Reconciling Extraterritorial Surveillance with International Privacy Rights: A Modest Framework

Rahul Srivastava†

† M.A. University of St. Andrews, 2019; J.D. candidate, Cornell Law School, 2022. This Note would not have possible without my mother, who always pushed me to pursue academic writing and research. This Note was borne out of conversations with Professor Victoria Pepper, who helped chisel my ideas throughout the drafting process. I am lucky to have relied on her background and expertise. The *Cornell International Law Journal* editors and associates were incredible; I am grateful for their insights and feedback. Finally, I want to thank the intelligence community around the world, whose work keeps us safe and once inspired a young boy's boundless curiosity.

54 Cornell Int'l L.J. 125 (2021)

Introduction

Edward Snowden's disclosures of the United States' surveillance programs produced an international outcry from citizens, human rights groups, and foreign governments. Beyond creating embarrassing conversations for American diplomats around the world, the disclosures had real-world consequences. Germany cancelled an intelligence collection agreement from 1968 with the United States and United Kingdom. The termination was directly a result of the disclosures and need to protect individual privacy.[1] More significantly, the Obama administration enacted Presidential Policy Directive-28 (PPD-28), making the United States the first country to give foreigners privacy protections from mass surveillance. Despite the change in American policy, both adversaries and allies of the U.S. continue to conduct unrestrained mass surveillance of foreigners. In the digital age, governments around the world pursue these policies to meet their national security needs.

Individuals across the world enjoy data privacy protections from industry but are simultaneously subject to surveillance from foreign governments. Countries conduct mass surveillance of foreigners, or extraterritorial surveillance,[2] as part of a country's signals intelligence (SIGINT) collection activity. Under international law, peacetime espionage broadly is likely lawful as no international agreement prohibits the practice and every country engages in the activity.[3] However, specific intelligence activities may implicate certain parts of international law. Nowhere is this more evident than in extraterritorial surveillance. In contrast to traditional peacetime espionage, extraterritorial surveillance involves blanket collection of personal information and everyday correspondences of entire populations or their subsets. There are two international agreements on human rights: The International Covenant for Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR). Both incorporate a universal right to privacy. However, extraterritorial surveillance intuitively goes against ideas of individual privacy. In a legal clash between these agreements and extraterritorial surveillance, the latter prevails. The ICCPR and UDHR are advisory, and many signatories, most notably the United States, do not think they have to follow the agreement outside their jurisdiction.

This Note aims to balance the national security imperative that warrants extraterritorial surveillance against the privacy rights included in the international human rights bundle. Furthermore, this Note proposes cre-

1. *See* David V. Gioe, *Tinker, Tailor, Leaker, Spy*, 129 THE NAT'L INTEREST 51, 56 (2014).

2. Governments collect bulk intelligence on foreigners living in other jurisdictions. Scholarship and press coverage use various terms that can be used interchangeably to describe the practice. Some of these terms include: foreign intelligence collection, SIGINT collection of foreigners, foreign intelligence surveillance, bulk surveillance of foreigners, and extraterritorial surveillance. This Note will uniformly use "extraterritorial surveillance."

3. *See* Matthew Reiley, *Transforming SIGINT to Fight Irregular Threats*, 25 AM. INTELLIGENCE J. 68, 68–72 (2007).

ating a two-tiered code of privacy protections for foreign individuals during extraterritorial surveillance. In a two-tiered system (Tiered Code), the lower tier (Tier I) will modestly restrain extraterritorial surveillance, while the higher tier (Tier II) will include suggestive protections that nations can adopt on a reciprocal basis. Crucially, this Note will use the Tiered Code to defend the viability of a multilateral agreement that places privacy restraints on extraterritorial surveillance—a discussion that is lacking in prevailing literature.

Tier I will include four provisions: (i) an express declaration that foreign intelligence collection that respects privacy is permissible; (ii) a transparent attribution of domestic law sources that permit foreign intelligence programs; (iii) narrowing the reasons for which collection is permitted; and (iv) limiting retention periods of collected data. A Tiered Code permitting extraterritorial surveillance but limited by privacy considerations will offer multiple benefits. First, expressly permitting a widespread practice will enhance the international legal order by providing clarity on a contested legal question and maintain respect for an internationally recognized human right. Second, asking governments to publish their domestic legal authority will create transparency about surveillance and provide a basis for robust policy debate. Third, restrictions on reasons for collection and length of storage will add to individual privacy while preserving national security imperatives.

Tier II will outline stronger and more specific restraints that countries may use as a basis for reciprocal agreements. Certainly, allies are more likely to enter into these agreements that grant stricter protections. For example, two countries can agree to surveillance standards similar to the ones offered for domestic constituents. This Note will introduce a stronger protection mechanism in Tier II, but a more exhaustive list of specific Tier II solutions will remain outside the scope of this Note.

The Tiered Code faces two major drawbacks that plague other proposals to restrain surveillance: (i) Authoritarian countries like China are unlikely to sign on to any privacy protections; and (ii) regulating intelligence agencies' clandestine programs will be difficult to enforce. Combined, these drawbacks can render any agreement moot and perhaps further undermine international law. Through the Tiered Code, this Note will tackle these concerns and argue for the viability of agreements in this arena.

Part I explains what extraterritorial surveillance is, how it's different from conventional espionage, and how the practice fares under international law. Notably, Part I explains that although extraterritorial surveillance implicates international privacy agreements, the agreements are inadequate tools to restrain surveillance. Part II discusses various solutions and why they do not adequately address the clash between surveillance and privacy. Part III introduces the Tiered Code, articulates Tier I's provisions, and defends potential drawbacks that would impact the Code or any multilateral agreement.

I. Peacetime Espionage, SIGINT and Extraterritorial Surveillance

A. What is Peacetime Espionage, SIGINT Collection, and Extraterritorial Surveillance?

Peacetime espionage consists of the methods countries use to obtain confidential information from other countries.[4] Usually, this information includes ". . . political strategies, economic ambitions, and military capabilities . . . ."[5] Signals intelligence, or SIGINT, is a tool that helps countries conduct peacetime espionage. The National Security Agency (NSA), responsible for SIGINT collection in the United States, defines SIGINT as "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems."[6]

Although espionage is often called the world's "second-oldest profession," SIGINT collection became a national security priority during World War I.[7] Countries began protecting SIGINT infrastructure such as telegraph stations and employed codebreakers and radio interceptors.[8] Modern SIGINT collection began during the Cold War, when countries began dealing with information "often trivial in quality and overwhelming in quantity."[9] Today, SIGINT includes the controversial surveillance programs that intercept, store, and analyze various communications between private individuals. For example, the NSA collected 534 million phone calls and text messages of U.S. persons in 2017, down from *billions per day* in 2013.[10] Domestic surveillance is restrained by constitutional rights, statutes, and political pressure. However, extraterritorial surveillance usually does not face any restrictions.[11]

B. The Need for SIGINT and Extraterritorial Surveillance

In the United States, modern-day bulk surveillance began to take shape after 9/11.[12] The 9/11 attacks and proliferation of cellular technol-

4. Iñaki Navarrete & Russell Buchan, *Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions*, 51 CORNELL INT'L L.J. 897, 902 (2019) [hereinafter Navarrete].

5. *Id.*

6. *Signals Intelligence*, NAT'L SEC. AGENCY, https://www.nsa.gov/what-we-do/signals-intelligence/ [https://perma.cc/K99W-XJX4] (last visited Dec. 14, 2020).

7. Jussi Parikka, *The Signal Haunted Cold War: Persistence of SIGINT Ontology*, *in* COLD WAR LEGACIES 167 (John Beck and Ryan Bishop eds., 2016).

8. *See id.*

9. *See id.* at 168.

10. Dustin Volz, *Spy Agency NSA Triples Collection of U.S. Phone Records: Official Report*, REUTERS (May 4, 2018, 3:56 PM), https://www.reuters.com/article/us-usa-cyber-surveillance/spy-agency-nsa-triples-collection-of-u-s-phone-records-official-report-id USKBN1I52FR [https://perma.cc/9DDU-R492].

