing its power.[105] Realists tend to assume that international law reflects the

102. One reason for a lack of theories predicting specific factors that motivate states to turn to international law at time X or Y may be the fact that these decisions are contingent on so many factors. *See* LOUIS HENKIN, HOW NATIONS BEHAVE: LAW AND FOREIGN POLICY 36–37 (1979) ("A government's policy as to whether some activity of international interest should remain unregulated, or what form regulation should take, is a political decision like others made by policy-makers in the light of national interest as they see it. But national interest is not a single or simple thing; and often various national interests are implicated, and policy-makers must attempt to balance, compromise, or choose among them. . . . For the United States, for example, a single issue may involve competing political, military, economic, and other public interests, as well as the interests of particular citizens or national companies.").

103. Stephen M. Walt, *International Relations: One World, Many Theories*, FOREIGN POL'Y, Spring 1998, at 29, 38; Anne-Marie Slaughter, *Liberal International Relations Theory and International Economic Law*, 10 AM. U. J. INT'L L. & POL'Y 717, 719 (1995) (summarizing realism, institutionalism, and liberalism).

104. *See, e.g.*, Kenneth W. Abbott, *Toward a Richer Institutionalism for International Law and Policy*, 1 J. INT'L L. & INT'L REL. 9, 28 (2005) (arguing for blend of institutionalism, liberalism, and constructivism); Oona A. Hathaway, *Between Power and Principle: An Integrated Theory of International Law*, 72 U. CHI. L. REV. 469 (2005).

105. Richard H. Steinberg, *Wanted — Dead or Alive: Realism in International Law*, *in*

interests of powerful states, which bring their will to bear in shaping those rules. Further, realists concede that international law may make states better off than they would be in the absence of those agreed rules.[106] Finally, realists believe that if a provision of international law runs contrary to a state's interests, that state will ignore the law.[107]

Like realism, institutionalism assumes that states are the primary actors in the international arena, but institutionalists tend to be more optimistic than realists about the ability of norms and principles (including international institutions) to mitigate the effects of anarchy and allow states to cooperate in pursuit of certain common ends.[108] As Robert Keohane famously argued, international regimes reduce transaction costs and therefore promote cooperation, including by improving informational exchanges among states, even in the absence of a hegemon that dominates the international arena and sets and enforces the system's rules.[109] These regimes establish standards of behavior for states to follow.[110] In the international law context, Kenneth Abbott notes that "institutionalism would seem to provide a natural framework for lawyers and other policy makers seeking innovative responses to global problems. After all, the whole panoply of cooperative arrangements . . . are in social science terms all 'institutions.'"[111] Like realists, institutionalists believe that states only comply with international law when it is in their interests to do so. However, institutionalists generally predict that institutions can be effective at changing state incentives, especially powerful states' incentives, in a wider range of circumstances than realists would.

Liberalism alters the realist and institutionalist assumptions about the nature of states. This school assumes that state interests are not fixed and dictated by a monolithic actor, but instead that those interests are established by individuals and groups within the state.[112] The resulting

---

INTERDISCIPLINARY PERSPECTIVES ON INTERNATIONAL LAW AND INTERNATIONAL RELATIONS 146, 149–50 (Jeffrey L. Dunoff & Mark A. Pollack eds., 2013) [hereinafter INTERDISCIPLINARY PERSPECTIVES]; JOHN J. MEARSHEIMER, THE TRAGEDY OF GREAT POWER POLITICS 2–3 (2001) (describing "offensive realism").

106. Steinberg, *supra* note 105, at 150. Thucydides, for example, explains that treaties of alliances can advance the strategic interests of the parties by making them more secure than they would be in the absence of those alliances. *Id.* at 151.

107. *Id.* at 150; Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1793 (2009).

108. Abbott, *supra* note 104, at 16; Barbara Koremenos, *Institutionalism and International Law*, *in* INTERDISCIPLINARY PERSPECTIVES, *supra* note 105, at 59, 60.

109. ROBERT O. KEOHANE, AFTER HEGEMONY: COOPERATION AND DISCORD IN THE WORLD POLITICAL ECONOMY 244 (1984); *see also* Koremenos, *supra* note 108, at 59–60 (noting Keohane's contribution).

110. KEOHANE, *supra* note 109, at 244–45.

111. Abbott, *supra* note 104, at 26 (footnotes omitted).

112. Slaughter, *supra* note 103, at 728.

preferences reflect the privileging of some domestic voices over others.[113] Liberalism also assumes that those players operate not only within their own domestic systems but also engage in transnational exchanges with international institutions, non-governmental organizations, or other foreign actors.[114] Further, many who adopt liberalism's core assumptions believe that democratic states are more likely to accept the legal regulation of international politics and to comply with international law once it is created.[115] Adherents to this school generally believe that a state assumes international legal obligations when relevant players within that state determine that it is in their interests to do so.[116]

Finally, constructivism views a state's interests and values as socially constructed, not fixed *ex ante*.[117] States develop norms in the context of their mutual interactions, internalize them, and then comply with them because they understand them to be correct or appropriate.[118] Constructivists believe that states "often respond to situations based on their perceptions of social expectations, their identities, internalized values, and similar subjective considerations."[119] International law thus provides a focal point around which states may develop, change, and memorialize their preferences through interactions with, deliberations among, and persuasion by other states.[120] Relatedly, although not strictly an IR theory, an "expressive" theory of law "examines law's potential for changing the social meaning of particular behavior by altering the social cost of undertaking that behavior."[121] That is, law may change an individual's behavior, regardless of the likelihood of punishment or sanction, by

113. Andrew Moravcsik, *Liberal Theories of International Law*, *in* INTERDISCIPLINARY PERSPECTIVES, *supra* note 105, at 83, 85 [hereinafter Moravcsik, *Liberal Theories*]; Andrew Moravcsik, *Taking Preferences Seriously: A Liberal Theory of International Politics*, 51 INT'L ORG. 513, 517 (2007).

114. Moravcsik, *Liberal Theories*, *supra* note 113, at 83.

115. Anne-Marie Slaughter, *International Law in a World of Liberal States*, 6 EUR. J. INT'L L. 503, 532 (1995).

116. Abbott, *supra* note 104, at 17–18.

117. ALEXANDER WENDT, SOCIAL THEORY OF INTERNATIONAL POLITICS 20 (1999) ("[T]he character of international life is determined by the beliefs and expectations that states have about each other, and these are constituted largely by social rather than material structures."); Abbott, *supra* note 104, at 14.

118. Hathaway, *supra* note 104, at 481; Jutta Brunnée & Stephen J. Toope, *International Law and Constructivism: Elements of an Interactional Theory of International Law*, 39 COLUM. J. TRANSNAT'L L. 19, 66 (2000) (arguing that legal "[l]egitimacy is rooted in . . . acceptance of the need for emerging norms, an acceptance promoted by reference to past practice [and] contemporary aspirations").

119. Kenneth W. Abbott, *Enriching Rational Choice Institutionalism for the Study of International Law*, 2008 U. ILL. L. REV. 5, 13.

120. *See* Gregory C. Schaffer & Mark A. Pollack, *Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance*, 94 MINN. L. REV. 706, 790 (2010) (noting constructivist view that law can provide focal point that creates normative pull).

121. Alex Geisinger & Michael Ashley Stein, *A Theory of Expressive International Law*, 60 VAND. L. REV. 77, 83 (2007).

providing important information about what behavior a society regards as acceptable. Richard McAdams terms this the "attitudinal theory" of expressive law, arguing that law can change individual behavior by signaling the underlying attitudes of a community or society.[122] If an individual seeks approval within his community, he will seek to comport with behaviors deemed acceptable by that set of actors.

Although states clearly act differently from individuals, states are concerned about their reputations in the international community.[123] Even powerful states "seek legitimacy and acceptance for their policies."[124] Adopting international norms does two things at once. First, the fact of norm adoption, coupled with the content of those norms, allows states to send an important message to interested observers about what behaviors those states now deem appropriate.[125] Second, norm adoption increases the social cost of undertaking behavior that is inconsistent with those new norms.

2. Application to Surveillance

Regardless of the underlying assumptions one makes about state behavior, it is possible to identify important reasons why states today would want to regulate foreign surveillance. Details about the pressures that states are facing to regulate foreign surveillance are set out in the next Subpart. However, I consider here in broad terms why, regardless of the IR perspective(s) one adopts or of one's view about what motivates states to act on the international plane, one should conclude that international regulation is likely to happen as a positive matter, or at least that states should consider regulation as a normative matter.

Those who hold traditional realist assumptions about state behavior are the least likely to believe that states would turn to international law to regulate surveillance, largely because surveillance tends to amplify the raw power of states to survive and — depending on how sophisticated their surveillance techniques are — to accrue power through political and military advantage. Yet even realists may acknowledge that each state would prefer a world in which its officials and citizens were less often

---

122. Richard H. McAdams, *An Attitudinal Theory of Expressive Law*, 79 OR. L. REV. 339, 340 (2000).

123. Andrew T. Guzman, *A Compliance-Based Theory of International Law*, 90 CALIF. L. REV. 1823, 1825 (2002).

124. HENKIN, *supra* note 102, at 31; RYAN GOODMAN & DEREK JINKS, SOCIALIZING STATES: PROMOTING HUMAN RIGHTS THROUGH INTERNATIONAL LAW (2013) (arguing that states (through their officials) adopt the norms of others in their environment and seek to maximize their status and prestige).

125. *See* Hathaway, *supra* note 104, at 492–93 (arguing that state decisions about whether to join treaties are influenced by anticipated reactions of domestic and foreign constituencies).

subject to foreign surveillance. Any one state is unlikely to take unilateral steps to decrease such surveillance, however. To achieve reduced surveillance, states would have to establish agreed cooperative behavior among like-minded states that share a high level of trust.[126] Even here, realists will be skeptical about compliance with those norms because it will be difficult to show that each state is complying with the agreed cooperative behavior. In other words, payoffs from defection may be relatively high because it will be hard to detect that a state has defected.

Nevertheless, realism assumes that states are instrumentally rational.[127] Some states, concerned that U.S. and U.K. foreign surveillance may violate international law, may feel obligated (or be ordered by their courts) to limit their current intelligence-sharing relationship with those states. To the extent that a lack of agreed surveillance norms reduces intelligence cooperation, this diminishes the power of states that otherwise would share intelligence. Adopting agreed surveillance norms could facilitate intelligence-sharing among norm-adhering states, allowing them to better protect themselves against threats by unfriendly states. Nor would the norms proposed in Part III eliminate states' ability to collect intelligence about the intentions of other states. Instead, adopting such norms could give Western states both reputational and efficiency advantages over states such as Russia and China. And to the extent that realists view international law as a mirror of power relations among states, states such as the United States, United Kingdom, Germany, and several other European states remain powerful at this moment in time.[128] Realists thus might expect a shift in the international legal regime to reflect the interests of those states.[129]

Those who take a traditional institutionalist perspective recognize the absolute advantages in creating regimes to diminish conflict and improve cooperation among states. As discussed in greater detail in the next

126. Jack L. Goldsmith & Eric A. Posner, *A Theory of Customary International Law*, 66 U. CHI. L. REV. 1113, 1171 (1999) (noting that treaties can record the actions that will count as cooperative moves in an ongoing repeat prisoner's dilemma or the actions that achieve the highest joint payoff in a coordination game).

127. John J. Mearsheimer, *The False Promise of International Institutions*, 19 INT'L SECURITY 5, 10 (1994–95).

128. Oona A. Hathaway & Ariel N. Lavinbuk, *Rationalism and Revisionism in International Law*, 119 HARV. L. REV. 1404, 1431 (2006) (reviewing JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW (2005)) ("[S]tandards of coordination will benefit stronger parties . . . .").

129. I assume here that the interests of this latter cluster of states are relatively homogenous. As discussed in Part II.B. *infra*, the United States and United Kingdom have particular interests in seeking international regulation to relieve the public pressures they face, but states such as Germany face a combination of public pressure to regulate their own spying and an interest in reducing the amount of spying their officials and nationals face from other states. Thus, the quantity of their interests is comparable, even if the quality of interests diverges somewhat.

Subpart, reports that states have been spying on each other's leadership disrupted existing relationships among friendly states (at the same time that they exacerbated already tense relationships between states such as the United States and China). The disclosures also potentially complicated intelligence cooperation. One intelligence partner could decide internally that it would violate its own domestic law to provide or receive certain types of intelligence from a surveilling state partner.[130] For example, if Denmark concluded that it could not accept certain types of intelligence information from the United Kingdom because it believed the United Kingdom had collected that intelligence in a manner that violated the ICCPR, that directly affects the U.K.-Danish intelligence sharing relationship. Bringing allies' interpretations of shared international obligations into harmony — as international norm development would do — promotes sustainable intelligence cooperation and broader data sharing.[131] In short, clear and objective surveillance norms that restrict current foreign surveillance practices can improve inter-state relationships, increase the information that adhering states have about each other's surveillance activities, produce structures that will suppress the instabilities fostered by the Snowden revelations, and embed the restraint in mechanisms that will be sticky because they are multilateral.[132]

Liberalists would express no surprise that corporations and foreign and domestic elites are serving as a key source of pressure to develop foreign surveillance norms. Those groups are helping to shape the preferences of Western states that, to date, have not been interested in regulating foreign

130. *But see* Posner, *supra* note 7 (noting that most countries cannot afford to cease intelligence cooperation with the United States because they rely on the robust U.S. surveillance capabilities).

131. For arguments that U.S. surveillance should reduce U.S.-European data sharing, see European Parliament Resolution of 12 March 2014 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, EUR. PARL. DOC. (2013/2188(INI)) ¶¶ AK, AQ (2014) [hereinafter European Parliament Resolution], *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139 (stating that the U.S. government's surveillance "has seriously eroded transatlantic trust" and calling for the European Commission to suspend data flows to certain U.S. organizations).

132. THOMAS M. FRANCK, FAIRNESS IN INTERNATIONAL LAW AND INSTITUTIONS 30 (1995) (discussing how clear, objective norms are more legitimate). Rational design, a subcategory of institutionalism, asks what *kinds* of institutionalized cooperation will emerge. One underlying "cooperation problem" that foreign surveillance leaks have revealed is that states' nationals are subject to (in their view) excessive surveillance by foreign governments. Rational design might predict that the underlying regime that states should develop in response will include certain flexibility mechanisms in light of uncertainty about the future state of the world, and some form of enforcement (e.g., cancellation of commitment) because of underlying incentives to defect. *See* Koremenos, *supra* note 108, at 62. The norms proposed in Part III could include, explicitly or implicitly, a cancellation of commitment, and their procedural nature leaves room for state flexibility in assessing the substantive propriety of carveouts to the right of privacy.

surveillance. Until recently, the conduct of foreign surveillance was relatively insulated from domestic politics, which blunted domestic influence over those surveillance policies. Now, however, the role of individuals in influencing state interests has become increasingly strong, because individuals feel directly affected by unfettered foreign surveillance. States therefore may decide that it is in their interests to adopt new norms to satisfy their domestic constituencies.[133] In a multilateral arrangement to limit certain types of foreign surveillance, each state will commit to reducing the number of situations in which it will spy on foreign citizens. Their own citizens accordingly will benefit from fewer intrusions on their privacy by other states. Corporations are another important constituency here, particularly in the United States.[134] If the United States were to adhere to a set of foreign surveillance norms accepted by several peer states, U.S. corporations should face reduced skepticism by foreign customers that they are complicit in unregulated surveillance activities.

