2018

"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance

Asaf Lubin
Maurer School of Law - Indiana University, lubina@iu.edu

"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance

Asaf Lubin*

Abstract

The digital age brought with it a new epoch in global political life, one neatly coined by Professor Philip Howard as the "pax technica." In this new world order, government and industry are "tightly bound" in technological and security arrangements that serve to push forward an information and cyber revolution of unparalleled magnitude. While the rise of information technologies tells a miraculous story of triumph over the physical constraints that once shackled mankind, these very technologies are also the cause of grave concern. Intelligence agencies have been recently involved in the exercise of global indiscriminate surveillance, which purports to go beyond their limited territorial jurisdiction and sweep in "the telephone, internet, and location records of whole populations." Today's political leaders and corporate elites are increasingly engaged in these kinds of programs of bulk interception, collection, mining, analysis, dissemination, and exploitation of foreign communications data that are easily susceptible to gross abuse and impropriety. When called out about any of these programs, policy makers often respond to their constituencies with a shrug and a smile: we only apply these programs to foreigners, you have nothing to worry about.

---

* J.S.D. Candidate at Yale Law School (expected 2018), resident fellow with the School's Information Society Project, and a Robert L. Bernstein International Human Rights Fellow with Privacy International. I want to thank the discussants, organizers, and participants at the Tel Aviv University, Buchmann Faculty of Law's 4th Annual Workshop for Junior Scholars in Law, titled "Law in a Changing Society"; the Sussex Center for Human Rights Research Conference, titled "Challenging Human Rights Disenchantment: 50 Years on from the ICCPR and ICESCR"; the Michigan Law School's Third Annual Young Scholars Conference; the Westminster International Law Lectures Series; and the PLSC-Europe and TILTing2017 Conferences. Thank you to all of you for your thoughtful comments, critiques, and questions surrounding previous drafts of this piece. I particularly wish to thank Margo Schlanger, Tal Zarsky, Marco Roscini, Marco Longobardo, Eliza Watt, Nico Van Ejik, and Nicholas Gross, for their invaluable feedback. I wish to thank the editorial board and staff of the Chicago Journal of International Law, and in particular Ben, Zach, Caroline, and Jared. I found the process of working with CJIL to be tremendously enjoyable, and the comments and edits provided by its staff to be significantly valuable in improving the overall quality of the final piece. The below is an expression of my own academic thoughts, and in no way should be construed to reflect the views of any of the organizations with which I am associated.

While the human rights community continues to adamantly uphold the myth of a universal right to privacy, in actuality the pax technica has already erected an alternative operational code, one in which "our" right to privacy and "theirs" are routinely differentiated. One higher set of standards and protections is provided for those within the territory of the state, and a lowered set is handed to those abroad. This distinction is a common feature in the wording of electronic communications surveillance regimes and the practice of signals intelligence collection agencies, and it is further legitimized by the steadfast support of the layman general public. Nonetheless, a liberal defense of this distinction is non-existent in the literature, as human rights scholars continue to oppose it arguing that it reflects in-group biases and violates the principle of non-discrimination.

In this piece I try to make the liberal case for the distinction, justifying, in a limited sense, certain legal differentiations in treatment between domestic and foreign surveillance. These justifications, as I show in the piece, are grounded in practical limitations in the way foreign surveillance is conducted, both generally and in the digital age more specifically. I will further make a controversial claim: that in fighting this absolutist battle for universality, human rights defenders are losing the far bigger war over ensuring some privacy protections for foreigners in the global mass surveillance context. Accepting that certain distinctions are, in fact, legitimate, creates an opportunity to step outside the bounded thinking of one-size-fits-all human rights standards for all surveillance practices, and begin a much needed conversation on what a uniquely tailored human rights regime might look like in the foreign surveillance context. This piece, thus, makes a first attempt at sketching out such a tailored framework, with the hope of bridging the divide between privacy scholars and national security practitioners.