11. This is not the case in the United States, as outlined in PPD-28, *supra* Section III.A.1.

12. Jake Laperruque, *The History and Future of Mass Metadata Surveillance*, POGO (June 11, 2019), https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance/ [https://perma.cc/76YC-28RK].

ogy increased the importance of extraterritorial surveillance.[13] For example, in relation to the operations in Afghanistan in October 2001, the U.S. began intercepting *all* satellite communication coming out of Pakistan.[14]

Modern-day "irregular warfare" has prioritized SIGINT over human intelligence (HUMINT) collection.[15] Given that enemies, often terrorists, reside in urban areas and blend amongst innocent civilians, deploying human intelligence officers is a more difficult task.[16] In contrast, surveillance programs can be deployed around the world simultaneously and obtain far greater quantities of information. As amorphous terrorist threats persist around the world, SIGINT collection has become a growing part of any country's national security toolkit.[17] Surveillance has been credited with thwarting terrorist attacks, but its effectiveness has been debated.[18]

C. Is Peacetime Espionage Legal Under International Law?

Extraterritorial surveillance implicates two considerations: peacetime espionage in the interest of national security and individual privacy. Although individual privacy is recognized internationally as a human right, peacetime espionage is not directly addressed through international agreements or treaties.[19] As a result, its legality is widely debated.

Some contend that espionage between two states is categorically illegal under international law, regardless of the method deployed in conducting espionage.[20] Peacetime espionage violates territorial sovereignty, as a country engaging in espionage is working outside its jurisdiction.[21] As almost every country prohibits espionage in its domestic laws,[22] any country acting to the contrary in another country violates that country's sovereignty.[23] The *Lotus* case in 1927 at the Permanent Court of International Justice found international law restricted States from "[E]xercis[ing] its power in any form in the territory of another State."[24]

While peacetime espionage may violate territorial sovereignty, the practice is likely lawful through customary international law (CIL).[25] Article 38 in the Statute of the International Court of Justice defines CIL as a

13. Matthew M. Aid, *All Glory is Fleeting: Sigint and the Fight Against International Terrorism,* 18 INTEL. & NAT'L SEC. 72, 104 (2004).
14. *Id.* at 105.
15. *See* Reiley, *supra* note 3, at 68.
16. *See id.*
17. *Id.*
18. *See, e.g.*, Michelle Cayford & Wolter Pieters, *The Effectiveness of Surveillance Technology: What Intelligence Officials Are Saying*, 34 THE INFO. SOC'Y 88 (2018).
19. Patrick C. R. Terry, *The Riddle of the Sands - Peacetime Espionage and Public International Law*, 51 GEO. J. INT'L L. 377, 379 (2020).
20. *See id.* at 380.
21. *See id.* at 383-84.
22. *See id.* at 384.
23. *See* Navarrete, *supra* note 4, at 907.
24. *See id.* at 906.
25. *See id.* at 900.

"general practice accepted as law."[26] This view is a begrudging admission that espionage's widespread use and acceptance in the international community makes the practice lawful.[27] Indeed, many countries have agreed to limit espionage against each other,[28] or conduct it together. Additionally, the absence of regulation against espionage makes the practice lawful.[29] Given that espionage could prevent conflict by revealing the capabilities of different countries, scholars even interpret espionage as a promoter of peace under the U.N. charter's self-defense principle.[30]

Nevertheless, evaluating peacetime espionage broadly leads to an imprecise analysis; various activities performed in the pursuit of obtaining intelligence implicate different parts of international law. For example, aerial surveillance could implicate self-defense (under Article 51 of the U.N. Charter), and certain intelligence could constitute intellectual property theft (under World Trade Organization agreements).[31] As a result, each espionage-related activity should be assessed independently under international law.[32]

D. Extraterritorial Surveillance is *Different* from Peacetime Espionage

In that vein, one can see that extraterritorial surveillance is distinguishable from peacetime espionage. Developments in technology have exponentially increased electronic communication, and created equally sophisticated ways to collect, store, and process the data collected from this communication.[33] Extraterritorial surveillance today involves governments collecting personal data from entire populations, making surveillance "cheap, easy, and ubiquitous."[34] While peacetime espionage affects state actors and suspected individuals, extraterritorial surveillance affects nearly everyone with an internet or cellular connection. Unlike conventional espionage, surveillance is not targeted. Most of this activity happens without the consent or even knowledge of individuals across the world. Like peacetime espionage, no international agreement directly addresses extraterritorial surveillance. International human rights agreements do grant universal privacy rights, but they are likely inapplicable to government surveillance programs.

---

26. Chantal Khalil, Note, *Thinking Intelligently About Intelligence: A Model Global Framework Protecting Privacy*, 47 GEO. WASH. INT'L L. REV. 919, 933 (2015).

27. *See* Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1074–75 (2006).

28. *See* Terry, *supra* note 19, at 381–82.

29. *See* Darien Pun, Comment, *Rethinking Espionage in the Modern Era*, 18 CHI. J. INT'L L. 353, 361–62 (2017).

30. *See id.* at 363.

31. *See* Chesterman, *supra* note 27, at 1073.

32. Terry, *supra* note 19, at 380.

33. *See* Brittany May Johnson, Note, *Foreign Nationals' Privacy Interests Under U.S. Foreign Intelligence Law*, 51 TEX. INT'L L.J. 229, 235 (2016).

34. *See id.* at 241.

1. International Agreements Concerning Privacy

The UDHR and ICCPR are the international law agreements that grant privacy rights. Most countries with surveillance programs like the United States, U.K., France, and Germany are signatories to these agreements.

The UDHR, adopted by the United Nations General Assembly (UNGA) in the immediate aftermath of World War II, declared that "[n]o one shall be subject to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. . ."[35] The UNGA similarly adopted the ICCPR in 1966 as part of two agreements to implement the UDHR.[36] The ICCPR language on privacy is nearly identical to the UDHR's.[37] However, the United Nations charter specifies that UNGA resolutions are simply recommendations.[38]

The impact of the UDHR and ICCPR on international law with regards to privacy may not matter. These agreements neither define the contours of privacy rights nor explain what constitutes an arbitrary interference of the privacy right granted.[39] Implicit in protecting individuals from *arbitrary* interference is an admission that privacy is not an absolute right. The UNDHR and ICCPR both recognize that governments may interfere with privacy rights; they do not specify to what extent governments may interfere.[40]

These agreements are also interpreted differently by different countries, blunting the impact that the agreements can collectively have on international law. For example, China has not ratified the ICCPR and supposedly utilizes unofficial translations of the agreement that contain lax language surrounding enforcing human rights obligations.[41] The United States does not consider the ICCPR to apply extraterritorially, meaning that the U.S. government does not have to meet international human rights obligations outside its territory.[42] While an International Court of Justice (ICJ) advisory opinion endorsed extraterritoriality,[43] the European Court of Human Rights adopted the American position.[44] Given that both the UNHR and ICCPR do not define the contours of "the right to privacy" and that countries do not consider the ICCPR to apply extraterritorially,

35. G.A. Res. 217 (III), at 73–74 (Dec. 8, 1948).

36. *See* Eric Manpearl, *The Privacy Rights of Non-US Persons in Signals Intelligence*, 29 FLA. J. INT'L L. 303, 332 (2018).

37. International Covenant on Civil and Political Rights art. 17, Mar. 23, 1976, 999 U.N.T.S 171 ("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 . . .").

38. Charter of the United Nations and the Statute of the International Court of Justice, art. 10–14, June 26, 1945, 59 Stat. 1031.

39. *See* Manpearl, *supra* note 36, at 332.

40. *See id.* at 331–32.

41. *See Suppressed in Translation*, ECONOMIST (Mar. 17, 2016), https://www.economist.com/china/2016/03/17/suppressed-in-translation [https://perma.cc/G9TL-JJZ5].

42. Aldo S. Zilli, Note, Approaching the Extraterritoriality Debate: The Human Rights Committee, the U.S., and the ICCPR, 9 SANTA CLARA J. INT'L L. 399, 401 (2011).

43. *See id.* at 415.

44. *See id.* at 416.

existing international human rights agreements may not protect privacy from extraterritorial surveillance.

Proceeding to box extraterritorial surveillance under the peacetime espionage umbrella ignores the human rights concerns that the practice implicates. Allowing governments to conduct unchecked, blanket surveillance on entire populations may not violate international law *per se*, but it ostensibly leaves no international right to privacy for the global citizenry. Additionally, domestic institutions and the general public increasingly want to protect their privacy from government surveillance. If popular support for domestic surveillance is limited, there is likely even less support for foreign governments doing the same. Unfortunately for these privacy advocates, existing international human rights agreements are unable to restrain extraterritorial surveillance.