Liberalism also anticipates that democracies will act differently from non-democracies, because of the way in which constituencies in a democracy are able to make their voices heard. It seems likely, based on the disparate incentives discussed below in Part II.C., that Western democracies will respond differently to pressures to rein in foreign surveillance than will non-democracies. Indeed, this Article argues that a likely outcome is an agreement among like-minded democracies on foreign surveillance norms, with other states joining on an *ad hoc*, trust-driven basis. Thus, liberalist assumptions might lead one to conclude that states both will (because they have come under pressure from various domestic constituencies to do so) and should (because many different constituencies agree on the need for some regulation) adopt new international surveillance norms.

Finally, if one starts from the premise (as many constructivists do) that state interests change in response to interactions with other states, one would recognize that state interests currently are evolving as states reconsider what types of foreign surveillance are appropriate. The Snowden revelations initiated a large number of inter-state interactions and critical public statements about the legality and propriety of surveillance of foreign leaders and citizens. These exchanges may have both triggered and reflected a shift in preferences, as states gain a new understanding of the types of surveillance that are technologically possible and develop a sense that some of these activities run contrary to legal or

133. Hathaway, *supra* note 104, at 492–93.

134. Melissa J. Durkee, *Persuasion Treaties*, 99 VA. L. REV. 63, 89 (2013) ("To the extent that corporations are powerful domestic constituencies, they can dominate state preferences, and shape the bargains states are prepared to make.").

moral constructs that — to this point — had been relatively inchoate. If Western democracies are particularly sensitive to changing public opinion, then constructivists might predict that the preferences of those states are more malleable and that those states may serve as "thought leaders" in developing international norms that reflect — and guide — the changing preferences. At the same time, adopting new international norms that strike a careful balance between liberty and security may signal states' continued commitment to their national security (a potent interest of at least some domestic groups within states), and indicate to groups acting within UN fora and to courts hearing foreign surveillance cases that states will resist a wholesale reworking of their preferences.

In the context of an expressive theory of law, adopting restrictions on foreign surveillance would contain both general and specific signals. The general signal would be a willingness to self-bind; the current perceived lack of state restraint drives much of the criticism of foreign surveillance. The specific signals depend on the content of the norms, but states should consider establishing rules that signal a willingness to limit the discretion of public officials,[135] make the rules themselves clearer and more transparent,[136] and establish accountability for the collection and use of data collected from surveillance. Finally, those who believe in law's expressive function would view the reputations of the states that adopt the norms as important. States will want to be in "good company": If the states that agree to new norms tend to adhere to their domestic and international obligations, the normative commitments will seem more serious and the expectation of compliance will be higher. This would be consistent with an approach that anticipates the adherence to new surveillance norms by a group of like-minded democracies that generally are committed to compliance with their international obligations.

B. Pressures to Create Foreign Surveillance Norms

This Subpart analyzes specific developments that render this a moment at which states should — and likely will — turn to international law. There are three overarching reasons why conditions are changing. First, we see a personalized and widespread understanding of the way in which foreign government surveillance affects individuals on an intimate level. The Snowden leaks gave a face to what people often treat as a theoretical

135. A.V. DICEY, INTRODUCTION TO THE STUDY OF THE LAW OF THE CONSTITUTION 183–205 (10th ed. 1959) (discussing importance of narrowing official discretion); David H. Moore, *A Signaling Theory of Human Rights Compliance*, 97 NW. U. L. REV. 879, 884 (2003) (arguing that sending signal of human rights compliance "demonstrates that a nation is able and willing to restrain the reach and exercise of its power").

136. THOMAS M. FRANCK, THE POWER OF LEGITIMACY AMONG NATIONS 64 (1990).

concept — privacy — and find easy to take for granted or ignore in their daily lives.[137] The fact that large numbers of people feel the impact of foreign surveillance is uncommon: Most events that happen on the international political stage are either of little interest to the average citizen or, if of intellectual interest, do not impact their lives directly. Second, there is an unusual alignment of interests among corporations, elite opinion, and "ordinary citizens" pointing in a pro-regulation direction. Contrast this to what may be the closest comparable geopolitical situation — climate change. There, some states, elite opinion, and ordinary citizens would like to see greater advances in international cooperation to reduce greenhouse gas emissions, but many corporations are concerned about such regulations.[138] Third, the governments most impacted by the Snowden revelations are Western democracies, which are sensitive to public — including international public — pressure.

This Subpart analyzes several categories of pressures states face to regulate their foreign electronic surveillance activities, most of which are second-order effects of the Snowden leaks. These pressures are political, human rights-based, and economic. The political pressures were immediate and sharp, but may fade over time. The human rights pressures will mount more gradually but will sustain themselves for years. The economic pressures seem likely to grow over time as the blow-back effects of state surveillance continue to unfold.

1. Political Pressures

The first pressures to emerge from the Snowden leaks were political. The revelations illuminated the fact that the United States spies on the communications of foreign leaders, including its allies. Perhaps more strikingly, the leaks contained information about NSA programs that collected massive amounts of communications information from average citizens, both American and foreign. These disclosures produced significant pressure on the U.S. government (and, to a lesser extent, the U.K. and Australian governments, which have cooperated with the United States) to rein in their activities.

---

137. *Cf.* M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29 (2011), http://www.stanfordlawreview.org/online/drone-privacy-catalyst.

138. *See, e.g.*, David L. Levy, U.S. Business Strategies and Climate Change 2–3 (May 19, 2006) (unpublished manuscript), *available at* http://www.wilsoncenter.org/sites/default/files/paperlevy.pdf (describing early corporate resistance to climate change regulation). One interesting question is whether, if severe climate events become increasingly frequent and dramatic around the globe, climate change issues become more "personalized," alter the calculations of corporations, and prompt a more forceful turn to international regulation.

For a state looking to gather intelligence about political, economic, and military developments in a foreign country, the obvious place to turn is to the communications of that country's leadership. After all, a country's most significant decisions are taken by those running its government. Obtaining access to the thinking and planning of foreign leaders is especially important where those states are hostile or are highly closed societies in which the media cannot operate to reveal political, economic, or military developments. There may be far fewer circumstances in which it is important or appropriate to surveil the communications of the leadership of friendly, democratic countries — a fact that became apparent in the wake of leaks that the United States was engaged in such activity.

The disclosure that the NSA accessed the contents of emails and phone conversations of various foreign leaders prompted an immediate and sharp outcry by some of those leaders, who view themselves as U.S. allies. These include Mexican President Felipe Calderon and his cabinet members; Brazilian President Dilma Rousseff and her key advisers; and German Chancellor Angela Merkel.[139] The United States is not alone, however, in using electronic surveillance this way. The United Kingdom's GCHQ reportedly collected phone calls of German officials and the EU Commissioner, emails of the Israeli Prime Minister and Defense Minister, and the substance of text messages from an African politician.[140] Brazil admitted to spying on diplomats from the United States, Russia, and Iran.[141] Australia attempted to surveil the phone calls of the President and Vice President of Indonesia.[142] In short, many states try to access the communications of other states' leaders.[143] It is safe to assume that states know that their leadership may be subject to actual or attempted surveillance, given the steps that states take to keep their leaders' communications secure.[144]

---

139. Glüsing et al., *supra* note 75 (Calderon and Rousseff); *Embassy Espionage*, *supra* note 27 (Merkel).

140. Laura Poitras et al., *Friendly Fire: How GCHQ Monitors Germany, Israel and the EU*, DER SPIEGEL, Dec. 20, 2013, http://www.spiegel.de/international/world/snowden-documents-show-gchq-targeted-european-and-german-politicians-a-940135.html.

141. Amar Toor, *Brazil Admits to Spying on US Diplomats After Blasting NSA Surveillance*, VERGE (Nov. 5, 2013, 5:33 AM), http://www.theverge.com/2013/11/5/5068024/brazil-admits-to-spying-on-us-russia-iran-diplomatic-targets-after-nsa-criticism.

142. Ewen MacAskill & Lenore Taylor, *Australia's Spy Agencies Targeted Indonesian President's Mobile Phone*, GUARDIAN, Nov. 17, 2013, http://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone.

143. Obama NSA Speech, *supra* note 1 ("There is a reason why BlackBerrys and iPhones are not allowed in the White House Situation Room. We know that the intelligence services of other countries — including some who feign surprise over the Snowden disclosures — are constantly probing our government and private sector networks, and accelerating programs to listen to our conversations, and intercept our emails, and compromise our systems.").

144. Charles Arthur, *Which Phones Do World Leaders Use?*, GUARDIAN, Mar. 28, 2014,

Even though states assume that other states are spying on their leadership, the NSA-related revelations produced significant political pressure on the United States — at least in the short term. German Chancellor Merkel placed an angry call to President Obama, chastising him for allowing the United States to listen to her phone calls.[145] Brazilian President Rousseff cancelled her state visit to the United States, a rare diplomatic move fashioned to send a clear signal of Brazil's displeasure. Even certain U.S. senators criticized the Administration for conducting such surveillance.

Although it remains unclear whether these revelations will incur any long-term damage to relationships between the United States and affected countries, the political pressure resulted in U.S. policy changes. In a speech in January 2014, President Obama announced, "[U]nless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies."[146] He did not define what constitutes a "compelling national security purpose" or which states count as "close friends and allies." Nevertheless, the announcement (which accompanied the release of Presidential Policy Directive 28) suggests that the United States will limit its existing surveillance of certain states' leadership and will engage in more careful consideration before initiating collection on the leadership of a significant number of states.[147] Other states may choose to follow suit.

Even more surprising than revelations about spying on foreign leaders were the disclosures about the U.S. Government's ability to collect both metadata of the calls and emails of foreign citizens and the substantive content of those phone calls (at least in certain countries). At least four types of collection implicate foreigners' data.

First, news reports suggest that since 2009, the U.S. Government has had the capacity to record all of the phone calls that occurred within a particular foreign state and replay those calls up to thirty days after they occur.[148] The U.S. Government reportedly sends millions of voice

---

http://www.theguardian.com/technology/2014/mar/28/which-phones-world-leaders-use (noting that for state affairs, German Chancellor Merkel uses a BlackBerry Z10 fitted with an encryption chip and that Russian President Vladimir Putin uses neither cell phone nor email).

145. Moulson & Dahlburg, *supra* note 28 (Merkel call).

146. Obama NSA Speech, *supra* note 1.

147. Office of the Press Sec'y, *Presidential Policy Directive -- Signals Intelligence Activities*, § 3, WHITE HOUSE (Jan. 17, 2014) [hereinafter *PPD-28*], *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (stating that it is "essential that national security policymakers consider carefully the value of signals intelligence activities in light of the risks entailed in conducting these activities").

148. Gellman & Soltani, *supra* note 83.

clippings from those calls for analysis and storage.[149] Second, news reports revealed that the United States engages in an "upstream" collection of communications passing through fiber optic cables en route to U.S. servers.[150] Because the United States has such a robust Internet and telephonic infrastructure, foreign calls and emails intended for foreign recipients often travel through U.S. servers and hubs because that offers the fastest route for a given data packet at a given time.[151] Third, the United States, in a program called PRISM, obtains the content of electronic communications from U.S. ISPs.[152] The targets of this program are non-U.S. persons outside the United States. Fourth, the United States, using Section 215 of the PATRIOT Act, obtained from various phone companies access to all of their bulk telephone metadata, which the government may query when it has a reasonable articulable suspicion that a phone number is associated with one of several specified foreign terrorist organizations.[153]

Although revelations about the NSA have dominated the headlines, the United States is hardly the only state to engage in clandestine data collection (often in bulk) on foreign citizens. The United Kingdom, for example, conducts a large-scale Internet collection program called Tempora, which reportedly draws data from about 200 fiber optic cables carrying Internet traffic between the United States and Europe and stores it for up to 30 days.[154] Vodaphone, the world's second-largest telecom

149. *Id.* News reports later identified this country as the Bahamas. Devereaux, Greenwald & Poitras, *supra* note 86.

150. Timberg, *supra* note 93 (describing "upstream collection").

151. PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 133 (2013), *available at* https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("By the early twenty-first century, a large percentage of the world's electronic communications passed through the United States . . . ."); Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, at 10 (Lawfare, 1 Research Paper Series No. 3, 2013), http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf (describing upstream collection); NAT'L SEC. AGENCY, THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT AND PARTNERSHIPS 4 (2013), *available at* http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf (noting that "[t]he United States is a principal hub in the world's telecommunications system").

152. Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST WONKBLOG (June 12, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

153. Bradbury, *supra* note 151, at 2–3. President Obama since has announced changes to this program, and as this Article was going to press, Congress enacted the USA FREEDOM Act, which amended Section 215. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

154. MacAskill et al., *supra* note 93; *see also* Nick Hopkins, *Justify GCHQ Mass Surveillance, European Court Tells Ministers*, GUARDIAN, Jan. 23, 2014, http://www.theguardian.com/uk-news/2014/jan/24/justify-gchq-mass-surveillance-european-court-human-rights.

carrier, recently reported that certain countries have direct access to its networks (including the ability to listen in on phone calls) without having to obtain warrants.[155] European states have supplied to the United States — under longstanding intelligence-sharing arrangements — millions of phone records they collected in war zones and other areas outside those countries' borders.[156] Germany's foreign intelligence agency monitors communications from a hub in Germany that handles international traffic to, from, and through Germany.[157] Sweden's signals intelligence agency retains metadata in bulk when the communications cross Swedish borders.[158] France reportedly sweeps up virtually all data transmissions (including phone calls and emails) that enter and leave France.[159] In short, many Western states are now known to be engaged in extensive foreign surveillance. The quantity of political pressure — from other states and the European Parliament,[160] among other actors — could be exacerbated by further revelations or may dissipate over time (particularly in bilateral relationships) as other political priorities take center stage.

In addition to direct public criticism of surveilling states, these disclosures have produced other sources of political pressure on the *status quo*. These pressures occur because some states work cooperatively with other states to collect and share intelligence and want to ensure that these relationships continue. These pressures take several different forms, including (i) pressure to enter into "no spy" agreements by which states undertake not to conduct surveillance on each other;[161] (ii) the erection or

155. Mark Scott, *Vodaphone Reveals Direct Access by Governments to Customer Data*, N.Y. TIMES BITS BLOG (June 6, 2014, 8:09 AM), http://bits.blogs.nytimes.com/2014/06/06/vodafone-reveals-direct-access-by-governments-to-customer-data/.

156. Adam Entous & Siobhan Gorman, *Europeans Shared Spy Data with U.S.*, WALL ST. J., Oct. 29, 2013, http://online.wsj.com/news/articles/SB10001424052702304200804579165653105860502.