Table of Contents

I. INTRODUCTION

On March 18, 2015, Amnesty International reported the outcome of a remarkable survey conducted with the help of a British company, YouGov, studying worldwide public reactions to the cascade of revelations by former National Security Agency (NSA) contractor-turned-whistle-blower, Edward Snowden.[1] The report analyzed the attitudes of roughly fifteen thousand people from across thirteen countries towards the lingering leaks surrounding the pervasiveness of modern-day governmental mass surveillance programs. One of the study's most revealing conclusions concerned the extent to which the majority of those interviewed reported tolerance towards surveillance directed at foreign nationals, as opposed to surveillance directed against citizens of their state. As summarized by Professor Chris Chambers:

> In all surveyed countries, more people were in favour of their government monitoring foreign nationals (45%) than citizens (26%). In some countries the rate of agreement for monitoring foreign nationals was more than double that of citizens. For instance, in Canada only 23% believed their government should monitor citizens compared with 48% for foreign nationals. In the US, 20% believed their government should monitor citizens compared with 50% for foreign nationals.[2]

Even more intriguing was the number of people who vehemently condemned domestic governmental surveillance while simultaneously fully condoning foreign surveillance. Nearly one in every three respondents in the U.S. shared this position.[3] Amongst the "Five Eyes" Member States,[4] on average, one

---

1 *Global Opposition to USA Big Brother Mass Surveillance*, AMNESTY INT'L (Mar. 18, 2015), http://perma.cc/AJL9-R77L.

2 Chris Chambers, *The Psychology of Mass Government Surveillance: How Do the Public Respond and Is It Changing Our Behaviour?*, THE GUARDIAN (Mar. 18, 2015), http://perma.cc/HVF2-VFTG.

3 *Id.*

4 The Five Eyes Intelligence Sharing Community grew out of the intimate cooperation between the U.K. and the U.S. during the Second World War, predominantly surrounding the breaking of the German Enigma by British and American crypto-analysts. This cooperation was formalized during the war, in the form of an agreement, signed on June 10, 1943, between British Government Code and Cipher School and the U.S. War Department in regard to certain "special intelligence." It was in fact the British government that approached the U.S. in 1945 to propose "continued peacetime SIGINT cooperation, based on their shared wartime experience." Martin Rudner, *Hunters and Gatherers: The Intelligence Coalition against Islamic Terrorism*, 17 INT'L J. INTELLIGENCE AND COUNTERINTELLIGENCE 193, 196 (2004). It was similarly the British who dispatched missions to Canada and Australia to elicit their participation in an expanded arrangement. *Id.* In doing so the British were hoping to establish a "Commonwealth SIGINT network under British leadership with global surveillance capability." *Id.* Between the first version of the UKUSA Agreement and the third reiteration of it, adopted on May 10, 1955, new appendices were introduced, which improved the status of Canada, Australia, and New Zealand to the position of "UKUSA-Collaborating Commonwealth Countries." Paul Farrell, *History of 5-Eyes—Explainer*, THE GUARDIAN (Dec. 2, 2013), http://perma.cc/4WPZ-LMKB. While the 1955 Agreement set certain restrictions on the

in every five respondents believed that the government should in fact continue to spy on *them*, but should avoid spying on *us* (23 percent of respondents in Canada, 22 percent of respondents in New Zealand, 17 percent of respondents in Australia, and 16 percent of respondents in Britain).[5] Three days prior to the publishing of Amnesty's report, the Pew Research Center published its own findings, which were strikingly similar. The March 16th, 2015 survey, which focused only on American public opinion, found 60 percent of respondents believed that it was okay for the government "to monitor communications of foreign leaders" and an additional 54 percent believed it was similarly acceptable for the government "to monitor communications of foreign citizens."[6] Nonetheless, at the very same time, 57 percent of those surveyed believed wholeheartedly that it would be completely unacceptable for the government "to monitor communications of U.S. citizens."[7]

In his evocative novel *Nineteen Eighty-Four*, George Orwell describes "doublethink" as a psychological phenomenon induced by the dystopian ruling Party. According to Orwell's masterpiece, doublethink is:

> To know and not to know, to be conscious of complete truthfulness while telling carefully constructed lies, to hold simultaneously two opinions which cancelled out, knowing them to be contradictory and believing in both of them, to use logic against logic, to repudiate morality while laying claim to it, to believe that democracy was impossible and that the Party was the guardian of democracy, to forget whatever it was necessary to forget, then to draw it back into memory again at the moment when it was needed, and then promptly to forget it again, and above all, to apply the same process to the process itself—that was the ultimate subtlety: consciously to induce unconsciousness, and then, once again, to become unconscious of the act of hypnosis you had just performed. Even to understand the word "doublethink" involved the use of doublethink.[8]

It begs the question, therefore: is our collective willingness to tolerate our government's surveillance when it's done to others, while rejecting it when it's done to us, a form of Orwellian "doublethink"? Are these two fundamental beliefs

---

sharing of intelligence with these states and assigned them certain tasks, today all five members seem to operate on a more equal footing. *See* Rudner, *supra*, at 197–98. For further reading on the Five Eyes Intelligence Arrangement, see U.K.-U.S. Communications Intelligence Agreement (3d ed. May 10. 1955), ¶¶ 1–5, 10, Appendix E, http://perma.cc/42SJ-Z6KP [hereinafter UKUSA Agreement]; Privacy Int'l v. Sec'y of State for the Foreign and Commonwealth Affairs et al., Case No. IPT/13/92/CH, Witness Statement of Charles Blanford Farr on Behalf of the Respondents, ¶ 25, Investigatory Powers Tribunal (May 16, 2014), http://perma.cc/P9HW-HFEJ.

5 Chambers, *supra* note 2.

6 Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RES. CTR. (Mar. 16, 2015), http://perma.cc/YW5K-2Y85.

7 *Id.*

8 GEORGE ORWELL, NINETEEN EIGHTY-FOUR 36 (1949).

mutually contradictory? Chambers, a professor of cognitive neuroscience, was quick to brand this sort of thinking as a fallacy. For him, those who refused to accept the legitimacy of domestic surveillance while simultaneously advocating for foreign surveillance were all surely suffering from an *intergroup bias*, or "in-group-favouritism/out-group derogation"[9]: the systematic tendency of humans to evaluate the members of their own membership group more favorably than the members of other membership groups.[10] For Chambers, therefore, the visible chasm between diverging public opinion towards domestic and foreign surveillance could only be explained through some form of a primitive xenophobic prejudice.

In many respects, Chambers' argument echoes the positions of human rights experts and non-governmental organizations (NGOs) that have long been fighting against intelligence legislation that establishes different legal regimes for domestic and foreign surveillance. Whereas the former is subjected to greater oversight and more robust procedural safeguards, the latter, as a matter of consistent state practice, is provided with few, if any, such protections. As I will discuss in Sections II and III, human rights activists denounce this conceptualization, putting forward the persuasive argument that the right to privacy, indeed any human right, is inherently universal, and therefore one's entitlement to privacy protections should persist, regardless of nationality or place of residency. According to this account, insofar as a piece of legislation introduces such distinctions, it must be denounced as a xenophobic violation of the principle of non-discrimination. It is this broad human rights stance that this paper aims to challenge. Are there any real justifications for legally distinguishing between domestic and foreign surveillance? Insofar as there are, what does that mean for the human right to privacy as it relates to the regulation of foreign mass surveillance?

The digital age brought with it a new epoch in global political life, one neatly coined by Professor Philip Howard as the "pax technica."[11] In this new world order, government and industry are "tightly bound" in technological and security arrangements that serve to push forward an information and cyber revolution of unparalleled magnitude.[12] While the rise of information technologies tells a

---

9 *See* Chambers, *supra* note 2.

10 Miles Hewstone, Mark Rubin & Hazel Willis, *Intergroup Bias*, 53 ANN. REV. PSYCHOL. 575, 576 (2002).

11 PHILIP N. HOWARD, PAX TECHNICA: HOW THE INTERNET OF THINGS MAY SET US FREE OR LOCK US UP 145–46 (2015) ("The pax technica is a political, economic, and cultural arrangement of social institutions and networked devices in which government and industry are tightly bound in mutual defense pacts, design collaborations, standards setting, and data mining.").