At the same time, policymakers are unlikely to abandon extraterritorial surveillance from the national security arsenal. Instead of skirting around international agreements, countries may be better served creating a mechanism that allows both extraterritorial surveillance and privacy protections to coexist.

II. Perspectives on Restraining Surveillance

A. Extraterritorial Surveillance Cannot be Regulated

Not everyone thinks extraterritorial surveillance should be restrained to protect privacy. In fact, permitting surveillance without restriction promotes peace.[45] Incomplete intelligence may lead countries to miscalculate their chance of success and begin armed hostilities.[46] Indeed, *inaccurate* intelligence has allowed countries to miscalculate threats and initiate war, as we saw with the U.S. invasion of Iraq in 2003.[47] Surveillance may provide countries with the valuable information that will prevent war. Stepping outside modern-day surveillance, unauthorized American reconnaissance flights over the Soviet Union, disclosed in the U-2 spy plane crisis,[48] informed the American government that the Soviet Union's military was not as powerful as once imagined, arguably contributing to Cold War stability.[49] One can argue that modern surveillance performs a similar function, just with better technology. Creating international norms or regulations protecting privacy instead will impede intelligence collection efforts and risk peace.[50]

Some contend that intelligence collection, or espionage broadly, cannot be regulated and that, therefore, we should concede that these gaps will

45. *See* John Yoo & Glenn Sulmasy, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH J. INT'L L. 625, 636 (2007).

46. *See id.* at 635.

47. *See* Richard K. Betts, *Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD*, 122 POL. SCI. Q. 585, 585 (2007).

48. *See* Luke Pelican, *Peacetime Cyber-Espionage: A Dangerous but Necessary Game*, 20 COMMLAW CONSPECTUS 363, 383 (2012).

49. *See id.*

50. *See* Yoo & Sulmasy, *supra* note 45, at 636.

persist.[51] This is because the scope of possible intelligence activity is so wide that it cannot be placed into regulatory boxes,[52] and that countries are unlikely to reciprocate protection from espionage extended by one country, notwithstanding any regulation's unenforceability.[53]

Adopting an approach that lets extraterritorial surveillance run an unchecked course will encounter stiff opposition from individuals and privacy groups. Additionally, whistleblowers have brought immense scrutiny into surveillance programs.[54] After the Snowden disclosures, the NSA considered cancelling its surveillance program because of the negative publicity it generated.[55] Instead of relying on preventing further unauthorized disclosures and the resulting public relations nightmares, intelligence agencies may be better served by recognizing privacy protections for foreign individuals.

B. Create More Rights

Various solutions propose setting up a new bundle of privacy rights and duties for nations to follow. Generally protecting the right to privacy through a "Privacy Principle" is one solution.[56] Existing human rights treaty obligations are difficult to apply to extraterritorial surveillance, especially in the face of widespread practice.[57] The principle will make surveillance presumptively wrong, and countries will face a heightened burden to justify surveillance activities.[58] Such a broad principle will likely allow nations to sign on as they will interpret privacy to conform with domestic laws and cultural norms. However, they will likely interpret the privacy principle to fit their existing surveillance practices.[59] Privacy is already a recognized human right, and a new principle would not change the status quo.

Not everyone thinks a new legal principle is needed. Rather, some scholars believe that privacy simply needs reinterpretation under existing treaty and customary international law.[60] One can reasonably argue that the ICCPR and customary law indicate that countries should apply privacy

---

51. A. John Radson, *The Unresolved Equation of Espionage and International Law*, 28 MICH J. INT'L L., 595, 596–97 (2007).

52. *See id.* at 614–16; *see also id.* at 605–10.

53. *See id.* at 619.

54. Jack Goldsmith, *Three Years Later: How Snowden Helped the U.S. Intelligence Community*, LAWFARE (June 16, 2016, 9:32 AM), https://www.lawfareblog.com/three-years-later-how-snowden-helped-us-intelligence-community [https://perma.cc/BL3T-MPS6].

55. Cale Guthrie Weissman, *The NSA Almost Killed its Own Call Surveillance Program Years Ago, Report Says*, BUS. INSIDER (Mar. 30, 2015, 12:09 PM), https://www.businessinsider.com/the-nsa-almost-cancelled-surveillance-program-due-to-snowden-2015-3 [https://perma.cc/3HN3-99MF].

56. Frédéric Gilles Sourgens, *The Privacy Principle*, 42 YALE J. INT'L L. 345, 349 (2017).

57. *Id. at* 389.

58. *Id. at* 389.

59. *See* Asaf Lubin, *A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens*, 42 YALE J. INT'L L. ONLINE 1, 7, 9 (2017).

60. *See id.* at 20.

rights extraterritorially.[61] However, a reinterpretation would effectively involve an about-face turn of stated American policy discussed earlier in this Note. Applying privacy extraterritorially is a plausible interpretation; it is not a plausible solution to addressing privacy concerns in extraterritorial surveillance.

C. The Need for a Middle Way

Allowing uninhibited surveillance will encounter strong public opposition. Equally, broadly asserting privacy rights may hinder national security goals and remain unappetizing to the governments that must agree to any new provisions. Some contend that the debate should at least distinguish between surveillance over foreigners and domestic persons.[62] Within their territory, countries have more tools aside from mass surveillance to monitor security threats *and* greater potential to abuse mass surveillance programs by denying civil liberties.[63] Therefore, imposing stricter surveillance restrictions on surveilling domestic constituents does not hamper national security needs but protects privacy and other civil liberties. Solutions that recognize this distinction, whether implicitly or expressly, effectively argue a middle way that balances the need for extraterritorial surveillance and the right to privacy. To that end, various solutions have been proposed.

While distinguishing between autonomous and manual intelligence collection,[64] one proposal suggests instituting a legal test that any surveillance program must satisfy.[65] An independent body who recognizes that the ICCPR applies extraterritorially will perform this legal test.[66] In this case, the U.S.'s current judicial review process for intelligence collection is insufficiently independent, so a new executive agency will be necessary.[67] However, asking governments to create new, independent executive agencies that will review national security operations will be an unprecedented undertaking towards a multilateral agreement.

Some have suggested neutral international bodies overseeing intelligence agencies and their practices.[68] While international courts and tribunals have greatly proliferated in recent years,[69] their effectiveness on enforcing international law is debatable.[70] Securing adequate judicial review for domestic surveillance has encountered many difficulties, mak-

---

61. *See id.* at 14.

62. *See* Asaf Lubin, *"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 CHI. J. INT'L. L. 502, 509 (2018).

63. *Id.* at 530–36.

64. *See* Peter Margulies, *Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68 FLA. L. REV. 1045, 1054 (2016).

65. *See id.* at 1052–53.

66. *Id.* at 1082; *see also id.* at 1053.

67. *Id.* at 1053.

68. *See, e.g.*, Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 362 (2016); Khalil, *supra* note 26, at 944.

69. Yuval Shany, *Assessing the Effectiveness of International Courts: A Goal-Based Approach*, 106 AM. J. INT'L. L. 225, 225 (2012).

70. *See id.* at 225–30.

ing it unlikely for international judicial bodies to receive any powers to examine clandestine surveillance programs.[71]

Some solutions argue a more restrained approach in imposing privacy restraints on extraterritorial surveillance. A sliding-scale approach would distinguish between extraterritorial surveillance involving non-state and state actors, imposing stricter privacy protections for the former.[72] States can use some guiding factors such as the nature of the intelligence activity's target, degree of clarity of international law on the intelligence activity, and existing overt action parallels in applying international law to their intelligence methods.[73] The sliding-scale approach may institute privacy during extraterritorial surveillance and give policymakers interpretive room to argue for their national security needs. This approach would require governments to consider constantly changing intelligence targets and unclear international law in sanctioning extraterritorial surveillance. Given the debate in international law on this topic, governments would interpret law as they see fit, and the status quo would prevail.

III. Introducing Tiered Code

This Note has discussed the varying flaws of the aforementioned solutions. Unfortunately, few solutions across the legal academy address these flaws: (i) securing buy-in from countries that do not respect privacy rights for even domestic constituents; and (ii) enforcement mechanisms to ensure compliance with any new legal restraints on extraterritorial surveillance. Any proposal that aims to regulate clandestine national security operations to accommodate human rights concerns for foreigners must specifically address these twin concerns and generally faces a heavy burden to prove its viability. Since no multilateral framework addresses extraterritorial surveillance, a new agreement must have limited scope.