157. IRA RUBINSTEIN, GREG NOJEIM & RONALD LEE, CTR. FOR DEMOCRACY & TECH., SYSTEMATIC GOVERNMENT ACCESS TO PERSONAL DATA: A COMPARATIVE ANALYSIS 14 (2013) [hereinafter CDT REPORT], *available at* https://cdt.org/files/2014/11/government-access-to-data-comparative-analysis.pdf.

158. Benjamin Wittes, *Mark Klamberg on EU Metadata Collection*, LAWFARE (Sept. 29, 2013, 1:03 PM), http://www.lawfareblog.com/2013/09/mark-klamberg-on-eu-metadata-collection/; Mark Klamberg, *FRA and the European Convention on Human Rights — A Paradigm Shift in Swedish Electronic Surveillance Law*, 2010 NORDISK ÅRBOK I RETTSINFORMATIKK 96 (Nor.) (describing Swedish electronic surveillance law).

159. Steven Erlanger, *France, Too, Is Sweeping up Data, Newspaper Reveals*, N.Y. TIMES, July 4, 2013, http://www.nytimes.com/2013/07/05/world/europe/france-too-is-collecting-data-newspaper-reveals.html.

160. European Parliament Resolution, *supra* note 131; HRC Concluding Observations, *supra* note 45.

161. Such an arrangement reportedly is contained in the Five Eyes signals intelligence agreement among the United States, United Kingdom, Canada, Australia, and New Zealand. Kady O'Malley, *From the Order Paper Question Archives: Do the "Five Eyes" Watch Each Other?*, CBC NEWS INSIDE POLITICS BLOG (Oct. 10, 2012, 3:35 PM), http://www.cbc.ca/newsblogs/politics/inside-politics-

specter of legal hurdles to cooperation, including domestic civil cases brought in the courts of the United Kingdom, Poland, and France for their surveillance activities or their cooperation with U.S. surveillance;[162] a case brought against the United Kingdom in the ECtHR;[163] and a criminal investigation against U.S. officials in Germany;[164] and (iii) European threats to stop various forms of data sharing with the United States.

Some of this litigation harkens back to what took place in the wake of U.S. revelations about its use of extra-judicial renditions and secret detention facilities after the September 11 attacks. There, foreign plaintiffs used foreign tribunals in an effort to pressure their own governments to influence U.S. policies.[165] In the end, no one foreign case was responsible for shifts in U.S. rendition and secret detention policies, but each contributed to the atmospheric pressure on the United States to alter its way of doing business. At this point, it is hard to predict how likely it is that any one of these legal or political hurdles will emerge in a form that notably limits one or more states from cooperating with others. But the possibility is there, and U.S. and foreign intelligence services surely are tracking such developments.

2. Rights-Driven Pressures

Whereas political pressures may be overtaken quickly by subsequent crises, rights-driven pressures historically begin slowly and build over time. Actions in the United Nations, the ICJ, the ECtHR, and other European domestic courts, and even domestic policy changes inside the United States reflect pressures to protect more assertively the right to privacy. Binding court decisions will impose direct requirements on states to alter the way that they conduct foreign surveillance; less binding actions in human rights bodies will press states to place greater weight on the privacy side of the privacy/security balance.

Several activities in the United Nations currently are imposing rights-based pressures on states. In the wake of the revelations about NSA surveillance of Chancellor Merkel's cell phone, Germany and Brazil

---

blog/2012/10/from-the-order-paper-question-archives-do-the-five-eyes-watch-each-other.html.

162. European Parliament Resolution, *supra* note 131, pmbl. & nn. 5–6 (noting cases before each of these courts); Owen Bowcott, *ISPs Take GCHQ to Court in UK over Mass Surveillance*, GUARDIAN, July 2, 2014, http://www.theguardian.com/world/2014/jul/02/isp-gchq-mass-surveillance-privacy-court-claim.

163. Hopkins, *supra* note 154.

164. *Snowden NSA: Germany to Investigate Merkel 'Phone Tap'*, BBC (June 4, 2014), http://www.bbc.com/news/world-europe-27695634.

165. *See, e.g.*, Ashley Deeks, *Litigating How We Fight*, 87 INT'L L. STUD. 427, 441 (2011) (describing how plaintiffs filed civil suit in United Kingdom against U.K. subsidiary of Jeppesen Dataplan, which plaintiffs alleged helped the CIA conduct rendition flights).

sponsored a UN General Assembly (UNGA) resolution addressing the right to privacy in the electronic age, which the UNGA adopted in December 2013.[166] The resolution "[a]ffirms that the same rights that people have offline must also be protected online, including the right to privacy[,]" and calls on states "[t]o review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy."[167] A preambular paragraph notes states' "deep[ ] concern[ ] at the negative impact that . . . extraterritorial surveillance . . . may have on the exercise and enjoyment of human rights."[168] This preambular language is contained in a non-binding resolution, which gives it limited standing in CIL formation, but quite often provisions that appear in preambular paragraphs in earlier UNGA resolutions find their way into more substantive provisions in later UN resolutions. Further, the resolution requests that the UN High Commissioner for Human Rights report on "the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale."[169] This issue therefore will remain on the UNGA's agenda for some time to come.

Other UN bodies have analyzed surveillance and its effects on the right to privacy. The Human Rights Council tasked the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression with producing a report on the implications of states' surveillance of communications on the rights to privacy and freedom of opinion and expression.[170] The Special Rapporteur's report criticized extraterritorial surveillance, expressing concern that such surveillance "raises serious concern with regard to the extra-territorial commission of human rights violations and the inability of individuals to know that they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance, or seek remedies."[171] He also was critical of states'

166. The Right to Privacy in the Digital Age, *supra* note 47. The UNGA adopted the resolution by consensus. The U.S. Government joined consensus on the resolution with an Explanation of Position that affirmed its "longstanding" views of the ICCPR, including Articles 2 and 17. That is, the United States reads the resolution as applying only to the extent that a state is acting on its own territory.

167. *Id.* ¶¶ 3, 4(c).

168. *Id.* pmbl.

169. *Id.* ¶ 5.

170. Human Rights Council Res. 16/4, Freedom of Opinion and Expression: Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, 16th Sess., Mar. 24, 2011, U.N. Doc. A/HRC/RES/16/4 (Apr. 8, 2011).

171. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Rep. on the Promotion and Protection of the Right to Freedom of Opinion and Expression*,

existing domestic surveillance laws, concluding that the laws often were "vague," "broadly conceived," and inadequate to protect against violations of privacy and freedom of expression.[172]

The UN Human Rights Committee, which monitors states' compliance with the ICCPR, recently issued Concluding Observations related to the U.S. submission and appearance before the Committee.[173] It recommended that the United States "take all necessary measures to ensure that its surveillance activities, both within and outside the United States, conform to its obligations under the Covenant, including article 17."[174] In so stating, the Committee firmly took the position that the United States has ICCPR obligations that extend to extraterritorial surveillance. The United States disagrees with this position,[175] but will continue to come under pressure to acknowledge that the ICCPR applies to at least some extraterritorial activity.

The United Nations is not the only body considering surveillance-related issues. The ICJ has before it a case that very likely will require it to opine on at least one aspect of international surveillance. Timor-Leste alleges that Australia raided the offices of Timor-Leste's Australian attorney and seized documents and other items that implicated Australia in bugging Timor-Leste's internal negotiations about a treaty.[176] Though the case is focused on the rights of states rather than the rights of individuals, an ICJ decision in Timor-Leste's favor would constitute the first binding pronouncement by an international court that some forms of extraterritorial surveillance violate international law.[177]

As noted above, surveillance cases are pending in the courts of France, Poland, and the United Kingdom.[178] In France, two rights groups asked a

---

Human Rights Council, ¶ 64, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) (by Frank LaRue) [hereinafter Special Rapporteur Report].

172. *Id.* ¶¶ 50–51.

173. HRC Concluding Observations, *supra* note 45. The HRC also criticized Sweden for a law that would give its executive broad powers of electronic surveillance. Human Rights Comm., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Concluding Observations of the Human Rights Comm.: Sweden, ¶ 18, U.N. Doc. CCPR/C/SWE/CO/6 (May 7, 2009).

174. HRC Concluding Observations, *supra* note 45, ¶ 22.

175. *See supra* text accompanying note 49.

176. *See* Ashley Deeks, *Can the ICJ Avoid Saying Something on the Merits About Spying in Timor Leste v. Australia?*, LAWFARE (Mar. 12, 2014, 5:00 PM), http://www.lawfareblog.com/2014/03/can-the-icj-avoid-saying-something-on-the-merits-about-spying-in-timor-leste-vs-australia/ [hereinafter Deeks, *ICJ on the Merits*]; Ashley Deeks, *East Timor's Case in the ICJ: Will the Court Decide Whether Spying Violates International Law?*, LAWFARE (Jan. 22, 2014, 10:00 AM), http://www.lawfareblog.com/2014/01/east-timors-case-in-the-icj-will-the-court-decide-whether-spying-violates-international-law/ [hereinafter Deeks, *Will the ICJ Decide*].

177. Deeks, *ICJ on the Merits*, *supra* note 176.

178. *See supra* note 162 and accompanying text.

French court to open a lawsuit against the NSA, FBI, and seven U.S. firms, which allegedly have facilitated NSA surveillance against French citizens.[179] In the United Kingdom, Amnesty International filed a complaint against the U.K. government, alleging that GCHQ unlawfully accessed Amnesty's communications using the Tempora program.[180] This case complains primarily about GCHQ's domestic or transnational, rather than extraterritorial, surveillance. Amnesty filed its suit with the Investigatory Powers Tribunal, claiming that GCHQ's surveillance violated Articles 8 and 10 of the United Kingdom's Human Rights Act of 1998, which recognizes the rights of privacy and free expression.[181] The Investigatory Powers Tribunal upheld GCHQ's actions, and Amnesty has appealed that decision to the ECtHR.[182] Other challenges have been lodged against GCHQ as well, including one by seven ISPs from different countries alleging that GCHQ used malicious software to break into their networks.[183] If the plaintiffs lose, they too presumably will appeal to the ECtHR.

Other plaintiffs have brought a case directly to the ECtHR.[184] There, the plaintiffs have asked the ECtHR to decide whether receipt by the United Kingdom of data from NSA's programs and GCHQ's transnational surveillance violates ECHR Article 8. If the ECtHR concludes that certain types of foreign surveillance violate the ECHR, all Council of Europe states parties would have to cease such surveillance to bring their behavior into compliance with a binding interpretation of the Convention. If states explicitly decide to apply certain international norms to their surveillance practices (such as those norms identified in Part III), and those norms provide credible (even if limited) privacy protections, the atmospherics surrounding these cases may improve, and states may find the cases brought against them easier to win.

Ironically, perhaps, recent unilateral changes to U.S. surveillance policies also contribute to pressures on the *status quo* in other states because the U.S. changes reveal ways in which states can curtail activities seen as over-

179. *French Lawsuit Filed over Alleged US Snooping*, FRANCE 24 (July 12, 2013), http://www.france24.com/en/20130711-france-legal-complaint-nsa-fbi-technology-firms-us-surveillance-allegations/.

180. Cynthia Miley, *AI Files Lawsuit Against UK Surveillance Program*, JURIST (Dec. 10, 2013, 9:33 AM), http://jurist.org/paperchase/2013/12/ai-files-lawsuit-against-uk-surveillance-program.php.

181. *Id.*

182. Owen Bowcott, *UK Mass Surveillance Laws Do Not Breach Human Rights, Tribunal Rules*, Dec. 5, 2014, http://www.theguardian.com/uk-news/2014/dec/05/uk-mass-surveillance-laws-human-rights-tribunal-gchq; Press Release, Amnesty Int'l, *supra* note 67.

183. Matthew Taylor & Nick Hopkins, *Amnesty to Take Legal Action Against UK Security Services*, GUARDIAN, Dec. 8, 2013, http://www.theguardian.com/world/2013/dec/09/amnesty-international-legal-action-uk-security-services; Bowcott, *supra* note 162.

184. Hopkins, *supra* note 154.

reaching. At least some of these policy changes might be classified as rights-driven. In January 2014, President Obama gave a speech recognizing that the privacy of foreign citizens must play a role in U.S. policy-setting, acknowledging the fears that attach to governmental bulk data collection, and advocating for increased transparency about electronic surveillance.[185] In Obama's words,

> the same technological advances that allow U.S. intelligence agencies to pinpoint an al Qaeda cell in Yemen . . . also mean that many routine communications around the world are within our reach. And at a time when more and more of our lives are digital, that prospect is disquieting for all of us.[186]

He noted that U.S. collection efforts "will only be effective if ordinary citizens in other countries have confidence that the United States respects their privacy, too."[187] And he acknowledged the importance of being as transparent as possible, even in an area of activity the very essence of which relies on secrecy. Although much about U.S. electronic surveillance remains non-public, the United States seems to have adopted a new commitment to transparency regarding its collection programs, which is a significant change from its posture before the Snowden leaks.[188] A U.S. willingness to be increasingly transparent will have overflow effects on the expectations of citizens of other states known to be engaged in foreign surveillance.

185. Obama NSA Speech, *supra* note 1.

186. *Id.*

187. *Id.* Though not directly focused on surveillance, the White House's Big Data and Privacy Working Group Review, issued on May 1, 2014, echoed this approach. The report stated, "Privacy is a worldwide value that the United States respects and which should be reflected in how it handles data regarding all persons[.] For this reason the United States should extend privacy protections to non-U.S. persons. . . . The Office of Management and Budget should work with departments and agencies to apply the Privacy Act of 1974 to non-U.S. persons where practicable, or to establish alternative privacy policies that apply appropriate and meaningful protections to personal information regardless of a person's nationality." EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 63 (2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

188. Litt, *supra* note 90 (noting that Snowden leaks have forced the U.S. intelligence community to rethink its approach to transparency and secrecy and that the government might have suffered less damage from the leaks if it had been more forthcoming *ex ante*); 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-speech-and-ppd-28-a-guide-for-the-perplexed/ (quoting Bruce Riedel as stating, "I don't think we've ever had a document like [PPD-28] that lays out the protocols and principles for American signals intelligence collection" and noting that not many other countries "have public documents that lay out principles and doctrines of surveillance permission and restraint").

3. Economic Pressures

Though political pressures may appear suddenly and fade quickly, economic pressures are likely to force a more sustained consideration of surveillance policies because the effects of the Snowden revelations will take longer to manifest themselves. One unexpected source of pressure on the non-regulation of extraterritorial surveillance has come from U.S. corporations. In 2009, Loch Johnson wrote that "when it comes to the security agenda of most intelligence services, commerce continues to take a back seat to direct threats to national survival."[189] While national security remains of paramount concern to states, the importance and power of the commercial interests of ISPs and social media companies such as Google, Yahoo, Facebook, and Microsoft should not be understated today. Snowden's revelations also have affected U.S. companies that provide cloud computing services, partly because such services often store data on servers with excess capacity — which may well be in the United States.[190] These companies fear the perception that they enabled NSA spying, and are suffering a significant loss of business overseas from customers who suspect that they will be easier targets for U.S. surveillance if they use U.S. products.[191] U.S. companies also are concerned that it will become more difficult for them to move their own business data from foreign affiliates to their home offices if foreign states begin to regulate more aggressively the movement of data overseas or mandate that domestic companies and affiliates use domestic products.[192] Several of these companies have called on the President and Congress to reform government surveillance by ceasing to collect Internet communications in bulk and bolstering checks and balances on executive powers.[193]

189. Johnson, *supra* note 78.

190. Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES, Mar. 21, 2014, http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

191. Declaration of Rajesh Jha at 4, ¶¶ 8–9, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., Nos. M9–150, 13–MJ–2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014); Elena Schneider, *Technology Companies Are Pressing Congress to Bolster Privacy Protections*, N.Y. TIMES, May 26, 2014, http://www.nytimes.com/2014/05/27/us/technology-firms-press-congress-to-tighten-privacy-law.html; Elizabeth Dwoskin, *New Report: Snowden Revelations Hurt U.S. Companies*, WALL ST. J. DIGITS BLOG (July 30, 2014, 1:58 PM), http://blogs.wsj.com/digits/2014/07/30/new-report-snowden-revelations-hurt-u-s-companies/ (stating that information in Snowden's leaks could cost U.S. cloud computing industry between $22 and $180 billion by 2016); Antonio Regalado, *Spying Is Bad for Business: Can We Trust an Internet That's Become a Weapon of Governments?*, MIT TECH. REV. (Mar. 18, 2014), http://www.technologyreview.com/news/525526/spying-is-bad-for-business/ (describing corporate concerns and harm to industry from NSA revelations).

192. Michael Hickins, *Spying Fears Abroad Hurt U.S. Tech Firms*, WALL ST. J., Feb. 3, 2014, http://online.wsj.com/news/articles/SB10001424052702303743604579350611848246016.

193. *An Open Letter to Washington*, REFORM GOV'T SURVEILLANCE (Dec. 2013),

Some countries already have started to turn inward. For instance, Brazil has announced that it will cease using Microsoft Outlook as its email system.[194] China plans to require "stricter vetting of companies selling Internet technology and services" in China.[195] Germany (among other countries) is considering whether to enact legislation that would make it difficult or impossible for American technology companies to operate inside Germany,[196] and as a result of the Snowden revelations the German government recently terminated its telecommunications contract with Verizon in favor of German company Deutsche Telekom.[197] With France, Germany has contemplated creating a European Internet that would allow Europeans to send and receive emails and other data without having them pass through U.S. networks and servers.[198] There are technical and practical downsides to such an idea, and experts claim that there are better ways to maximize data protection without altering the route that data packets take.[199] Nevertheless, fears about harm to the corporate bottom line have prompted U.S. Internet-oriented companies to urge the U.S. Administration to be more transparent about its surveillance and to restrict its intelligence-gathering.[200]

C. Asymmetric State Incentives

The interstate dynamics of foreign surveillance matter in considering how international norms should and may develop. States fall into roughly three categories in their approach to surveillance regulation: (1) Western and other democratic states; (2) technologically powerful non-democracies or quasi-democracies such as Russia, China, and Iran; and (3) non-technologically advanced states. Each set of states has different incentives

---

https://www.reformgovernmentsurveillance.com (signed by Google, AOL, Yahoo, and others).

194. Miller, *supra* note 190 (describing also the decision by a German company to use Deutsche Telekom rather than a U.S. company for its cloud computing services).

195. Chris Buckley, *Beijing Levels New Attack at U.S. Cyber-Spying*, N.Y. TIMES SINOSPHERE BLOG (May 26, 2014, 8:23 AM), http://sinosphere.blogs.nytimes.com/2014/05/26/beijing-levels-new-attack-at-u-s-cyber-spying/.

196. Miller, *supra* note 190.

197. Aaron Mamiit, *German Government Drops Verizon Contract in Fear of U.S. Espionage*, TECH TIMES (June 27, 2014, 9:11 AM), http://www.techtimes.com/articles/9292/20140627/german-government-drops-verizon-contract-in-fear-of-u-s-espionage.htm.

198. Sam Ball, *Plans to Stop US Spying with European Internet*, FRANCE 24 (Feb. 18, 2014), http://www.france24.com/en/20140217-european-internet-plans-nsa-spying/.

199. Mark Ward, *Can Europe Go Its Own Way on Data Privacy?*, BBC (Feb. 18, 2014), http://www.bbc.com/news/technology-26228176.

200. David Jackson, *Obama Talks Privacy and Surveillance with Tech CEOs*, USA TODAY, Mar. 21, 2014, http://www.usatoday.com/story/news/nation/2014/03/21/obama-google-national-security-agency-surveillance/6697593/ (reporting that Facebook's Mark Zuckerberg urged the government to be "much more transparent about what they're doing" (internal quotation marks omitted)).

to commit (or not commit) to a new set of international norms governing surveillance. States in the first category face real pressure to modify the *status quo*, and will accrue certain benefits if they do so. States in the third category bear limited costs if they sign on to more rigorous surveillance rules because their ability to conduct surveillance is limited. For many of these states, new limits on surveillance offer only upside gains.[201] States in the second category, however, will be unlikely to adopt new norms in the short to medium term, particularly because they face less internal public pressure to do so.[202] Additionally, their citizens may have a greater tolerance for (or at least a higher expectation of) governmental interference with their communications than does the public in a democracy.[203]

In light of these disparate incentives and an interest in obtaining reciprocal benefits when deciding to adopt limiting norms, states will be loath to formally adopt these principles unilaterally.[204] Even in the face of public pressure, states surely will calculate that they will lose more than they gain by accepting these principles without comparable commitments from other states. This suggests that states should initiate discussions among like-minded states, such as those whose practice is discussed here, about what norms will be acceptable to those states and will be seen to increase privacy protections extraterritorially.[205]

---

201. Nevertheless, some smaller states may be allied with large, technologically advanced states and may benefit from the latter's more robust capacities through intelligence-sharing arrangements. These smaller states will be more cautious about pressing for robust surveillance regulations.

202. CDT REPORT, *supra* note 157, at 24 (noting that Chinese law allows the state to inspect electronic communications instruments of any organization or individual for purposes of state security, with few limitations); Obama NSA Speech, *supra* note 1 ("No one expects China to have an open debate about their surveillance programs, or Russia to take privacy concerns of citizens in other places into account.").

203. Adam Taylor, *Putin Told Edward Snowden that Russia Doesn't Use Mass Surveillance on Its Citizens. Here's a Reality Check.*, WASH. POST, Apr. 17, 2014, http://www.washingtonpost.com/blogs/worldviews/wp/2014/04/17/putin-told-edward-snowden-that-russia-doesnt-use-mass-surveillance-on-its-citizens-heres-a-reality-check/ (noting that there has been little debate in Russia about surveillance and that many Russians accept the trade-off between security and loss of communications privacy).

204. ROBERT E. SCOTT & PAUL B. STEPHAN, THE LIMITS OF LEVIATHAN: CONTRACT THEORY AND THE ENFORCEMENT OF INTERNATIONAL LAW 94 (2006) ("[A]ll parties have an interest in cementing their contractual relationship within an embedded framework based on reciprocity."); Benjamin Wittes, *Assessing the Review Group Recommendations: Part V*, LAWFARE (Jan. 6, 2014, 7:59 AM), http://www.lawfareblog.com/2014/01/assessing-the-review-group-recommendations-part-v/ (noting importance of reciprocity); Posner, *supra* note 7 (arguing that it is not in U.S. interests to extend extraterritorial protections unilaterally); Joel Brenner, *A Fruitcake of a Report*, LAWFARE (Dec. 20, 2013, 8:15 AM), http://www.lawfareblog.com/2013/12/a-fruitcake-of-a-report/ ("[T]he fundamental principle here must be mutuality . . . .").

205. Though states themselves will decide who sits at the table during such discussions, preferably representatives from foreign offices, the intelligence communities, and official privacy advocates would be present for any norm-shaping conversations. This might also be a situation in

One possibility, therefore, is that these norms develop first (and possibly exclusively) among states that adhere to them publicly and privately.[206] The norms discussed below should attract relatively widespread agreement among democratic, Western countries and perhaps other democracies such as Israel, Japan, South Korea, India, and Turkey. But it might be the case that states will only agree to apply these norms to their surveillance of other states that accept the same norms. In such a case, the norms would begin among a relatively small group of states, with the chance of spreading in direct relation to the level of trust that these early-adopting states have toward other states that later purport to accept the norms.

The idea that it is desirable to develop a set of international norms that applies only to a subset of states — but that ultimately may evolve into CIL that applies to states more broadly — will not be without controversy.[207] Yet there is historical precedent for this. During the Cold War, the Soviet Union adopted an approach to international law — a set of principles it referred to as "peaceful coexistence" — that diverged in important ways from the West's approach.[208] The Soviet Union and the West also developed different rules for determining what counted as international law.[209] Where, as in today's world, there are multiple powerful actors whose interests are not obviously aligned (notably, the United States, United Kingdom, Russia, and China), we should expect competing claims about the contents of international legal obligations.[210]

The question then becomes whether this is an attractive state of affairs. What transpired during the Cold War included a European decision to establish strong regional human rights organs and the adoption of

---

which states wish to have a representative from their parliament or legislature, particularly someone who sits on an intelligence oversight committee.

206. A corresponding possibility is that states in the second category, such as Russia and China, publicly object to new norms in this area, precisely because they fear that early norms developed among such a group will have a lasting effect in international law. Doing so would incur political costs, even on those types of states, because it would seem highly rights-averse to argue publicly that states should be able to operate under secret surveillance laws, or that the government must have unfettered capacity to surveil all communications.

207. However, depending on the form that such international norms took, this outcome might not look very different from a decision by a group of states to conclude a multilateral treaty that would remain open to later accession by other states.

208. Leon Lipson, *Peaceful Coexistence*, 29 L. & CONTEMP. PROBS. 871, 878 (1964) (describing Soviet rejection of norms of nonaggression and protection of minority and democratic rights); Victor P. Karpov, *The Soviet Concept of Peaceful Coexistence and Its Implications for International Law*, 29 L. & CONTEMP. PROBS. 858, 864 (1964) (arguing that peaceful coexistence should be the basis of the whole structure of international law).

209. Paul B. Stephan, *Symmetry and Selectivity: What Happens in International Law When the World Changes*, 10 CHI. J. INT'L L. 91, 92 (2009).

210. *Id.* at 101.

important multilateral instruments such as the ICCPR. When the Cold War ended, the former Soviet republics, for various reasons, were willing to adopt many of those human rights principles.[211] This is not to predict that China and Russia will ultimately conclude that it is in their interests to adhere to new international surveillance norms. It is to argue that there are advantages to having smaller groups of states advance certain norms, even in the absence of universal support. Taking this approach allows states that are impatient for progress on the international plane to accelerate that progress without being hamstrung by the lowest common denominator around which states can coalesce.[212] It also permits those states that are unhappy about the direction of international legal developments to allow others to proceed as long as they are not forced to adopt policies they see as contrary to their national interests.

D. Between International Laws and Norms

The developments described herein reveal a moment ripe for international legal change, regardless of one's underlying assumptions about international relations between states. Yet, unlike much domestic law, international law is slow to develop. It often takes a long time to negotiate a new treaty on a complicated issue. It is possible that states will decide to negotiate a multilateral treaty to regulate this area of activity. But it is unlikely that the states with the greatest surveillance capabilities — the United States, United Kingdom, Russia, and China — would be able to agree on appropriate norms of foreign surveillance.

It is far more likely that states will develop customary international norms of foreign surveillance. That, too, is a time-consuming prospect. It takes years of state practice and *opinio juris* for CIL to form.[213] This Article does not claim that the norms proposed in Part III constitute CIL, or will constitute CIL in the near future. It does claim, however, that the norms described herein are the ones around which states should coalesce in the short term, and that if they do so, these norms are likely to become CIL in the medium term. States might decide to indicate their support for these norms (or, indeed, other surveillance-related norms) in a variety of ways. They might sign on to a "commitment to principles," conclude a political memorandum of understanding, or issue unilateral but parallel statements

211. *Id.* at 113.

212. HENKIN, *supra* note 102, at 38 ("[N]othing prevents the like-minded from making law for themselves when less-than-universal agreements serve some purpose.").

213. In this regard, I adopt the requirement of "traditional custom," which envisions extensive state practice, accompanied by *opinio juris*, before a principle may be deemed to rise to the level of CIL. Anthea Elizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 AM. J. INT'L L. 757 (2001).

indicating their view that certain norms reflect internationally acceptable behavior. Though state practice will remain relevant in determining when these ideas crystallize into international norms that are binding on a wider set of states, the fact and shape of these norms will depend, in large part, on what states say about the norms that they think bind them (*opinio juris*) rather than what they do. This is because surveillance is, by definition, clandestine, and states often decline to reveal their capacities and actions.[214]

At the same time that states may develop CIL norms regarding surveillance, another parallel process of international law development will undoubtedly take place. That parallel process is the ongoing interpretation of the privacy provisions in the ICCPR and ECHR. Both states and other actors that interpret treaties will continue to engage in the process of claim and counterclaim about what those provisions mean and how to apply them to this new world of foreign surveillance. This interpretive process can coexist with a decision by certain states to adopt new procedural norms regulating surveillance, and in fact would prove complementary in establishing appropriate standards.

III. AN INTERNATIONAL FRAMEWORK FOR SURVEILLANCE

A. Regulations' Structural Underpinnings

If we believe that the international normative landscape should (and likely will) change as a result of the contemporary pressures described above, we naturally must ask what the new norms should look like. Answering that question becomes easier when one first considers what the source of the new norms should be.

I have previously argued that domestic laws can and do serve as the basis for international legal developments, particularly in the face of highly politicized issues, non-reciprocal incentive structures, issue complexity, and different conceptions of the proper governing legal framework.[215] Each of these factors is present in the surveillance debate. The revelations about various states' technological capabilities and the uses to which they have put those capabilities have rendered the issue highly sensitive politically among allies. States possess widely varied capabilities to conduct surveillance, and therefore are likely to confront different incentives when considering whether and how to regulate such surveillance. Further, the

214. *Id.* (discussing respective weight placed on *opinio juris* in "new custom," though for reasons other than secrecy); *see also* Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L L. 507 (2015).

215. *See* Deeks, *Domestic Humanitarian Law*, *supra* note 6.

issue is complex: It is difficult to know precisely what types of surveillance each state is conducting, what technologies they are using, and what their targets are. Moreover, the issue implicates concepts of personal privacy. Different cultures have widely disparate views on what privacy entails and the grounds on which it is legitimate for a state to surmount that privacy.[216] Finally, various states view existing treaty provisions as more or less relevant to regulating privacy. These states also perceive security threats differently. All of these factors suggest that commonalities found in domestic laws will be an important source of norms in the surveillance area.