To that end, this Note proposes creating a "Tiered Code" of restraints on extraterritorial surveillance. Additionally, this Note will measure the Tiered Code to the twin concerns that will plague any international agreement on extraterritorial surveillance. In effect, this defense will show that modest international agreements on this issue are viable. These restraints will protect foreigners' privacy in the surveillance process. A Tiered Code will create two tiers of restraints: Tier I restraints will be limited and binding on countries while Tier II will comprise stricter restraints that countries may unilaterally enact or collectively agree upon at a later date. The Tiered Code will have multiple benefits: (i) clarifing international law—extraterritorial surveillance that respects privacy is permissible; (ii) outlining permissible practices that will create reference points for a robust public policy debate, (iii) creating substantive protections for individual

71. *See* Ira Rubenstein et al., *Systematic Government Access to Personal Data: A Comparative Analysis*, 4 INT'L DATA PRIV. L. 96, 110 (2014) (comparing surveillance laws of 13 countries).

72. *See* Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 669 (2016).

73. *See id.* at 672–75.

privacy on a global scale; and (iv) balancing national security and international human rights concerns.

A. Tier I: Modest Provisions

To maintain viability, Tier I's baseline provisions need to restrain states while preserving an important national security tool. An effective agreement will require consent from countries with serious surveillance capabilities and urgent national security needs. Tier I should comprise the following provisions: (i) express declaration that extraterritorial surveillance that respects privacy is permissible; (ii) transparent attribution of domestic law sources that permit extraterritorial surveillance; (iii) narrowing the reasons for permitting surveillance; and (iv) limiting the time period that data is retained.

1. Express Declaration that "Extraterritorial Surveillance that Respects Privacy is Permissible"

This agreement will include an express declaration that extraterritorial surveillance that respects individual privacy is permissible. Intelligence agencies may recoil at the suggestion that they will have to respect foreigners' privacy. Around the world, domestic laws afford foreigners with few privacy protections.[74] These jurisdictions include the U.K. and the EU among others.[75] India and China, home to 36% of the world population,[76] do not even limit government surveillance of domestic residents.[77]

However, intelligence agencies will be remiss to imagine that the status quo of unrestricted intelligence collection on foreigners will persist. PPD-28,[78] which carries the substantive legal force as an Executive Order,[79] makes the United States the only major world power to recognize foreigners' privacy rights in surveillance.[80] Despite the Trump administration's penchant for reversing the Obama administration's policies,[81] PPD-28 persists.[82] Multiple reasons informed this continuation: (i) Public pressure

74. Rubenstein et al., *supra* note 71, at 115, 118.

75. *See generally*, Rubenstein et al., *supra* note 71; *see also* Eric Manpearl & Steve Slick, *Revisiting Legacy Restrictions on the Intelligence Community's Handling of SIGINT Data on Non-Americans*, LAWFARE (Oct. 17, 2019, 10:10 AM), https://www.lawfareblog.com/revisiting-legacy-restrictions-intelligence-communitys-handling-sigint-data-non-americans [https://perma.cc/KP7W-UGKE].

76. *India vs. China by Population* STAT. TIMES, http://statisticstimes.com/demographics/china-vs-india-population.php [https://perma.cc/SQN8-JVPN] (last visited Dec. 12, 2020).

77. *See* Rubenstein et al., *supra* note 71, at 106.

78. Administration of Barack Obama, 2014 Directive on Signals Intelligence Activities, DAILY COMP. PRES. DOC. 1 (2014) [hereinafter PPD-28].

79. U.S. Att'g Gen., Office of Legal Counsel, Memorandum Opinion on Legal Effectiveness of a Presidential Directive, as Compared to an Executive Order, 24 Op. O.L.C. 29 (Jan. 29, 2000).

80. *See* Manpearl & Slick, *supra* note 75.

81. Juliet Eilperin & Darla Cameron, *How Trump is Rolling Back Obama's Legacy*, WASH. POST, (Jan. 20, 2018), https://www.washingtonpost.com/graphics/politics/trump-rolling-back-obama-rules/ [https://perma.cc/BV2H-EWYE].

82. *See* Manpearl & Slick, *supra* note 75.

from the Edward Snowden disclosures;[83] (ii) the Privacy Shield agreement between the United States and EU;[84] and (iii) the continuing existence of U.S. intelligence capabilities.[85] The Privacy Shield is a European-American agreement that facilitates data transfer from the EU to the United States, and ensures that European data is protected by the stricter European standard.[86] In light of the Snowden revelations, PPD-28 proved essential to the Privacy Shield's viability.[87] This shows that beyond political pressure, business reasons may warrant stricter privacy protections, too.

Ardent human rights advocates may disagree with any declaration that permits foreign intelligence collection, particularly if legal remedies for affected individuals are not devised. Declarations became common practice in twentieth century international relations[88] Many of these declarations constitute "soft law," which is often dismissed as a normative statement without binding authority.[89] Indeed, "soft law" is partly why the privacy rights expressly granted in multiple international agreements already discussed do not restrain states from surveilling foreigners. Many soft law declarations delineate negative rights, which inherently require restraint from actors.[90] Without enforcement mechanisms, restraining intelligence agencies into respecting foreigners' privacy will be a tall task. If one considers this declaration on its own, perhaps as a UNGA Resolution, then it will indeed constitute "soft law."[91]

Nevertheless, even mere declarations can have legal impact. A significant number of international conventions have become the legal offspring of the U.N. General Assembly resolutions.[92] Consider the Declaration of the Rights of Indigenous Peoples as an example. Existing provisions in the ICCPR did not specifically address the problems facing indigenous peoples

83. *See id.*

84. *See id.*

85. *See* Goldsmith, *supra* note 54.

86. U.S. DEP'T OF COMM., INT'L TRADE ADMIN., THE EU-U.S. AND SWISS-U.S. PRIVACY SHIELD FRAMEWORKS 1, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdg [https://perma.cc/H74G-D8J7] (last visited Sept. 17, 2021).

87. *See* Manpearl & Slick, *supra* note 75.

88. *See, e.g.*, Declaration concerning the Laws of Naval War, Feb. 26, 1909 (establishing maritime law code in 1909); Declaration of Philadelphia, May 10, 1944 (establishing International Labor Organization in 1944); Declaration of the Rights of the Child, 1923; United Nations Declaration of Human Rights, Dec. 10, 1948 (granting individuals, among other rights, a right to privacy).

89. DINAH L. SHELTON, SOFT LAW, HANDBOOK OF INTERNATIONAL LAW 3 (2008), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2048&context=faculty_publications [https://perma.cc/ZLS9-4NJL] [hereinafter Soft Law].

90. STEPHEN F. CAPONE, ENCYCLOPEDIA OF GLOBAL JUSTICE (Deen K. Chatterjee, ed., 2011) https://link.springer.com/referenceworkentry/10.1007/978-1-4020-9160-5_338 [https://perma.cc/DRP8-7VP3] (last visited Sept. 17, 2021).

91. *Hard Law/Soft Law*, EUROPEAN CENTER FOR CONSTITUTIONAL AND HUMAN RIGHTS, https://www.ecchr.eu/en/glossary/hard-law-soft-law/ [https://perma.cc/6WQD-JFJA] (last visited Sept. 17, 2021).

92. Mauro Barelli, *Role of Soft Law in the International Legal System: The Case of the United Nations Declaration on the Rights of Indigenous Peoples*, THE INT'L & COMP. L.Q. 957, 963 (2009).

and left crucial gaps such as protecting indigenous intellectual property.[93] The resulting Declaration addressed these concerns and grew from a proposal put forward in 2005 by the United Nations Human Rights Commissioner.[94] Similarly, the ICCPR grants individuals privacy rights but does not address the issues extraterritorial surveillance implicates.

New soft law may also interact with existing soft law to enhance existing law. Generic outlines in the Charter of the Organization of American States helped create the Inter-American Commission on Human Rights, which enforced the American Declaration of the Rights and Duties of Man.[95] Notably, the Charter hardly discussed human rights.[96] Although a binding agreement is preferable, a "soft" declaration that asks intelligence agencies to respect foreigners' privacy may influence subsequent agreements. The United Nations High Commissioner for Human Rights annual report in 2014 implicitly recognized foreign surveillance as expected practice and called on limitations that protect individual privacy.[97] A declaration alone can be an offspring of the report and spur further resolutions in international organizations—either leading to binding international law or, at the very least, becoming a factor in the policymaker's calculus.