In the context of the evolution of international humanitarian law (IHL), I argued that contemporary conflicts pose new challenges to the existing body of international law, such that there is a *non liquet* in the law governing certain kinds of non-international armed conflicts. I further argued that new domestic rules emanating from courts, legislatures, and executive branches will have significant effects on future IHL developments. Probable results include: "affecting the likelihood of a future international agreement on those rules; the substance of those future rules in the event such an agreement emerges; the way in which states interpret certain existing treaty provisions; and the content of state practice that contributes to the formation of new rules of customary international law."[217]

The same can be said for the evolution of international norms on espionage: Domestic laws, which continue to evolve but provide at least basic substantive and procedural rules about domestic and transnational surveillance, will affect the way in which those international norms develop. These laws have proven to work effectively in practice (at least as far as they govern domestic and transnational surveillance); have been the subject of public debates during which legislators have considered how to balance privacy and security; and are (mostly) publicly accessible. Furthermore, to the extent that general international norms track common concepts reflected in states' domestic laws, external observers may have greater confidence that states will comply with the international norms, because governments tend to comply more rigorously with domestic laws than international law.[218]

---

216. For differences even among Western states, see James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004).

217. Deeks, *Domestic Humanitarian Law*, *supra* note 6, at 134–35.

218. Goldsmith & Posner, *supra* note 126, at 1175 (indicating that while domestic law is enforced in well-ordered societies, international law is not reliably enforced). *But see* Goldsmith & Levinson, *supra* note 107 (calling into question whether constitutional law regulating government action is more enforceable than international law). *See also* INTERCEPTION OF COMMUNICATIONS COMMISSIONER, 2012 ANNUAL REPORT, 2012–13, H.C. 571, SG/2013/131, at 12–18, 38 (U.K.), *available at*

The following norms derive primarily from the domestic laws of five Western states: the United States, the United Kingdom, Canada, Germany, and Australia.[219] I selected these states because they have some of the most extensive laws regulating surveillance. By implication, these states have given extensive attention to the appropriate balance between privacy and national security; effective ways to monitor and counter-balance the government's surveillance power; and the need for government actors to adopt internal protections for the data they collect and handle. These laws admittedly are not necessarily representative of domestic laws across various regions.[220] Further, the norms are drawn from the laws as they appear on the books, rather than as they apply in practice. Governments may interpret and apply published laws in ways that are not obvious to the average citizen.[221] That said, the existence of a published law makes it politically more difficult for a government to resist principles drawn from that law.

The bulk of these domestic laws focus on regulating executive actors' electronic surveillance of their own citizens or residents, as well as collection that takes place in their state's territory — that is, domestic and some transnational surveillance. Very few laws around the globe regulate purely extraterritorial collection.[222] One sensible reason for this is that domestic surveillance laws are primarily intended to prevent government officials from abusing or manipulating that very system of government. Improper surveillance of the citizenry (based, for example, on political views or associations) might corrupt the political system by allowing those currently holding power to suppress the opposition and unlawfully remain in power.[223] A related reason to regulate domestic surveillance more

---

http://www.iocco-uk.info/docs/2012%20Annual%20Report%20of%20the%20Interception%20of%20Communications%20Commissioner%20WEB.pdf (describing seriousness with which U.K. officials take their responsibilities to comply with the Regulation of Investigatory Powers Act (RIPA)); Obama NSA Speech, *supra* note 1 ("[N]othing that I have learned since[ ] indicated that our intelligence community has sought to violate the law . . . .").

219. I consider several other states' laws in passing, including those of France, Italy, and Sweden.

220. China and India provide almost no protection or oversight regarding government surveillance, whether for law enforcement or national security purposes. CDT REPORT, *supra* note 157, at 17.

221. *Id.* at 17 ("In many countries, the published law appears to say something different from what governments are reportedly doing.").

222. *Id.* at 19–20 ("Most countries, even those that have recognized privacy as a universal right, seem to apply much lower protections (if any) to surveillance directed at foreigners.").

223. Obama NSA Speech, *supra* note 1 ("[F]ew, if any, spy agencies around the world constrain their activities beyond their own borders."); S. REP. NO. 95-604, pt. 1, at 7–8 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908–10 (noting that FISA was a response to congressional investigations of abuses of surveillance directed at American political organizations); SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE

aggressively than foreign surveillance is that a state can generally affect the lives of those it surveils in more intrusive and harmful ways when the subjects of surveillance are present on that state's territory.[224] Yet another reason relates to the set of tools that states have in their domestic and international toolboxes. States arguably need greater flexibility to collect communications intelligence overseas because they have fewer alternative tools to use there than they do domestically (where states can rely on police investigations, warrants, national security letters, and so on).

As a result, it is important to be cautious about drawing principles from statutes directed at domestic or transnational surveillance (which often implicate the state's own citizens) to regulate extraterritorial surveillance (which usually implicates only citizens of other states).[225] But the communications of some foreign nationals already incidentally receive some procedural protections by virtue of the fact that their communications happen to transit, say, the United States, or occur between that foreign national and a U.S. citizen.[226] That is, although these communications by foreign nationals are not protected by the same types of minimization procedures as those of U.S. nationals, they are subject to statutory regulation in the form of the Foreign Intelligence Surveillance Act (FISA) and judicial oversight by the Foreign Intelligence Surveillance Court.[227] Even if there are creditable political and practical reasons to prioritize the privacy of citizens, there is little conceptual reason not to

---

ACTIVITIES AND THE RIGHTS OF AMERICANS, bk. II, S. REP. NO. 94-755 (1976) (discussing history of abusive surveillance by U.S. agencies); *Intelligence Services Act 2001* (Cth) s 12A (Austl.) (stating that the Director of the Defense Signals Directorate must reasonably ensure that "nothing is done that might lend colour to any suggestion that his or her agency is concerned to further or protect the interests of any particular section of the community"). *But see* Milanovic, *supra* note 2 (manuscript at 18–19) (arguing that this claim is weak because some individuals protected by U.S. surveillance statutes play no role in the U.S. political process).

224. Thanks to Alan Rozenshtein for this insight.

225. Of course, if one takes the view that nationality should be irrelevant to the privacy protections that one receives, one readily would extend existing domestic and transnational surveillance regulations to extraterritorial collection. *See* Milanovic, *supra* note 2 (manuscript at 25) ("[C]itizenship is normatively irrelevant for the threshold question of whether a human rights treaty applies to a particular act of surveillance.").

226. Foreign Intelligence Surveillance Act of 1978 § 702 (codified as amended at 50 U.S.C. § 1881a (2012 & Supp. I 2013)).

227. For example, FISA § 702, as amended, constrains the type of activity about which the U.S. government can collect information; establishes pre-collection approval procedures in the form of certifications by senior executive officials; and requires the Foreign Intelligence Surveillance Court to review those procedures before collection may occur. 50 U.S.C. § 1881a. The government must notify a person in advance that it intends to use information collected against him under Section 702 in a judicial or administrative proceeding. *Id.* §§ 1806(c), (d); 1881e. That person can challenge the lawfulness of the acquisition before the government introduces the gathered information as evidence. *Id.* §§ 1806(e)–(g); 1881e. The remedy is to suppress the use of that evidence. *Id.* §§ 1806(g); 1881e.

accord similar protections to the communications of all foreign nationals.[228] Governments know how those rules work in practice. They also have established frameworks of oversight that could, in many cases, be extended quite easily to purely extraterritorial surveillance. Finally, governments understand what they have to gain or lose by expanding existing protections and procedures. Existing domestic laws related to transnational surveillance therefore provide important foundational concepts from which states can derive additional, extraterritorially directed norms.

Although domestic law is the most likely source of ideas for international surveillance norms, there is some limited international practice that might also provide guidance.[229] Most famously, five English-speaking democracies have entered into an arrangement by which they share electronic surveillance duties and products. The Five Eyes agreement structures intelligence cooperation and establishes accepted behavioral norms and practices among the allied intelligence services of the United States, United Kingdom, Canada, Australia, and New Zealand.[230] Although this arrangement, the contents of which are not public, may not contribute heavily to the creation of international norms regarding foreign surveillance, the original U.K.-U.S. Agreement (UKUSA) from which the Five Eyes agreement derives details the types of communications that each state is to collect and treats as impermissible some uses of those communications.[231]

---

228. Executive Order 12,333, which regulates the authorities and responsibilities of the U.S. intelligence community, offers an example of rules that provide greater protections to U.S. persons than to foreigners. *See, e.g.*, Exec. Order No. 12,333, 3 C.F.R. 200, §§ 2.3–2.5 (1982), *reprinted as amended in* 50 U.S.C. § 401 note (2012). Whether a foreign national's communications fall within the protections of Section 702 or the more bare-bones E.O. 12,333 therefore depends on facts outside the control of that national. If his communications data begins and remains overseas, Section 702 will not attach (unless that data happens to be held overseas by a U.S.-based ISP). If his communications data transits the United States through a U.S.-based ISP, it will. While this may not be logical or defensible, it suggests that if the Executive Branch finds Section 702 workable in pursuit of foreign intelligence, it should be possible to apply similar protections to purely extraterritorial intelligence collection.

229. *See* Chesterman, *supra* note 35, at 1095 (noting possible relevance of multilateral intelligence-sharing practice to international norms of what is permissible).

230. JAMES COX, CANADA AND THE FIVE EYES INTELLIGENCE COMMUNITY 4 (Canadian Int'l Council & Canadian Defence & Foreign Affairs Inst., Strategic Studies Working Grp. Papers, 2012), *available at* http://opencanada.org/wp-content/uploads/2012/12/SSWG-Paper-James-Cox-December-2012.pdf.pdf.

231. The Five Eyes agreement is not the only example of "no spy" agreements. The Soviet Union and its satellite territories reportedly concluded such agreements, though the satellites quickly violated their obligations. Reisman, *supra* note 29, at 421 n.3. Little else is known about the agreements.

For example, UKUSA defined "foreign communications" somewhat more narrowly than the United States did domestically at the time. UKUSA stated that "foreign communications" constituted

> all communications of the government or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor, and shall include . . . communications of a foreign country which may contain information of military, political or economic value.[232]

This provision excludes foreign nationals as a general category of individuals who may be subject to surveillance. Further, UKUSA requires the parties to ensure that without prior notification and consent of the other party, "no dissemination of information derived from Communication Intelligence sources is made to any individual or agency, governmental or otherwise, that will exploit it for commercial purposes."[233] UKUSA also envisions that the parties will establish identical security regulations to protect communications intelligence.[234] While not particularly useful as an international norm, it indicates advantages in harmonizing rules in this area.

The norms discussed in the next Subpart ultimately should be acceptable to a variety of states. If states shift their practices to reflect these norms, they will be initiating state practice related to electronic surveillance. The early adopters will not be doing so out of a sense of *opinio juris* — after all, as this Article has argued, these pressures and norms are nascent — but as more and more states adhere to these norms (or express public support for them), international law slowly will take shape.

B. Six Norms

Once one identifies domestic law as a profitable source of ideas for international surveillance regulation, one naturally asks: What should those norms look like? Not surprisingly, this is a challenging question to answer, in part because people have very different ideas about what the substantive

---

232. British-U.S. Communication Intelligence Agreement, U.S.-U.K., art. 3 n.3, Mar. 5, 1946 [hereinafter UKUSA], *available at* http://www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf; *see also* Farrell, *supra* note 29 (quoting UKUSA, *supra*). *Compare* UKUSA, *supra*, *with* NAT'L SEC. COUNCIL, INTELLIGENCE DIRECTIVE NO. 9, *supra* note 12 (defining "foreign communications" as "includ[ing] all telecommunications and related materials . . . of the government *and/or their nationals* or of any military, air, or naval force, . . . or of any person or persons acting or purporting to act therefor" (emphasis added)).

233. UKUSA, *supra* note 232, art. 9.

234. *Id.* art. 8.

right to privacy entails.[235] Line-drawing in this area is very hard; one may be comfortable with particular examples of spying because one dislikes the subject of the spying, or believes that the activity being surveilled deserves to be made public and condemned. At the same time, one may be uncomfortable with other examples of spying because one is sympathetic to the subject of spying, or believes that the activity being surveilled warrants protection and support.[236]

Not only has the international community been slow to agree on the situations to which a substantive right to privacy attaches or the extent to which to credit that right. It also has failed to develop agreed-upon concepts of when a state may infringe on that right to privacy, such that the infringement is not arbitrary or unlawful.[237] For example, the Human Rights Committee stated in General Comment 16 that states may only interfere with the right to privacy "on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."[238] That statement says nothing about what that regulating law may or may not provide. As noted above, substantive norms derived from an interpretation of ICCPR Article 17 are in the early stages of development,[239] but there is much work to be done before states reach a consensus on the correct way to apply Article 17 to foreign surveillance.

As a result, the first kinds of international norms to emerge should be procedural rather than substantive. That is, they should regulate the kinds of procedural protections that states should impose on their own intelligence collection, rather than offer substantive definitions of what areas of personal activity are entitled to privacy and the situations in which states may interfere with that privacy. As I use the term, "procedural"

---

235. *See, e.g.*, Orin Kerr, *More on the (Alleged) Global Right to Privacy*, LAWFARE (Dec. 2, 2013, 1:28 AM), http://www.lawfareblog.com/2013/12/more-on-the-alleged-global-right-to-privacy/ (critiquing another analyst's arguments for failing to describe what a global right to privacy against government interference would look like); Special Rapporteur Report, *supra* note 171, ¶ 21 ("Despite the widespread recognition of the obligation to protect privacy, the specific content of this right was not fully developed by international human rights protection mechanisms at the time of its inclusion in [the ICCPR]. The lack of explicit articulation of the content of this right has contributed to difficulties in its application and enforcement.").

236. *See, e.g.*, Conor Friedersdorf, *The U.S. Has No Right to Spy on Masses of Regular People in Other Countries*, ATLANTIC (Sept. 11, 2013), http://www.theatlantic.com/politics/archive/2013/09/the-us-has-no-right-to-spy-on-masses-of-regular-people-in-other-countries/279546/ ("What I am suggesting is that certain kinds of international spying are morally permissible and legitimate, while others are immoral and illegitimate. Drawing a coherent line is extremely difficult . . . .").

237. Special Rapporteur Report, *supra* note 171, ¶ 21.

238. Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, 191 ¶ 3, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. 1) (May 27, 2008) [hereinafter HRC General Comment 16] (providing the Human Rights Committee's 1988 comments on Article 17 of ICCPR).

239. *See supra* Part I.B.3.b.

surveillance norms are objectively verifiable and do not require case-by-case or discretionary value judgments about privacy or security equities in assessing compliance with the norm.[240] Just because a norm is procedural does not mean that it has no effect on substantive rights, though. The procedural norms may in fact affect how states (re)interpret the provision in ICCPR Article 17 that forbids intrusions into privacy that are "arbitrary or unlawful."[241] Foreign surveillance that is conducted consistent with these procedural norms may be deemed non-arbitrary, at least as a baseline. These procedural norms benefit from being less discretionary than substantive norms, easier to assess for compliance, and easier to codify in plain language.

Any international norms that states develop should promote — and be seen to promote — four goals. First, international surveillance norms should further the transparency of the applicable rules. One persistent complaint about surveillance laws has been that the rules that bind states have been interpreted by those states and courts in ways that few could predict.[242] As U.S. Senator Ron Wyden colorfully put it, speaking about the secret interpretation of Section 215 of the USA PATRIOT Act, under which the United States gained access to the telecommunications of various foreign terrorist organizations, "Look at the gap between what people think the law is and how it's been secretly interpreted . . . . Holy Toledo!"[243] As a result, those subject to the rules are not aware of these "secret" interpretations but are directly affected by them. New international norms should promote greater transparency about what the rules are and the ways in which states are interpreting them.

Second, future international norms should limit the ability of governmental officials to act in an unduly discretionary way. There are at least two ways in which government officials might have discretion in the

240. A description of substantive privacy norms focuses on metaphysical concepts and balancing of values. *See, e.g.*, Beth Van Schaack, *Results of High Commissioner's Data Call Available Online*, JUST SECURITY (Apr. 18, 2014, 4:17 PM), http://justsecurity.org/9558/results-high-commissioners-data-call-online/ (noting that "many states (e.g., Guatemala, Germany, Hungary) conceptualize the bucket of rights implicated by mass and targeted surveillance more broadly as rights to dignity, autonomy, self-determination, and/or personality" and that "security and law enforcement forces are subject to the proportionality principle mandating that the least restrictive means be employed to achieve a legal aim").

241 ICCPR, *supra* note 39.

242. Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES, July 6, 2013, http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html; Winston Maxwell, *Systematic Government Access to Private-Sector Data in France*, 4 INT'L DATA PRIVACY L. 4, 6 (2014).

243. Ryan Lizza, *State of Deception: Why Won't the President Rein in the Intelligence Community?*, NEW YORKER, Dec. 16, 2013, http://www.newyorker.com/magazine/2013/12/16/state-of-deception (internal quotation marks omitted).

surveillance context: discretion to authorize surveillance procedurally, and discretion to choose the targets of surveillance. The easier it is for governmental officials to exercise such discretion on either front, the greater the possibility of abuse. The more precise and detailed the surveillance rules, the smaller the window for arbitrary official actions.[244]

Third, these norms should increase the accountability of state officials for the actions they take. Electronic surveillance, though now much more widely understood, remains cloaked in secrecy. Full public accountability over surveillance operations poses a challenge, because one must have access to classified information in order to assess the full scope of the government's performance. But various actors other than the general public may promote the accountability of those conducting surveillance.

Finally, these norms should reduce the disparity in treatment between citizens and foreigners. After all, this disparity undergirds much of the international outcry about foreign surveillance. The idea that a government should act with particular restraint when surveilling its own citizens remains a compelling one for many states, including because governments have a wider range of alternative tools by which to protect their own security when dealing with domestic threats.[245] However, the justifications for disregarding foreigners' privacy entirely are difficult to uphold, and many existing domestic laws provide some protections to foreigners' communications, albeit in unpredictable ways. That is, many of these laws provide some privacy protections to foreigners incidentally, based on the routes that communications happen to take or the location of the foreign national undertaking the communication, but fail to protect the privacy of other foreign nationals entirely. New norms should reduce this disparity in treatment.

1. Legality and Notice of Applicable Rules

One critical norm is the norm of "legality." That is, it is important for all persons to know how their own state and other states are regulated in conducting foreign surveillance. General Comment 16 affirms this point: The gathering of personal information by public authorities "must be regulated by law."[246] The idea of legality may be parsed into at least two concepts: knowledge about which individuals may be subject to

244. This assumes that the rules themselves do not build in excessive discretion.

245. Orin Kerr, *A Reply to David Cole on Rights of Foreigners Abroad*, LAWFARE (Nov. 2, 2013, 1:54 AM), http://www.lawfareblog.com/2013/11/a-reply-to-david-cole-on-rights-of-foreigners-abroad/ [hereinafter Kerr, *A Reply to David Cole*]. *But see* Milanovic, *supra* note 2 (manuscript at 25) (arguing that there is no compelling justification for distinguishing between privacy rights for citizens and non-citizens).

246. HRC General Comment 16, *supra* note 238, at 193 ¶ 10.

surveillance, and knowledge about which state agencies may undertake such surveillance against them. General Comment 16 asserted that states should "specify in detail the precise circumstances in which such interferences may be permitted[,]" thus providing adequate notice to individuals about the situations in which a state may observe their conduct.[247] Notwithstanding the Human Rights Committee's efforts in General Comment 16, the Special Rapporteur complained about a continued lack of clarity on this front, stating that individuals currently are unable to know that they might be subject to foreign surveillance.[248]

This approach extends the more traditional idea that citizens should have access to the laws by which they and their government are bound. Under this new norm, citizens of State A should have knowledge not only of those surveillance laws that authorize and regulate their own government's surveillance, but also should have access — if desired — to the rules governing other states that may collect their communications data. Note also that a norm of legality would alter the nature of much current surveillance activity. Much of today's activity is an "unknown unknown"[249] — citizens do not know whether foreign surveillance is taking place, let alone what the rules are (if any) for such surveillance. This new norm would convert government surveillance from an action that takes place in deep secrecy to an action that occurs in shallow secrecy.[250] The norm of legality would shift surveillance to a "known unknown," where potential surveillance targets would be on greater notice that they might be subject to surveillance, but would not know in any particular case whether a state actually was monitoring their communications.

States are beginning to enact specific laws (or policies) authorizing purely extraterritorial intelligence collection and defining its parameters.[251] German law allows the German intelligence services to gather information about other countries that is important to the foreign and national security policy of Germany, at least some of which presumably happens extraterritorially.[252] In Italy, the law authorizes its intelligence community

247. *Id.* at 192 ¶ 8.

248. Special Rapporteur Report, *supra* note 171, ¶ 50; *see also* Owen Bowcott & James Ball, *Social Media Mass Surveillance Is Permitted by Law, Says Top UK Official*, GUARDIAN, June 17, 2014, http://www.theguardian.com/world/2014/jun/17/mass-surveillance-social-media-permitted-uk-law-charles-farr (stating that U.K. government interpreted domestic surveillance law in manner unknown to Parliament).

249. Donald H. Rumsfeld, Sec'y, Dep't of Def., DoD News Briefing (Feb. 12, 2002) (transcript available at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636) (coining the phrase).

250. David E. Pozen, *Deep Secrecy*, 62 STAN. L. REV. 257, 260 (2010).

251. Special Rapporteur Report, *supra* note 171, ¶ 64.

252. Christopher Wolf, Testimony Before the Privacy & Civil Liberties Oversight Board: A Transnational Perspective on Section 702 of the Foreign Intelligence Surveillance Act 11–12 (Mar.

to collect information so as to "protect the independence, integrity and security of the Republic . . . against threats originating abroad,"[253] which implies an authorization to engage in overseas surveillance. Indeed, the mere existence of an "external" security agency suggests that overseas activities are within its remit. Yet most states' domestic laws provide far more information about and structure for domestic and transnational surveillance than they do for purely extraterritorial activity.

The United States embraced the "legality" principle in Presidential Policy Directive 28. That Directive states, "The collection of signals intelligence shall be authorized by statute or Executive Order" and must be undertaken in accordance with U.S. law.[254] The list of purposes for which the United States can conduct bulk intelligence acquisition shall be kept public to the maximum extent feasible, consistent with national security.[255] In *Weber*, the ECtHR deemed it essential that Germany's law authorizing strategic interception contained detailed rules that were clear enough to give a citizen "adequate indication" of the circumstances and conditions under which the government may resort to measures of surveillance.[256] For the ECtHR, that meant that the statute must specify, *inter alia*, "the nature of the offences which may give rise to an interception order [and] a definition of the categories of people liable to have their telephones tapped."[257]

States adhering to this principle must walk a fine line. On the one hand, states likely would agree that it is appropriate for domestic laws to provide some level of detail about the categories of activity that could be subject to surveillance. However, embedding "foreseeability" into a law does not (and should not) require the state to provide a "self-defeating form of notification."[258] Without basic knowledge of programs, though, the citizenry cannot debate activities conducted in its name. Further, clarity

---

19, 2014), *available at* https://www.pclob.gov/library/20140319-Testimony-Wolf.pdf; *Germany's Surveillance Policies*, PRIVACY INT'L, https://www.privacyinternational.org/reports/germany/ii-surveillance-policies (last visited Oct. 16, 2014) (stating that Germany's "G-10 Law allows warrantless automated wiretaps of domestic and international communications by [both federal and state authorities] for purposes of protecting the freedom and the democratic order, preventing terrorism and illegal trade in drugs and weapons"); *see also* ALBERT J. MARCELLA, JR. & CAROL STUCKI, PRIVACY HANDBOOK: GUIDELINES, EXPOSURES, POLICY IMPLEMENTATION, AND INTERNATIONAL ISSUES 92 (2003) (summarizing some German jurisprudence on the G-10 Law).

253. Wolf, *supra* note 252, at 12 (translating Legge 3 agosto 2007, n. 124, art. 6 (It.)).

254. *PPD-28*, *supra* note 147, § 1(a); *see also* Exec. Order No. 12,333, 3 C.F.R. 200, § 2.8 (1982), *reprinted as amended in* 50 U.S.C. § 401 note (2012) ("Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States.").

255. *PPD-28*, *supra* note 147, § 2.

256. Weber & Saravia v. Germany, 2006-XI Eur. Ct. H.R. 309, 335 ¶ 93.

257. *Id.* at 336 ¶ 95.

258. CDT REPORT, *supra* note 157, at 34.

about the law reveals the nature and extent of safeguards against abuse and helps the public assess whether those safeguards are working effectively.

2. Limits on Reasons to Collect or Query Data

Most states would agree that there should be some limits on the substantive reasons that states may collect electronic surveillance ("collection limits"), or at least on the types of inquiries states may make of the data they have collected ("use limits"). It is far easier to forecast that states would agree to the fact there should be some collection or use limits than to forecast what states would agree those limits should be. U.S., German, and Swedish laws suggest ways that states can limit the use of surveillance data to a fixed list of objectives.[259] The United States, for example, has stated that it will use metadata it has collected only to detect and counter espionage and other activities directed by foreign powers against U.S. interests, terrorist threats, proliferation of weapons of mass destruction (WMDs), cyber threats, threats to U.S. or allied forces, and transnational criminal threats.[260] Sweden's law limits the collection of data content (as opposed to metadata) to a robust but clear set of purposes:

259. For the United States, see *PPD-28*, *supra* note 147, § 2; Exec. Order 12,333, § 1.1(d) (authorizing broad uses for surveillance but requiring the intelligence community to place "special emphasis" on detecting and countering espionage, terrorism, and the development, possession, proliferation, or use of weapons of mass destruction). For Germany, see Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz [G-10] [G-10 Statute], June 26, 2001, Bundesgesetzblatt I. [BGBl. I] 1254, 2298, as amended, § 5(1) (listing reasons that German intelligence may conduct strategic, warrantless surveillance of telephonic and Internet lines: the risk of an armed attack on Germany; the commission of international terrorist acts with a direct relation to Germany; international weapons or drug trafficking; or certain cases of counterfeiting and money laundering); Paul M. Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, 2 INT'L DATA PRIVACY L. 289 (2012); PRIVACY INT'L, *supra* note 252; *Weber*, 2006-XI Eur. Ct. H.R. at 321 ¶ 27. For Sweden, see Klamberg, *supra* note 158.

260. *PPD-28*, *supra* note 147, § 2. The FISA, as amended, authorizes the Executive Branch to conduct surveillance without a warrant on foreign persons reasonably believed to be outside the United States, in order to acquire information relating to the U.S. government's ability to protect against actual or potential attacks or other grave hostile acts by a foreign power or its agent; sabotage, international terrorism, or international proliferation of WMDs by a foreign power or its agent; clandestine intelligence activities; or information with respect to a foreign power or foreign territory that relates to the national defense or national security of the United States or its conduct of foreign affairs. 50 U.S.C. §§ 1801(e), 1881a (2012 & Supp. I 2013). Executive Order No. 12,333, which applies in those cases in which the United States conducts surveillance entirely overseas and no U.S. person is involved in the communications, allows a broader range of collection, including the acquisition of significant foreign intelligence (defined as information related to the capabilities, intentions, and activities of foreign powers, organizations, or persons), and the detection and countering of international terrorist activities and espionage conducted by foreign powers. Exec. Order No. 12,333, §§ 2.2, 3.5(e). Obviously the United States would need to consider whether it is willing to streamline and provide greater detail about categories of data to be collected (or examined from within bulk collection).

external military threats, peacekeeping-related information, international terrorism and organized crime, proliferation of WMDs, external threats against infrastructure, conflicts outside Sweden that affect international peace and security, counter-intelligence, and actions and aims of foreign powers of material interest for Swedish foreign, security, and defense policy.[261] An important question for states is whether they could agree to create either collection or use limits based on a detailed list of issues such as Sweden's or Germany's, rather than leaving the limits in broad terms such as "information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons"[262] — a concept so broad as to be virtually limitless.[263]

Rather than focus on what collection is permitted, states also could decide to deem specific types of communications to be prohibited from use. As noted above, the ICJ has before it a case in which Timor-Leste alleges that Australia raided the offices of its Australian attorney and seized documents and other items that implicated Australia in bugging Timor-Leste's internal discussions about a treaty negotiation.[264] An ICJ decision in favor of Timor-Leste might contribute to the development of a norm limiting the use of foreign espionage by establishing that there is a use prohibition on a foreign state's gaining access to another state's attorney-client discussions related to peaceful settlements of disputes. Germany's constitutional court already has expressed concern about state access to private attorney-client discussions.[265] The NSA has indicated that it takes particular precautions to ensure that, when collected, such conversations may not be disseminated unless reviewed by NSA's General Counsel's office; in the criminal context, NSA and DOJ protect such conversations from use in criminal prosecutions.[266] Collectively, this activity may foster the development of a norm that offers special protections against the exploitation of attorney-client communications.

---

261. Klamberg, *supra* note 158.

262. Exec. Order No. 12,333, § 2.1.

263. While the other five norms in this Subpart are almost entirely procedural in nature, this norm could have substantive aspects. States simply could agree that as a procedural matter their laws must establish and publicize a list of permissible reasons to conduct foreign surveillance, without harmonizing their lists. Alternatively, states could agree on substantive types of surveillance-worthy targets (or queries).

264. *See* Deeks, *ICJ on the Merits*, *supra* note 176; Deeks, *Will the ICJ Decide*, *supra* note 176.

265. Schwartz, *supra* note 259, at 293–94.

266. Letter from Keith B. Alexander, Dir., Nat'l Sec. Agency, to James R. Silkenat, President, Am. Bar Ass'n (Mar. 10, 2014), *available at* https://www.aclu.org/files/natsec/nsa/Alexander%20ABA%20Response.pdf; Poitras et al., *supra* note 140 (describing GCHQ assertion that its interception "is categorically not about industrial espionage" (internal quotation marks omitted)).