2. *Transparent Attribution of Domestic Law Sources that Permit Extraterritorial Surveillance*

Part of the consternation among privacy advocates over unbridled extraterritorial surveillance originates from the growing proliferation of secret law.[98] In the United States, secret law includes Foreign Intelligence Surveillance Court (FISC) jurisprudence and opinions by the Department of Justice's Office of Legal Counsel (OLC).[99] Classified opinions by the OLC carry legal force and have secretly sanctioned U.S. policy at home and abroad; these include "enhanced interrogation techniques"[100] and even

93. *Id.* at 959.

94. *Id.* at 967.

95. *Id.* at 962; *see also* Inter-American Commission on Human Rights, *Basic Documents Pertaining to Human Rights in the Inter-American System*, http://www.cidh.oas.org/basicos/english/Basic1.%20Intro.htm [https://perma.cc/NV2H-543X] (last visited Apr. 12, 2021).

96. *Id.*

97. U.N. High Commissioner for Human Rights, *Summary of the Human Rights Council Panel Discussion on the Right to Privacy in the Digital Age*, ¶ 50, U.N. Doc. A/HRC/28/39 (Dec. 19, 2014). For an electronic link, see https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/247/08/PDF/G1424708.pdf?OpenElement [https://perma.cc/SXP2-UQNS].

98. Dakota S. Rudesill, *Coming to Terms with Secret Law,* 7 HARV. NAT'L SEC. J. 241, 245–46 (2016).

99. *Id.* at 248–49.

100. *See* Scott Shane et al., *Secret U.S. Endorsement of Severe Negotiations*, N.Y. TIMES (Oct. 4, 2007), https://www.nytimes.com/2007/10/04/washington/04interrogate.html [https://perma.cc/EVR4-6PHY].

warrantless domestic surveillance of U.S. persons.[101] This phenomenon is not limited to the United States, as more countries likely produce secret law than otherwise.[102] Countries even engage in secret multilateral intelligence collection agreements, ranging from the now well-known Five Eyes agreement between the United States, U.K., Canada, Australia, and New Zealand to the sprouting anti-Islamic State intelligence sharing collective of Russia, Iraq, Iran, and Syria.[103] The scope of secret law in the United States and around the world is unknown due to its inherently clandestine nature.[104] Some have argued that even though China surveils its citizens without limitation, Chinese law's express grants to do so are preferable to classified legal opinions that govern U.S. surveillance.[105]

Secret law's proliferation across the world certainly implicates domestic persons' concerns. Nevertheless, governments afford domestic persons political and legal rights not available to foreigners.[106] The legality principle warrants that individuals should be reasonably notified of the laws they're subjected to.[107] Originally grounded in criminal law, the principle is already a part of international human rights law.[108] It is included in both binding and non-binding international agreements,[109] including the UDHR and ICCPR.[110] Under Tier I, governments should extend the legality principle to foreigners. Governments should publish laws that subject foreigners to surveillance and the government agencies responsible for carrying out surveillance.[111] Intelligence agencies will still be able to protect their capabilities, but their operations would move from "deep secrecy" to "shallow secrecy."[112]

Not only will individuals know that they may be subject to surveillance from foreign countries, but they will also know what laws govern this surveillance. Citizens of Country X may not have constitutional rights in Country Y, but they may be able to pressure Country X's government to negotiate more limitations in surveillance from Country Y. Any compara-

101. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?smid=EM-share [https://perma.cc/K5C8-64AK].

102. Lubin, *supra* note 62, at 542.

103. Brian Mund, *Legalizing Intelligence Sharing: A Consensus Approach*, 9 AM. U. NAT'L SEC. L. BRIEF 1, 5 (2019) (noting additional intelligence alliances including between European and African states, and between China, Russia, and central Asian states).

104. *See* Rudesill, *supra* note 98, at 249–50.

105. *See* James D. Fry, *Privacy, Predictability, and Internet Surveillance in the U.S. and China: Better the Devil You Know?*, 37 U. PA. J. INT'L L. 419, 499 (2015).

106. *See, e.g.*, *Rights of Permanent Residents and Foreign Nationals*, GEO. L. LIBR., https://guides.ll.georgetown.edu/c.php?g=592919&p=4170926 [https://perma.cc/47QT-7QFG].

107. KENNETH S. GALLANT, THE PRINCIPLE OF LEGALITY IN INTERNATIONAL AND COMPARATIVE CRIMINAL LAW 11 (2008).

108. *See id.* at 157.

109. *Id.*

110. *See id.* at 175.

111. *See* Deeks, *supra* note 68, at 351–53.

112. *See id.* at 352.

tive discussion on extraterritorial surveillance will be based on published laws and official interpretations, similar to those of domestic surveillance.[113]

Governments are already authorizing extraterritorial surveillance in their statutes. German and Italian law implicitly permits extraterritorial surveillance.[114] The U.K.'s Investigatory Powers Act and France's International Electronic Communications Law expressly authorize extraterritorial surveillance.[115] Even though parts of PPD-28 were classified, the executive order still articulated the laws and agencies governing extraterritorial surveillance. For example, Section 2.3 of Executive Order 12333 governs dissemination and retention of data.[116] Surveillance standards outlined by these countries continue to face criticism, especially from privacy advocates.[117] Nevertheless, the public debate over these laws represents a paradigm shift: There are now grants and limits of extraterritorial surveillance for privacy advocates, national security policymakers, and the general public to evaluate. These benefits will be extended once the provision sees universal acceptance.

The first two provisions of Tier I will help legitimize both extraterritorial surveillance *and* limitations protecting foreigners' privacy. The next two create substantive limits on extraterritorial surveillance. They outline limited permissible reasons for surveillance and how long collected intelligence may be stored. Given that the provisions are closely related, they will be discussed together.

3. Narrowing the Reasons for Which Collection is Permitted

Many surveillance capabilities are unknown. We know that governments can intercept phone calls, emails, text messages, and financial transactions—even when they are encrypted.[118] On a global scale, this constitutes a trove of information that can be used beyond just maintaining national security or conducting foreign policy. Modern, state-sponsored economic espionage deploys rapidly evolving cyber capabilities, the legality of which constitutes its own debate under international law.[119] Using

113. *See, e.g.*, THE LAW LIBRARY OF CONGRESS, FOREIGN INTELLIGENCE GATHERING LAWS (2016).

114. *See* Deeks, *supra* note 68, at 352–53.

115. Asaf Lubin, *A New Era of Mass Surveillance is Emerging Across Europe*, JUST SEC. (Jan. 9, 2017), https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/ [https://perma.cc/CQ3H-Q6L3].

116. PPD-28, *supra* note 78.

117. *See* Lubin, *supra* note 115; James Vincent, *The UK Now Wields Unprecedented Surveillance Powers—Here's What it Means*, VERGE (Nov. 29, 2016, 12:05 PM) https://www.theverge.com/2016/11/23/13718768/uk-surveillance-laws-explained-investigatory-powers-bill [https://perma.cc/R9WC-ZDAQ] (quoting U.N. privacy chief who called surveillance laws "beyond scary").

118. James Ball et al., *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN (Sept. 5, 2013), https://ir.stonybrook.edu/xmlui/bitstream/handle/11401/9864/2revealedhowusandukspyagenciesdefeatinternetprivacyandsecurityworldnewsguardianweekly.pdf?sequence=1 [https://perma.cc/FDC6-LA28].

119. Catherine Lotrionte, *Countering State-Sponsored Cyber Economic Espionage Under International law*, 40 N.C. J. INT'L L. & COM. REG. 443, 444–45 (2015).

extraterritorial surveillance programs to favor domestic industry and steal intellectual property is certainly part of that debate but remains beyond the scope of this Note. As part of creating substantive limits on extraterritorial surveillance, countries should agree to limit the reasons for collection to only national security related purposes.

Limiting the scope of permissible surveillance will likely reduce the volume of data collected—enhancing individual privacy. However, limiting surveillance broadly to "national security purposes" leaves room for interpretations that may not restrict the volume of information collected. Restricting surveillance to national security purposes should expressly exclude obtaining trade secrets, stifling dissent, and disfavoring people on the basis of their identity as permissible reasons for surveillance. Indeed, that may be why PPD-28 included this clarification while articulating similarly narrower reasons for collection.[120]

4. Limiting Retention and Disclosure of Data

Limiting reasons for conducting extraterritorial surveillance addresses the pre-collection process. Safeguards should also be installed for the post-collection process, where intelligence analysts or machines will parse through the data collected. Given the wide net surveillance programs cast, intelligence agencies do not use the vast majority of the data they collect. Tier I should mandate that countries delete unnecessary data after a reasonable time period. Countries can compare domestic laws addressing extraterritorial surveillance to establish an appropriate time period. PPD-28 permits retention for five years;[121] a proposed Norwegian bill set the limit to eighteen months;[122] and British, Spanish, and Italian law each permit retention for up to one year.[123]

Combined, these two provisions would represent the most stringent limitations under international law on extraterritorial surveillance. Governments would follow a more uniform protocol on their surveillance practices. The next section will evaluate these two limits and Tier I broadly by considering twin issues that will affect any multilateral agreement: enforcement concerns and incorporating countries that do not respect privacy.