Another substantive area in which the United States and United Kingdom appear to support use limits is intelligence about foreign companies to share with domestic companies, to provide the latter with economic advantages.[267] At the same time, the United Kingdom and United States conduct espionage against economic targets to enforce sanctions regimes and detect bribery that may disadvantage their domestic industries. This is a relatively fine line to draw and one that seems increasingly hard to defend.[268] Jack Goldsmith suggests that states such as China and France will be unreceptive to an approach that prohibits economic espionage to advantage domestic industry, because both states conduct extensive economic espionage to aid such industries and see limited distinctions between economic and military security.[269] Indeed, French law permits interceptions to protect France's "economic and scientific potential,"[270] which suggests that France may be loath to forego industrial collection opportunities.[271]

Many human rights and civil liberties groups have called for a reduction in the quantity of information that is collected and held by governments — that is, collection limits, not just use limits. It likely will be more technologically difficult for states to adhere to collection limits than to adhere to use limits, however.[272] States seem committed to the idea that they require access to as much data as possible to accurately locate terrorist

267. Obama NSA Speech, *supra* note 1 ("We do not collect intelligence to provide a competitive advantage to U.S. companies or U.S. commercial sectors."); *see also PPD-28*, *supra* note 147, § 1(c).

268. David E. Sanger, *Fine Line Seen in U.S. Spying on Companies*, N.Y. TIMES, May 20, 2014, www.nytimes.com/2014/05/21/business/us-snooping-on-companies-cited-by-china.html (noting that although the United States does not directly share economic intelligence with U.S. corporations, it uses that intelligence to advance U.S. trade interests in state-to-state negotiations).

269. Jack Goldsmith, *On French Espionage*, LAWFARE (July 5, 2013, 7:38 AM), http://www.lawfareblog.com/2013/07/on-french-espionage/ (describing France as leader in conducting industrial espionage); Jack Goldsmith, *Why the USG Complaints Against Chinese Economic Cyber-Snooping Are So Weak*, LAWFARE (Mar. 25, 2013, 9:01 AM), http://www.lawfareblog.com/2013/03/why-the-usg-complaints-against-chinese-economic-cyber-snooping-are-so-weak/; David Sanger, *Differences on Cybertheft Complicate China Talks*, N.Y. TIMES, July 10, 2013, http://www.nytimes.com/2013/07/11/world/asia/differences-on-cybertheft-complicate-china-talks.html.

270. Wolf, *supra* note 252, at 11 (quoting 1991 legislation codified in the Internal Security Code) (internal quotation marks omitted).

271. *Id.* at 13 (describing Italy's national surveillance law as allowing collection to protect Italy's economic, scientific, and industrial interests).

272. Witness Statement of Charles Blandford Farr, Privacy Int'l v. United Kingdom, Case No. IPT/13/92/CH, ¶ 149 (Investigatory Powers Trib. 2014) (U.K.) ("[I]t will be apparent that the only practical way in which the Government can ensure that it is able to obtain at least a fraction of the type of communication in which it is interested is to provide for the interception of a large volume of communications, and the subsequent selection of a small fraction of those communications for examination by the application of relevant selectors.").

plots and connections among suspected terrorists, among other threats.[273] President Obama's proposed changes to the Section 215 metadata collection program admittedly show a softening on this front. Those changes would halt metadata collection by the U.S. government, but allow it to continue to use that data, albeit on an inquiry-by-inquiry approach to the companies that hold the data. In short, norms formed to limit the subjects of electronic surveillance should focus on the uses to which governments may put available data (whether held by themselves or by telecoms and ISPs), rather than attempt to limit the collection of data *ex ante*.[274] Several other principles in this section also focus on ways that governments may limit the use of information rather than its initial collection. This is consistent, for instance, with the approach some U.S. courts have taken to the Fourth Amendment; for them, a search (and therefore an infringement on privacy) occurs when information is exposed to possible human observation, rather than when it is copied or processed by a computer.[275]

Three principles may be interwoven with the development of a norm on collection or use limitations: (1) the idea that collecting metadata is less intrusive than collecting the contents of those communications;[276] (2) the idea that bulk collection of data is less privacy-intrusive than the targeting of individual communications;[277] and (3) the sense that targeted surveillance by State A that captures the communications of foreign "ordinary citizens" warrants greater oversight (or more stringent restrictions) than A's surveillance of State B's government officials and activities. The third principle might manifest itself in a norm that

273. ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *vacated* No. 14–42–CV, 2015 WL 2097814 (2d Cir. May 7, 2015) ("The [U.S.] Government . . . launched a number of counter-measures, including a bulk telephony metadata collection program — a wide net that could find and isolate gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data. This blunt tool works only because it collects everything.").

274. Groups such as the ACLU object to the fact that the government holds the data, but it is not clear from the laws examined that states other than the United States currently are sensitive to this concern.

275. In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014). *Cf.* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013) (concluding that any search of bulk metadata is a search of any particular person's metadata); *see also* Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 555 (2005).

276. CDT REPORT, *supra* note 157, at 27 (noting that Australia, Canada, Germany, the United Kingdom, and the United States, among others, make a legal distinction between data content and metadata, with the governments having to meet higher standards to access the former).

277. David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach*, LAWFARE (May 20, 2013, 9:00 AM), http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-approach/ (asking whether U.S. laws should distinguish normatively between collection that targets a specific person and bulk collection, the former of which may be more intrusive).

establishes more limited reasons for which a state may conduct targeted foreign surveillance on non-governmental officials than for which it may pursue the communications of foreign leaders or state officials.[278]

3. Periodic Review of Surveillance Authorization

Virtually all of the states whose domestic laws I reviewed permit surveillance only for limited initial time periods, though those periods generally are subject to renewal after 30 to 180 days.[279] This ensures that some state actor periodically reviews whether the surveillance remains appropriate, and precludes — at least formally — indefinite surveillance of a particular target. This norm also might include annual reviews of surveillance targets generally, to ensure that states are not unnecessarily or inappropriately surveilling categories of people.[280] This norm means that the state must continue to make its case that an individual or entity meets the statutory targeting standards.[281] Such a norm also furthers state interests, by ensuring that state resources remain dedicated to situations that are producing important information about terrorism, espionage, or other national security issues, rather than pursuing stale or unfruitful leads.

4. Limits on Retention of Data

France's laws require telecom and "hosting" providers in France to collect and retain for one year information revealing the identity of people storing data on the Internet, including their email addresses, login information, and connections to their data.[282] Similarly, in Italy and Spain, telecommunications providers must retain electronic telecommunications data for one year.[283] The law is silent on the length of time the French

278. A possible parallel is the ECtHR case law on freedom of expression. That court has held that public figures must be willing to tolerate wider criticism than the average citizen. Lingens v. Austria, 103 Eur. Ct. H.R. 14, 26 ¶ 42 (1986).

279. *See, e.g.*, Regulation of Investigatory Powers Act, 2000, c. 23, § 9(6) (U.K.) (depending on type of warrant, renewal after five days, three months, or six months); *Australian Security Intelligence Organisation Act 1979* (Cth) s 25A(6)–(7) (six-month duration); Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23, § 21(5) (depending on type of case, sixty days or one year); 50 U.S.C. § 1881a (one year for surveilling foreign persons reasonably believed to be outside the United States); *id.* § 1805(d)(1) (three months, four months, or one year, depending on target); *see also* Ass'n for Eur. Integration and Human Rights v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R., Judgment, ¶ 76 (2007), *available at* http://hudoc.echr.coe.int (requiring that state establish limits on duration of monitoring).

280. *See, e.g.*, *PPD-28*, *supra* note 147 (requiring the Executive to review its intelligence priorities and sensitive targets annually at a senior level).

281. *See, e.g.*, USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287–88 (2001) (requiring 90-day reviews of telephonic metadata collection associated with several foreign terrorist organizations by the Foreign Intelligence Surveillance Court).

282. Wolf, *supra* note 252, at 11.

283. *Id.* at 13.

government may retain data it collects or otherwise obtains, however. President Obama recently proposed a procedure whereby U.S. telecommunications carriers would not be required to retain their data for any longer than they normally do.[284] Intelligence officials reportedly acknowledge that "the operational impact of that change would be small because older data is less important."[285] PPD-28 also states, "Personal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons."[286]

The European Court of Justice recently struck down the EU Data Retention Directive, which required member states to ensure that telecommunications and ISPs retain data (including the source and destination of communications and cell phone location data) for not less than six months and not more than two years.[287] Its holding seems to require that any revised European directive must demonstrate greater tailoring between the type of activity under surveillance and the length of time that states may require telecommunications and data companies to retain data related to that activity.[288] Whether this will affect the length of time that states choose to retain data in their possession (rather than in the hands of companies) remains an open question. But if states conclude that the length of time service providers retain data is sufficient for national security purposes, they should modify their own retention limits accordingly.

5. Preference for Domestic Action

Another principle around which states should coalesce is a preference for surveillance by the state in which suspicious activities by non-governmental actors are taking place. That is, when an individual is planning terrorist acts or attempting to proliferate WMDs, the state in which that individual is located is — at least theoretically — the best suited to gather intelligence on his activities. The preference assumes three

284. Federal regulations only require that telecommunications carriers retain that data for eighteen months. The NSA currently retains the phone data it obtains from those carriers under Section 215 of the PATRIOT Act for five years. Charlie Savage, *Obama to Call for End to N.S.A.'s Bulk Data Collection*, N.Y. TIMES, Mar. 24, 2014, http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?_r=0.

285. *Id.*

286. *PPD-28*, *supra* note 147, § 4(a).

287. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd. v. Ireland (Apr. 8, 2014), *available at* http://curia.europa.eu. The Directive (2006/24) applied to all data involving fixed telephony, mobile telephony, Internet access, Internet e-mail, and Internet telephony. *Id.* ¶ 56.

288. *Id.* ¶ 62 (finding that Directive does not limit data retention to what is strictly necessary).

things, however. First, it assumes that the territorial state has adequate capacity to engage in the necessary surveillance and is willing to share that intelligence with one or more other states. Second, it assumes that the territorial state is not involved in the bad acts; in many cases, a surveilling state conducts electronic surveillance against the territorial state's officials because those officials themselves are engaged in activities that pose national security threats to the surveilling state. Third, from a human rights perspective, it assumes that the territorial state has reasonably robust domestic laws that protect the target's privacy and other rights. After all, that is the advantage to establishing such a preference: It relies on the fact that most states regulate more stringently the surveillance of those in their territory than those outside it.

Lurking in the background of discussions of espionage is the fact that the domestic laws of many states criminalize the act of spying when conducted on their territory.[289] States parties to the Council of Europe Cybercrime Convention also have an obligation to enact laws criminalizing access to a computer system without right and the technical interception without right of non-public transmissions of data within a computer system.[290] These facts strengthen the idea that State A should prefer for State B to undertake domestic surveillance of targets on the territory of State B whenever possible. By doing so, State A thus will limit the criminal exposure of its officials. That said, the strength of State A's preference may not be particularly robust, because it often will be difficult for State B to prosecute foreign officials who have conducted espionage on State B's territory. This is because those foreign officials often never set foot in State B and because of the attribution problems discussed above.[291]

The evolution of such a norm would have an added benefit. One frequent complaint by human rights and civil liberties groups is that State A is obtaining intelligence from State B on State A's own citizens, collected in a way that State A could not have gathered it directly.[292] A preference

289. This asymmetry likely will remain, even if states adopt international norms of the kind discussed in this Subpart. States are almost certain to retain domestic laws that criminalize spying by foreign agents, even if the international norms they adopt treat spying more sympathetically.

290. Council of Europe Convention on Cybercrime arts. 2–3, *opened for signature* Nov. 23, 2001, E.T.S. No. 185.

291. *See supra* Part I.C. On attribution, see Scott J. Shackelford, *Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1299 (2013) ("In 2011, the DoD admitted to losing some 24,000 files to cyberespionage. But the responsible spies are often not being punished. Instead, they remain at large due in part to problems of attribution and extradition." (footnotes omitted)).

292. Estelle Shirbon, *Europe's Spies Work Together on Mass Surveillance: Guardian*, REUTERS, Nov. 2, 2013, *available at* http://www.reuters.com/article/2013/11/02/us-europe-surveillance-idUSBRE9A103K20131102 ("GCHQ files leaked by Snowden showed the British agency taking credit for advising European counterparts on how to get around domestic laws intended to restrict

for domestic collection would reduce the number of situations in which it either appears to be — or is in fact — the case that one state has obtained information about its citizens from an ally that is not bound by the same collection laws that the first state is. In other words, it increases the opportunities for compliance with domestic law and reduces the opportunities for non-compliance.[293]

This approach carries shades of a necessity or exhaustion requirement, something that appears in the limited human rights jurisprudence on surveillance. Many domestic laws embed a requirement that the official authorizing surveillance determine that such surveillance is necessary and that there is no less intrusive way to collect the intelligence.[294] Although surveillance by the territorial state is not necessarily less intrusive than surveillance by the foreign state as a practical matter, the former may be more stringently regulated and thus less intrusive as a legal matter.

6. Neutral Oversight Bodies

One critical aspect of operating an intelligence community is having actors outside the chain of command of that community who can provide independent oversight.[295] By definition, the public cannot serve as a direct watchdog, because so much of the community's activities happen in secret. Independent actors may take various forms: parliamentary bodies, respected third-party actors appointed by the head of government, inspectors general, or courts. Such bodies might act *ex ante*, as gatekeepers authorizing surveillance before it occurs, or *ex post*, providing either broad or detailed oversight over a state's foreign surveillance practices or serving as a place for the public to lodge complaints about unlawful surveillance.[296]

---

their surveillance powers."). Executive Order 12,333, § 2.12, specifically prohibits U.S. intelligence agencies from asking other governments to engage in intelligence collection that the agencies themselves could not conduct. Exec. Order No. 12,333, 3 C.F.R. 200, § 2.12 (1982), *reprinted as amended in* 50 U.S.C. § 401 note (2012).

293. *See* Declaration of Rajesh Jha at 5, ¶ 10, In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., Nos. M9–150, 13–MJ–2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) ("[M]any of our partners and enterprise customers . . . see the U.S. government's unilateral approach to obtaining private data in this case as a threat to the privacy and protection of enterprise data as well. This concern is greatly reduced when the U.S. government is perceived to be acting in cooperation with their counterparts in other governments (thereby ensuring local enterprises that they remain entitled to the privacy and procedural protections of their own governments).").

294. Pitter, *supra* note 8, at 11.

295. In *Klass v. Germany*, which dealt with the targeted surveillance provisions of Germany's G-10 law, the ECtHR required oversight by an independent entity. Klass v. Germany, 28 Eur. Ct. H.R. (ser. A) at 26 ¶ 56 (1978).