5. Enforcement Concerns

Any international agreement on extraterritorial surveillance will fall apart if signatories do not adhere to its provisions. With an express declaration that permits extraterritorial surveillance, asking governments to

120. *See* Johnson, *supra* note 33, at 249.

121. PPD-28, *supra* note 78.

122. Alexander Fanta, *Amidst Pandemic, Norway Moots Powers for Spy Agency*, NETZPOLITIK.ORG (May 5, 2020, 3:00 PM), https://netzpolitik.org/2020/amidst-pandemic-norway-moots-powers-for-spy-agency/ [https://perma.cc/EXK4-LHDE].

123. For British retention period, see Bill Goodwin, *UK's Phone and Internet Bulk Data Surveillance Unlawful, Says EU Court opinion*, COMP. WKLY. (Jan. 16, 2020, 4:34 PM), https://www.computerweekly.com/news/252476876/UKs-phone-and-internet-bulk-data-surveillance-unlawful-says-EU-court-opinion [https://perma.cc/X8VV-5RZT]; for Spanish and Italian retention periods, see Deeks, *supra* note 68, at 358.

publish or create law that governs extraterritorial surveillance may be relatively easy to comply with. However, Tier I's final two provisions on collection will require governments to modify clandestine operations, many of which remain classified. Intelligence programs often deal with transparency and accountability issues in front of domestic stakeholders: lawmakers, public interest organizations, and the general public.[124] In liberal democracies, these stakeholders have checked government action with mixed results. Enforcing adherence to a Tiered Code would be even more difficult; it would require governments to hold their peers accountable over what would be any government's most classified programs. Moreover, a country's extraterritorial surveillance programs are inherently directed at other countries, heightening the level of secrecy surrounding these operations. Fundamental distrust lingers between intelligence agencies;[125] even allies sometimes refrain from sharing relevant intelligence to each other, fearing that the information may be compromised.[126] If agencies suspect that others are not complying, then they are unlikely to comply either.

Assuming a worst-case scenario, where no enforcement provisions play out and the Tiered Code becomes "soft law", a multilateral framework expressly articulating restraints on extraterritorial surveillance could be similarly valuable as the Declaration. However, existing factors may enable self-regulated enforcement.

First, expressly permitting surveillance and publishing the laws that carry them will have a spillover effect: greater public engagement and resulting accountability. Extraterritorial surveillance is a departure from traditional peacetime espionage; the former gathers personal information on billions of unsuspecting individuals across the world. Public outcry from the Edward Snowden disclosures led the United States to unilaterally institute PPD-28. In 2014, a majority of Americans disapproved of NSA surveillance of Americans,[127] and an even greater majority from forty-three other countries disapproved of NSA surveillance on foreign individuals.[128] With a multilateral framework, domestic persons will know that their government permitted other countries to collect information on them at the

124. *See* Steven Aftergood, *Secrecy and Accountability in U.S. Intelligence*, FED'N OF AM. SCIENTISTS (Oct. 9, 1996), https://fas.org/sgp/cipsecr.html (proposing new measures to hold intelligence agencies accountable).

125. *See, e.g.*, Daniel Severson, Note, *American Surveillance of Non-U.S. Persons: Why New Privacy Protections Only Offer Cosmetic Change*, 56 HARV. INT'L L.J. 465, 510-11 (commenting that U.S. intelligence may have spied on German government officials because they may have helped skirt sanctions against Iran).

126. *See, e.g.*, Siobhan Gorman & Julian E. Barnes, *Spy, Military Ties Aided Bin Laden Raid*, WALL ST. J. (May 23, 2011 12:01 AM), https://www.wsj.com/articles/SB10001424052748704083904576334160172068344 [https://perma.cc/YZ5V-HAJ5] (reporting how the U.S. did not share intelligence with Pakistan prior to the Bin Laden raid).

127. George Gao, *What Americans think about NSA surveillance, national security, and privacy*, PEW RSCH. CTR. (May 29, 2015), https://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/ [https://perma.cc/V46Y-MGYR].

128. *Id.*

expense of maintaining national security. Most individuals would like to see their governments make sure that their privacy is protected by enforcing the agreement's restraints. They may even pressure for stronger enforcement mechanisms. Public access to surveillance is already on the rise through leaks, voluntary government transparency, and even growing detectability.[129]

Second, the agreement's restraints will empower potential whistleblowers, as violations will be easier to identify instead of being shrouded in ambiguous international law. States have become increasingly responsive to whistleblower revelations.[130] Indeed, the Snowden disclosures invited official scrutiny for the American, German, Spanish, Mexican, and Brazilian governments.[131] To comply with international law, the United States also took pre-emptive steps restraining more spying, fearing further disclosures.[132] Individuals may be more motivated to disclose foreign government surveillance than their own governments themselves, who are influenced by factors including public embarrassment.[133]

Any multilateral framework restraining intelligence agencies will have another asset at its disposal: other intelligence agencies. Intelligence agencies, especially those who cooperate, can enforce legal obligations on others.[134] Given that intelligence agencies have similar methods, overlapping jurisdictions, and institutional expertise, they are the first and most likely to flag each other's violations of internationally agreed-upon practices. Combined with public criticism, disclosing alleged improprieties may create diplomatic fallout. Indeed, diplomatic fallout from the Snowden disclosures may have motivated supposed newfound CIA restraints on spying on Western allies.[135] States may also make intelligence cooperation contingent on following certain principles, such as restricting collection reasons and data storage. Before and after 9/11, U.K. intelligence agencies sought assurances from their American counterparts that shared intelligence will not be used to carry out the death penalty.[136] While much remains classified, intelligence cooperation is more pervasive than commonly perceived. For example, the "Five-Eyes" countries, and the United States in particular, have cooperated with countries that include Israel, Morocco, Pakistan, Egypt, Japan, and South Korea.[137] Even the United States and Iran shared intelligence in the immediate aftermath of the 9/11 attacks.[138] A different political environment makes cooperation

129. *See* Deeks, *supra* note 72, at 615–21.

130. Roslyn Fuller, *A Matter of National Security: Whistleblowing in the Military as a Mechanism for International Law Enforcement*, 15 San Diego Int'l L.J. 249, 253 (2014).

131. *See id.* at 259–60.

132. *See id.* at 260.

133. *See* Deeks, *supra* note 72, at 620.

134. *See* Ashley Deeks, *Intelligence Communities, Peer Constraints, and the Law*, 7 Harv. Nat'l Sec. J. 1, 4 (2016).

135. *See id.* at 42.

136. *See id.* at 29.

137. *See id.* at 8–9.

138. *See id.* at 8.

between the two unlikely today, but it illustrates that, given the right circumstances, any two countries could share classified information.

Common throughout this discussion, and indeed the entire Note, is the U.S. intelligence community. As the world's pre-eminent military power, the United States likely also has the strongest intelligence capabilities.[139] Asking the strongest intelligence power to exercise restraint may narrow the gap between the United States and other countries. Therefore, buy-in from the United States may be necessary; without it, any multilateral framework is unlikely to stand. Luckily, PPD-28 has endured for six years and across two politically different presidential administrations. Given the unique limitations that regulating intelligence agencies presents, stricter enforcement mechanisms should wait until after an international framework is operationalized. Rather than try the "Hail-Mary" touchdown, a multilateral agreement should go for the first down.

6. Countries that Do Not Respect Privacy

The discussion in this Note has largely centered on developed, Western democracies. Countries outside this part of the world also engage in rigorous debate over privacy protections as well. In 2019, the High Court of South Africa found the country's ". . . bulk surveillance activities and foreign signals interception . . . unlawful and invalid."[140] In 2017, India's Supreme Court held that the Constitution implicitly guaranteed a right to privacy.[141] Nevertheless, India's government has engaged in unchecked bulk surveillance domestically,[142] making an extraterritorial surveillance program a plausible scenario. Given its democratic tradition and developing privacy jurisprudence, instituting India into a multilateral agreement may be possible; authoritarian countries that do not grant privacy rights are a much bigger problem. None are more significant on the world stage than China, who now plays a similarly indispensable role to the United States in international politics.

Chinese law permits unchecked surveillance on its own citizens.[143] Although there is a clamor for privacy protections in Western countries, different cultural attitudes may reduce the political urgency to limit surveillance in some countries. Chinese surveillance goes back millennia: The state possessed extensive records of its citizens partly to monitor move-

139. *See id.* at 53.

140. *Amabhungane Centre for Investigative Journalism v. Minister for Justice and Correctional Services* 2019 (1) ZAGPPHC 384 at 68 (S. Afr.). Note that the High Court of South Africa is not the highest constitutional court in the country. The case is pending before the Constitutional Court.

141. *K.S. Puttaswamy* v. *Union of India*, (2017) 10 SCC 1 (India).

142. *See* Anjani Trivedi, *In India, Prism-like Surveillance Slips Under the Radar*, TIME (June 30, 2013), https://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/ [https://perma.cc/QF4S-LE3H].

143. *See* Fry, *supra* note 105, at 423.

ments from home.[144] And recently, a study comparing American, Chinese, and Indian social networking users' attitudes towards privacy found that Americans were the most concerned over their privacy and Indians the least.[145] Given China's authoritarian political structure and cultural attitudes, using public disclosures is an unlikely tool to enforce Chinese adherence to privacy in surveillance.

Although counterintuitive, protections from Chinese extraterritorial surveillance may be easier to secure than from domestic surveillance. Firstly, monitoring foreigners to check dissent is not as necessary as is monitoring domestic persons. Criticizing the authoritarian government constitutes a national security threat because it challenges the government's legitimacy. That may have motivated the Chinese government's new security law in Hong Kong, which bundles dissent along with conventional national security threats.[146] Everyday Brazilian citizens in Sau Paulo criticizing the Chinese government are not as large a national security threat as Chinese citizens doing the same in Shanghai.

Secondly, China's ambitions as a global superpower may motivate concessions. Anti-Chinese sentiment is rising around the world, precipitated by China's initial mismanagement of COVID-19.[147] A think-tank associated with China's highest intelligence body shares this assessment, arguing that anti-Chinese sentiment is at its highest since 1989.[148] Eroding political freedoms in Hong Kong, border conflicts with India, the South China Sea dispute in southeast Asia, and trade disputes with the EU, the United States, and Australia have created a hostile international climate for China.[149] Chinese business and alleged intelligence efforts are seeing the impact: the U.K. and the United States have banned China-based Huawei

144. David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUT. & INFO. L. 1, 31–32 (1999).

145. Yang Wang et al., *Who is Concerned About What? A Study of American, Chinese, and Indian Users' Privacy Concerns on Social Media Sites*, TRUST & TRUSTWORTHY COMPUTING 147, 148 (2011).

146. Grace Tsoi & Lam Cho Wai, *Hong Kong Security Law: What is it and is it Worrying?*, BBC (June 30, 2020), https://www.bbc.com/news/world-asia-china-52765838 [https://perma.cc/LU5B-D7NA].

147. For changing opinions in Africa, see Simon Marks, *Coronavirus Ends China's Honeymoon in Africa*, POLITICO (Apr. 16, 2020, 4:52 PM), https://www.politico.com/news/2020/04/16/coronavirus-china-africa-191444 [https://perma.cc/9BGB-LSYZ]; for changing opinions in the U.S., see Jacob Fromer, *Anti-China Sentiment in US at 'Historic High', Pew Research Survey Finds, Amid Friction Over Trade, Coronavirus and Human Rights*, SOUTH CHINA MORNING POST (July 31, 2020, 2:33 AM), https://www.scmp.com/news/china/diplomacy/article/3095415/anti-china-sentiment-us-historic-high-pew-research-survey [https://perma.cc/FJ2F-MFAV].

148. *Exclusive: Internal Chinese Report Warns Beijing Faces Tiananmen-like Global Backlash Over Virus*, REUTERS (May 4, 2020, 7:23 AM), https://www.reuters.com/article/us-health-coronavirus-china-sentiment-ex/exclusive-internal-chinese-report-warns-beijing-faces-tiananmen-like-global-backlash-over-virus-idUSKBN22G19C [https://perma.cc/EW2K-ZGR3].

149. *Id.*; *see also* Sameer Yasir & Hari Kumar, *India Bans 118 Chinese Apps as Indian Soldier Killed on Disputed Border*, N.Y. TIMES (Sept. 2, 2020), https://www.nytimes.com/2020/09/02/world/asia/india-bans-china-apps.html [https://perma.cc/BNA6-CRCL].

from installing 5G infrastructure over concerns that the Chinese government will use Huawei to spy on Western governments.[150] The EU and India are heading in that direction,[151] and the latter has banned more than 100 Chinese mobile applications in the country.[152] Combined with the reduced national security risks from surveilling foreigners, the prevailing international climate may force China to grant protections from extraterritorial surveillance.

Securing buy-in from the world's second largest economy and most powerful authoritarian regime may cajole other authoritarian countries to do the same. An agreement without China and other authoritarian regimes may still have value. It could be self-contained and limited to protecting only citizens of signatories. Over time, as more countries sign on and incorporate even Tier II provisions with select partners, privacy protections over extraterritorial surveillance may become commonplace and part of the customary international law (CIL).

CIL, which is the accrual of general state practice into legal obligation, can be as binding on states as treaty law.[153] The debate over the CIL formation process falls on two methods: the traditional process requires "general state practice and . . . assumption of such practice as law,"[154] while the modern approach relaxes the two elements of the traditional approach and usually requires either one.[155] Scholars differ on the right approach[156] but Tier I protections will allow either approach to apply to extraterritorial surveillance. In fact, the proliferation of national data privacy laws around the world,[157] including limited developments in China,[158] suggest that data privacy is becoming a part of CIL. Given data privacy's overlap with extraterritorial surveillance, a multilateral agreement may tip the scales in estab-

150. For the U.K., see Arjun Kharpal, *UK to Phase Out Huawei Gear from 5G Networks in a Major Policy U-turn After U.S. Sanctions, Reports Say*, CNBC (Jul. 6, 2020, 12:50 AM), https://www.cnbc.com/2020/07/06/huawei-uk-5g-gear-to-be-phased-out-of-networks-in-major-policy-u-turn.html [https://perma.cc/G86T-TQPD]; for the United States, see Cheng Ting-Fang & Lauly Li, *Huawei Enters a New World: How the U.S. Ban Will Affect Global Tech*, NIKKEI ASIA (Sept. 14, 2020, 6:06 AM), https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-enters-a-new-world-How-the-US-ban-will-affect-global-tech [https://perma.cc/D7EJ-5BUN].

151. For the EU, see Iain Morris, *Europe is Showing Huawei the Exit*, LIGHT READING (Oct. 9, 2020), https://www.lightreading.com/5g/europe-is-showing-huawei-exit/d/d-id/763814 [https://perma.cc/U643-WAV6]; for India, see Amy Kazmin & Stephanie Findlay, *India Moves to Cut Huawei Gear From Telecoms Network*, FIN. TIMES (Aug. 24, 2020), https://www.ft.com/content/55642551-f6e8-4f9d-b5ba-a12d2fc26ef9 [https://perma.cc/JD3K-LUUT].

152. Yasir & Kumar, *supra* note 149.

153. *See* Michael P. Scharf, *Seizing the Grotian Moment: Accelerated Formation of Customary International Law in Times of Fundamental Change*, 43 CORNELL INT'L L.J. 439, 445 (2010).

154. Monika Zalnieriute, *An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance,* 23 INT'L J. L. OF INFO. & TECH. 99, 108 (2015).

155. *See id.* at 111.

156. *See generally id.* (describing different scholarly approaches).

157. *See id.* at 117 (referring to 101 out of 193 member states of the U.N. with data privacy laws).

158. *See id.* at 118.

lishing extraterritorial surveillance with privacy protections as part of CIL. Such developments will invariably restrain states interested in being part of a community of nations.