296. The recent UNGA privacy resolution calls on states to establish independent, effective oversight mechanisms capable of ensuring transparency and accountability of state surveillance of communications. The Right to Privacy in the Digital Age, *supra* note 47, ¶ 4(d).

What is important is that the oversight is sufficiently removed (in terms of political pressure and chain of command) from the actors being overseen.

The laws of each state examined provide at least one form of neutral oversight, and often several. In Germany, the Parliamentary Control Panel receives reports from intelligence agencies about their activities, and the G-10 Committee decides on the "permissibility and necessity" of intelligence agency surveillance, combining both *ex ante* and *ex post* review.[297] Australia's intelligence watchdog is the Inspector-General of Intelligence and Security, who both reviews intelligence agency activities and receives complaints from Australian citizens about surveillance.[298] The United States employs an intelligence community inspector general, an inspector general for each intelligence agency, two Congressional intelligence committees, and the Foreign Intelligence Surveillance Court.[299] Canada, Italy, France, the United Kingdom, and Sweden all have various forms of intelligence oversight.[300] In each case, the overseers are granted extensive access to classified information and activities. Non-legislative overseers tend to report to the highest actor in the government. Legislative overseers generally have the power of subpoena, though their mandates sometimes are cabined.

The laws of some of the states examined suggest that it is possible that states will adopt a norm ensuring that foreign nationals may submit allegations of unlawful surveillance either to a regular court or a specific tribunal. The United Kingdom's Investigatory Powers Tribunal receives individual complaints about the legality of particular GCHQ actions, with no limitation on the nationality of the complainant.[301] The United States

297. Wolf, *supra* note 252, at 12 (citation omitted) (internal quotation marks omitted).

298. *Inspector-General of Intelligence and Security Act 1986* (Cth) s 8 (Austl.).

299. *See* Joel Brenner, *Power, Secrecy, and Intelligence Oversight*, LAWFARE (June 11, 2013, 8:22 AM), http://www.lawfareblog.com/2013/06/power-secrecy-and-intelligence-oversight/ (arguing that NSA has robust internal and external compliance mechanisms, including in the form of House and Senate intelligence committees, the Justice Department, and the Inspector General).

300. The Security Intelligence Committee reviews CSIS's activities in Canada. Wolf, *supra* note 252, at 10. Italy has a parliamentary committee (COPASIR) that is supposed to ensure that the internal and external security agencies operate in accordance with Italian law. *Id.* at 12. In France, the Prime Minister's authorizations of targeted interception are presented to a "special security commission" that can evaluate the justification for the warrant. *Id.* at 11. Sweden has a Defense Intelligence Court that authorizes data collection after an application from Sweden's signals intelligence agencies. Elizabeth Pond, *What the NSA Can Learn from Sweden*, WORLD POLICY BLOG (Aug. 9, 2013, 11:31 AM), http://www.worldpolicy.org/blog/2013/08/09/what-nsa-can-learn-sweden. The United Kingdom has established an Investigatory Powers Tribunal, made up of nine senior members from the legal field, which has jurisdiction to hear complaints under the Regulation of Investigatory Powers Act. It also has an Interception of Communications Commissioner who reviews the government's compliance with RIPA, and an Intelligence and Security Committee in Parliament that has access to highly classified material and oversees the government's operational intelligence activities. Wolf, *supra* note 252, at 14.

301. Regulation of Investigatory Powers Act, 2000, c. 23, § 65.

allows domestic courts to hear direct challenges by individuals who suspect that they have been subject to unlawful surveillance, if they can show that they have standing.[302] (Australia's Inspector-General of Intelligence and Security accepts complaints against the Australian Signals Directorate (Australia's NSA equivalent), albeit only from its citizens.) However, other states might view such bodies with skepticism, as likely to require them to expend substantial resources in preparing responses to a large number of complaints in a way that protects classified information, and possibly to create domestic causes of action and remedies for foreign nationals.

C. Possible Critiques and Responses

1. Unduly Weak Norms

These rules, taken collectively, are unlikely to satisfy human rights or civil liberties advocates, who undoubtedly will pressure states to agree to more protective steps than those just described. For instance, a large group of NGOs supports the International Principles on the Application of Human Rights to Communications Surveillance, which assert that for foreign surveillance to be compatible with human rights, individuals must have the ability to challenge surveillance laws; "[d]eterminations related to Communications Surveillance must be made by a competent judicial authority"; individuals "should be notified of a decision authorising Communications Surveillance . . . [unless doing so] would seriously jeopardize the purpose for . . . [the] Surveillance" (and in any case should be notified by the time the surveillance ends); and "States should not compel service providers . . . to collect or retain particular information purely for State Communications Surveillance purposes."[303]

These groups may conclude that these six norms are thin gruel, a useful starting point but in no way an end point.[304] These norms would not provide that a court must, in each instance, issue a warrant before the government may collect intelligence on a foreign individual or entity. The norms would not require that a state treat foreign nationals the same way that it treats its own citizens. Nor would they require states to provide

---

302. The United States repeatedly has objected on "state secrets" and standing grounds to judicial review of cases challenging NSA surveillance. *See, e.g.*, ACLU v. NSA, 493 F.3d 644 (6th Cir. 2011) (standing); Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190 (9th Cir. 2008) (state secrets).

303. NECESSARY & PROPORTIONATE, *Principles*, *supra* note 3; *see also* ACLU, *supra* note 3 (arguing for similar principles).

304. *See, e.g.*, Special Rapporteur Report, *supra* note 171, ¶¶ 82–90 (recommending that surveillance should occur only under the most exceptional circumstances; that individuals should have a right to notice after the fact of surveillance against them and the ability to seek redress for the unlawful use of such measures; and that "States should not retain . . . particular information purely for surveillance purposes").

notice to individuals after the surveillance was complete, or to establish fora in which foreign nationals might complain about being subjected to unlawful surveillance.

While some of these proposals seem worth aspiring to, few of these concepts currently appear in states' domestic laws. (It is possible that certain states will alter their domestic laws to reflect the types of changes the rights groups seek.) Although these proposals surely will influence actors who serve within the UN system or on treaty bodies such as the Human Rights Committee, the purpose of this Part is to focus on the existing laws of states, identify points of similarity, and, from there, extract basic international norms around which states could and should coalesce in the near term. Further, most of the norms discussed here find an affinity in a subset of the principles promoted by these groups.[305] And many of the six norms are aimed at rendering the conduct of foreign surveillance and the handling of data duly proportional to the threat faced by states. Proportionality has proven an important notion for the Human Rights Committee and the ECtHR in evaluating measures that implicate privacy.[306] Further, the fact that states realistically might accept the proposed norms makes them more normatively appealing, particularly where states representing a significant percentage of electronic surveillance capabilities adhere to the norms and those states are committed to legal compliance.

A related concern is that states might establish these norms at an overly high level of generality. If so, states could interpret the norms in such a way that the norms fail to provide much actual restraint on state action. One might argue that it is worse for states to be able to point to modest foreign surveillance regulations — and thus alleviate some pressure on themselves while making few changes in practice — than to continue with the unregulated *status quo*, which forces states to defend their practices more robustly on the merits. But customary norms often exist at a relatively high level of generality, and their existence gives leverage to critics of state surveillance to press for greater restraint.

2. Public Adherence/Private Noncompliance

There is a danger that states will adopt these norms publicly but continue to conduct foreign surveillance much as they do today. Because it may be relatively difficult to ascertain whether states actually are complying

---

305. *See, e.g.*, NECESSARY & PROPORTIONATE, *Principles*, *supra* note 3 (supporting principles of legality, legitimacy, and limited aims of surveillance, transparency, oversight mechanisms, and destruction of data after use).

306. *See* Milanovic, *supra* note 2 (manuscript at 66, 70–71).

with some of the six norms, there is ample room for a hypocritical embrace of the norms without a corresponding change in behavior. Two factors potentially mitigate this concern. The first is that many Western (and some non-Western) states refuse to adopt international norms publicly unless they genuinely plan to comply with them.[307] In this view, formally accepting international rules without the intention or ability to comply with them serves to weaken, not strengthen, the international regime. Where these states view the international rules at issue as beneficial, they view their ability to comply with those rules as a *sine qua non* for formally adopting them in the first place. The second mitigating factor is that public revelations about surveillance programs are on the rise. As a result, non-compliance with stated norms is more likely to come to light. In democracies, non-compliance with publicly accepted norms is more costly to states, whose publics are accustomed to holding their governments to the laws they have adopted. Citizens are more likely to call for compliance with domestic laws than international laws, yet most states have a contingent of elites who seek to hold their governments accountable for international legal compliance as well.

3. Undue Protections for Foreigners

I argue above that it is reasonable to expect that new norms offering increased procedural protections to foreign nationals will evolve from norms regulating domestic and transnational surveillance. Opponents of extraterritorial regulation will raise at least three objections. The first is that foreign nationals do not deserve the same levels of protection that nationals do.[308] The second is that states simply have fewer tools to use overseas to detect and thwart threats than they do domestically, and so must preserve additional flexibility to conduct surveillance abroad. The third is that the volume of purely extraterritorial surveillance is much greater than that which occurs domestically against foreign nationals. In this view, regulations that apply to extraterritorial surveillance will prove unduly onerous for state intelligence services.

As to the first and second issues, the communications of some foreign nationals already incidentally receive some procedural protections, particularly when those communications either occur within the surveilling state or involve the surveilling state's nationals on one side of the

307. *See, e.g.*, John Bellinger, Legal Adviser, U.S. Dep't of State, Remarks at the Hague: The United States and International Law (June 6, 2007), *available at* http://2001-2009.state.gov/s/l/2007/112666.htm (explaining why the U.S. government will not adhere to a treaty unless and until it is confident that it can comply with its obligations).

308. *See, e.g.*, Kerr, *A Reply to David Cole*, *supra* note 245.

communication. In the United States, for instance, those types of foreign national communications are subject to statutory regulation and judicial oversight by the Foreign Intelligence Surveillance Court. Some of these protections are incidental, and are less robust than those accorded to a state's own nationals. But the fact is that the laws of virtually all of the states discussed above accord protections to foreign nationals in certain circumstances now. The norms proposed would allow states to retain a distinction between domestic and foreign surveillance requirements; they simply would narrow that distinction in ways that should be manageable for states.

This leads to the third objection: an undue burden on intelligence collection. The norms surely would require increased state efforts on the front end, as the intelligence communities re-orient their operations and regulations and make technological adjustments to their collection processes. And where states must devote limited resources to implement a wider range of protections, they might have fewer resources to devote toward protecting the privacy of their own nationals. The norms discussed above, however, are unlikely to significantly increase the workload of the intelligence community. The concept of legality simply means that the rules are made more transparent in advance. Limits on the purposes of collection would decrease the scope of what currently is collected or queried, at least with regard to adhering states. Limits on retention of data affect the date by which data must be destroyed, but the workload would remain unchanged. Preference for action by partner states might actually decrease the collectors' workload, though it could increase the need for ongoing coordination among allies' intelligence agencies. Neutral oversight bodies admittedly would be required to oversee a greater scope of activity (by adding extraterritorial surveillance in adhering states to their current mandates of domestic and transnational surveillance), which would increase their workload. On balance, however, these burdens appear manageable.

4. State Preference for Flexibility

Finally, even if one is persuaded that states will self-regulate their surveillance practices, one might conclude that such regulation will take a purely domestic form. Altering domestic surveillance laws preserves greater flexibility to amend those laws if an event such as a major terrorist attack were to occur. Reaching an agreed set of norms on the international plane makes the norms stickier, and thus harder to revisit if states conclude that they require greater flexibility to respond to new threats. States also might conclude that the emerging human rights approach to surveillance fails sufficiently to take account of real security risks and the

need to respond nimbly as technology and threats change. As a result, states might be inclined to limit the amount of surveillance regulation that occurs on the international plane, so as not to provide added credibility to those who believe that the issue implicates international human rights. After all, enshrining greater procedures and tighter standards in domestic laws alone still would allow states to advance the "rule of law" criteria noted above. In this critique, even if Western states develop shared standards or memoranda of understanding, they may emphasize in these documents that the agreed norms do not constitute treaty commitments and that states retain the authority to modify them quickly, in an effort to minimize, rather than increase, the sense of *opinio juris*.

Whether one agrees with this critique depends on one's views of the strength of pressure on states from UN bodies and human rights groups, which seek to internationalize the issue; the quantum of benefits states think they will accrue by adopting norms multilaterally rather than unilaterally; and the importance of harmonizing surveillance approaches to ensure continued intelligence sharing among allies. These factors are, to some extent, unknowable: The outcome depends on the level of commitment of human rights advocates; the amount of pressure that the Snowden revelations have placed on intelligence cooperation among NATO and other allies; and internal state information and deliberations that are not publicly accessible. This Article assumes, though, that the pressure from human rights and civil liberties bodies will be sustained, and that states will view the benefits of multilateral arrangements as sufficiently valuable to warrant accepting certain limitations on their flexibility.

CONCLUSION

The international community finds itself today at the intersection of two phenomena. On one hand, the past decade has witnessed the massive increase in the use of electronic communications among people all over the world, as a way to share information, express opinions, talk to friends and family, conduct business, and undertake all sorts of licit and illicit activities.[309] On the other hand, governments have increased their technological capabilities to plumb those electronic communications. Further, because non-state actors can pose significant security threats — particularly in the form of terrorism or proliferation of weapons of mass destruction — states believe that they must surveil not only communications by foreign governments, but also communications by

309. Special Rapporteur Report, *supra* note 171, ¶¶ 2, 13.

foreign private citizens. These communications flow seamlessly across international borders; the technical architecture of digital communications means that communications of interest to states are deeply intermingled with irrelevant communications of ordinary citizens. This poses a central dilemma for law and policy.

International law has a critical role to play in beginning to resolve this dilemma, and the pressures are there for it to do so. Adopting a number of procedural norms to regulate foreign surveillance would help states and their citizens begin to balance the competing equities of privacy and security in concrete and observable ways. This approach strikes a middle ground between the cynics, who are unduly optimistic in predicting that regulatory pressures will subside in short order, and those in the human rights and civil liberties communities who seem confident that states quickly will retreat from foreign electronic surveillance to a posture that is far more protective of individual privacy.

Even if states were to coalesce around the norms offered herein, the project is just starting. Many substantive questions remain unanswered: Should states treat bulk collection differently from collection on individual targets? Should states conclude that it is more permissible to collect on foreign officials, who presumably are on greater notice that they are engaged in matters of interest to other states, than to collect on average citizens? How wide a gap is acceptable between the treatment of the communications of a state's nationals and foreign nationals? And does it make sense to draw geographic distinctions about where data is collected, held, or reviewed, as contemporary approaches do? This Article has proposed a launching point for basic procedural norms of foreign surveillance. Conversations about these other thorny questions, many of which will occur as states flesh out the meaning of ICCPR Article 17, almost certainly will take far longer to resolve. For now, the sense — among governments, elites, and average citizens — that something must relieve the *non liquet* of foreign surveillance in international law means states should pursue basic norms that they can adopt, at a cost they believe they can bear.