B. Tier II

Although Tier I's binding provisions will restrain intelligence agencies more than ever before, privacy advocates may continue to be skeptical. Indeed, the American Civil Liberties Union continues to advocate completely ending surveillance.[159] Amnesty International unequivocally considers mass surveillance to be illegal per international law.[160] Governments with pressing national security concerns are unlikely to adopt such extreme positions.[161] Nevertheless, further restraints on intelligence agencies are possible. Tier II will create suggestive limits that countries may adopt bilaterally or voluntarily, incrementally or wholeheartedly—however they choose among themselves.

Distinguishing Tier I and Tier II provisions will create a baseline of privacy protections against extraterritorial surveillance. The "scale" of increasing protections will provide human rights advocates, national security policymakers, and the general public with a common reference point. This will certainly be a springboard for a redefined policy debate; it will also become a tool for negotiations between countries. Some possible Tier II provisions include the following: (i) asking governments to publish their interpretations of domestic law surrounding surveillance; (ii) giving foreigners the same privacy protections as domestic constituents; (iii) creating neutral oversight bodies that monitor compliance; (iv) giving foreigners subject to surveillance standing to sue in domestic court; (v) creating a sanctions regime for violations; and (vi) enabling domestic agencies to gather intelligence for allies.

Given Tier II's voluntary and flexible structure, any agreement can include a more exhaustive list of provisions. Provisions can be technically refined, accurately reflecting the technological developments in surveillance. This section will introduce a Tier II provision and illustrate its possible operation.

1. Creating Oversight Mechanisms

As the efficacy of intelligence operations often depends on covert actions, arguing for international oversight is likely a non-starter to intelligence agencies. However, governments have agreed to international oversight in multiple national security arenas, most notably in nuclear weapons

159. *See End Mass Surveillance Under the Patriots Act*, AM. C.L. UNION, https://www.aclu.org/issues/national-security/privacy-and-surveillance/end-mass-surveillance-under-patriot-act [https://perma.cc/S9LR-P36D] (last visited Mar. 13, 2021).

160. *See* Ben Beaumont, *Easy Guide to Mass Surveillance*, AMNESTY INT'L (Mar. 18, 2015, 12:01 AM), https://www.amnesty.org/en/latest/campaigns/2015/03/easy-guide-to-mass-surveillance/ [https://perma.cc/LJL9-YMLX].

161. *See, e.g.*, Zalnieriute, *supra* note 154, at 122, 128–29 (discussing certain countries' mass surveillance programs in the context of national and international security).

non-proliferation. For example, the New START Treaty between the United States and Russia limits nuclear weapons for both countries, and more importantly, permits 18 on-site inspections *every year*.[162] Except in 2020, both countries have successfully implemented these inspections.[163] Similarly, the Joint Comprehensive Plan of Action (JCPOA) attempts to limit Iran from developing nuclear weapons, and empowers the International Atomic Energy Agency (IAEA) to inspect Iranian nuclear energy sites at will.[164]

The motivation behind these agreements is certainly distinguishable: Nuclear weapons can cause far greater harm than any extraterritorial surveillance. However, these agreements show that if necessary, governments may agree to oversight over sensitive national security operations. Like these agreements, oversight may only exist among a small number of countries. The Five Eyes alliance, which permits the United States, U.K., Canada, Australia, and New Zealand to share signals intelligence, may be a good place to start.[165] Information surrounding the alliance is sparse, and disclosures suggest that oversight mechanisms are limited.[166]

Nevertheless, intelligence cooperation stretching back decades creates institutional trust between these agencies that may permit instituting oversight mechanisms.[167] Domestic watchdogs of intelligence agencies in the Five Eyes countries already work together through the Five Eyes Intelligence Oversight and Review Council (FIORC).[168] The Five Eyes agreement has led to similar intelligence practices and domestic oversight mechanisms within these countries, creating "institutional convergence."[169] In fact, the oversight similarities are so profound that they could be collectively referred to as "a Five Eyes model of oversight."[170] Adding oversight mechanisms that ensure extraterritorial surveillance is regulated will be a relatively easier undertaking between these countries.

---

162. *New START Treaty*, U.S. DEP'T OF STATE, https://www.state.gov/new-start/ [https://perma.cc/8RWW-NR6F] (last visited Mar. 13, 2021).

163. *See New START Treaty Inspection Activities*, U.S. DEP'T OF STATE, https://www.state.gov/new-start-treaty-inspection-activities/ [https://perma.cc/XJ6S-ME4W] (last visited Mar. 13, 2021).

164. *See Iran Nuclear Deal: key details*, BBC NEWS (June 11, 2019), https://www.bbc.com/news/world-middle-east-33521655 [https://perma.cc/9MY7-3L4U].

165. *See* Scarlet Kim & Paulina Perlin, *Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance*, LAWFARE (Mar. 25, 2019, 9:11 AM), https://www.lawfareblog.com/newly-disclosed-nsa-documents-shed-further-light-five-eyes-alliance [https://perma.cc/E2KA-M3XF].

166. *See id.*

167. *See id.* (noting that intelligence cooperation between the Five Eyes countries began in 1955).

168. *Five Eyes Intelligence Oversight and Review Council (FIORC)*, NAT'L COUNTERINTEL. & SEC. CTR., https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc [https://perma.cc/YZ7X-3VSK] (last visited Mar. 13, 2021).

169. Richard Morgan, *Oversight through Five Eyes: Institutional Convergence and the Structure and Oversight of Intelligence Agencies* in GLOBAL INTELLIGENCE OVERSIGHT 43 (2016).

170. *See id.* at 46.

Crucially, privacy and civil liberties are part of the popular discourse in each of the Five Eyes Countries. In 2019, Canada created the National Security and Intelligence Review Agency to oversee the country's intelligence and surveillance apparatus.[171] The Snowden revelations not only prompted the United States to end some domestic surveillance through the USA Freedom Act,[172] but also motivated calls for change in New Zealand's surveillance laws.[173] Surveillance's unpopularity may motivate the Five Eyes countries to add stronger teeth to extraterritorial surveillance protections. Oversight mechanisms may spill over to other countries' part of the Tiered Code. Non-Five Eyes governments may see that oversight does not compromise intelligence capabilities, and their citizens may want the stronger protections afforded to Five Eyes' citizens. Indeed, scores of countries beyond the Five Eyes are legitimate liberal democracies.

The two-Tiered Code can achieve a hitherto elusive purpose: a baseline agreement on privacy protections for foreigners while preserving a vital national security tool. Rather than being considered the final agreement on regulating extraterritorial surveillance, the Tiered Code should be considered the first.

Conclusion

The proliferation of extraterritorial surveillance has run into a new realm of international law unexplored by traditional scholarship surrounding peacetime espionage: privacy as a human right. Existing human rights treaties like the ICCPR and UDHR cannot enforce privacy restrictions on extraterritorial surveillance. Still, the Snowden disclosures and resulting outcry prompted the United States government to unilaterally issue PPD-28, the first and most sweeping protections for foreigners in extraterritorial surveillance. Given that extraterritorial surveillance will persist as widespread practice, it needs a global agreement balancing national security needs and international human rights, such as privacy.

This Note advocates creating a Tiered Code, where Tier I permits limited extraterritorial surveillance and Tier II includes more stringent restraints that countries may voluntarily adopt or bind themselves to at a future date. Aside from providing foreigners with substantive privacy protections, the Tiered Code will also articulate a basis for continuing debates on balancing privacy and national security. Through the Tiered Code, this Note not only advocates a modest solution to limiting extraterritorial sur-

171. *See* Catharine Tunney, *Canada's National Security Landscape Will Get a Major Overhaul This Summer*, CBC NEWS (June 23, 2019, 4:00 AM), https://www.cbc.ca/news/politics/bill-c59-national-security-passed-1.5182948 [https://perma.cc/FT8C-CEX4].

172. Sabrina Siddiqui, *Congress Passes NSA Surveillance Reform in Vindication for Snowden*, GUARDIAN (June 3, 2015, 2:28 AM), https://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden/ [https://perma.cc/59PF-5W6L].

173. *See* Joy Liddicoat, *Eyes on New Zealand*, *in* GLOBAL INFORMATION SOCIETY WATCH: COMMUNICATIONS SURVEILLANCE IN THE DIGITAL AGE 178, 179–80 (2014), https://giswatch.org/sites/default/files/eyes_on_new_zealand.pdf [https://perma.cc/N837-9DYW].

veillance but also defends the viability of multilateral agreements on restraining extraterritorial surveillance. Rather than let unchecked extraterritorial surveillance operate behind closed doors, permitting limited surveillance is the better option.