12 *See id.* at 146–47.

miraculous story of humanity's triumph over the physical constraints that once shackled it, these very technologies are also the cause of grave concern. Intelligence agencies have been recently involved in the exercise of global indiscriminate surveillance, which purports to go beyond the agencies' limited territorial jurisdiction and sweep in "the telephone, internet, and location records of whole populations."[13] Today's political leaders and corporate elites are increasingly engaged in these kinds of programs of bulk interception, collection, mining, analysis, dissemination, and exploitation of foreign personal communications data, all of which are easily susceptible to gross abuse and impropriety.[14] When called out about any of these programs, policymakers would often respond to their constituencies with a shrug and a smile: *we only apply these programs to foreigners; you have nothing to worry about*.[15]

While the human rights community continues to adamantly uphold the myth system of a universal right to privacy (discussed in Section II.B), in actuality the pax technica has already erected and solidified an alternative operational code in which "our" right to privacy and "theirs" are routinely differentiated. This

---

13 Barton Gellman, *Edward Snowden, after Months of NSA Revelations, Says His Mission's Accomplished*, WASH. POST (Dec. 23, 2013), http://perma.cc/LR4H-EEBJ. *See generally* THE SNOWDEN READER (David P. Fidler ed., 2015).

14 *See* BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 4–5 (2015):

> Here is what's true. Today's technology gives governments and corporations robust capabilities for mass surveillance. Mass surveillance is dangerous. It enables discrimination based on almost any criteria: race, religion, class, political beliefs. It is being used to control what we see, what we can do, and, ultimately, what we say. It is being done without offering citizens recourse or any real ability to opt out, and without any meaningful checks and balances. It makes us less safe. It makes us less free. The rules we had established to protect us from these dangers under earlier technological regimes are now woefully insufficient; they are not working. We need to fix that, and we need to do it very soon.

15 One commonly cited example is President Obama's reaction to the disclosures surrounding the PRISM internet communications collection program. On June 7, 2013, during a press conference in San Jose, California, President Obama was asked to address the reports, which triggered the following statement:

> [W]ith respect to the internet and emails—this does not apply to U.S. citizens and it does not apply to people living in the United States . . . . All I can say is that in evaluating these programs they make a difference in our ability to anticipate and prevent possible terrorist activity . . . they are under strict supervision by all three branches of government and that they do not involve . . . reading the emails of U.S. citizens or U.S. residents absent further action by a federal court.

ABC News, *Obama on Prism, Phone Spying Controversy: "No One Is Listening to Your Phone Calls,"* YOUTUBE 3:56–4:07, 7:47–8:25 (June 7, 2013), https://www.youtube.com/watch?v=rENTl5JKzlQ. Facebook CEO Mark Zuckerberg was later quoted reacting to President Obama's statement by saying that "some of the government's statements have been particularly unhelpful . . . like, oh, we only spy on non-Americans . . . the government blew it." Megan Garber, *Mark Zuckerberg's Advice to the NSA: Communicate*¸ THE ATLANTIC (Sept. 18, 2013), https://perma.cc/LET7-53G5.

distinction is a common feature in the wording of electronic communications surveillance laws, and of the practice of signals intelligence collection agencies (SIGINT), and it is further legitimized, as we have witnessed, by the steadfast support of the lay public.

In this piece I will offer some pushback to the human rights agenda, trying to justify, in a limited sense, certain legal differentiations in treatment between domestic and foreign surveillance. These justifications are not rooted, as I will show, in xenophobic biases but rather in practical limitations in the way foreign surveillance is conducted, both generally and in the digital age more specifically. I will further make a controversial claim, that in fighting this absolutist battle for universality, human rights defenders are losing the far bigger war over ensuring privacy protections for foreigners in the global surveillance context. Accepting that certain distinctions are, in fact, legitimate, would give us an opportunity to step outside the bounded thinking of a one-size-fits-all European Court of Human Rights (ECtHR) surveillance jurisprudence. We could begin a much-needed conversation on what tailored human rights standards might look like for foreign surveillance activities.

My analysis proceeds in three parts. In Section II of this Article, I examine the myth system and the operational code surrounding foreign surveillance. I compare the arguments raised by the vast majority of the international community and legal scholarship as they relate to privacy protections and the principle of non-discrimination with the vast practice of states in the organization of their foreign surveillance apparatuses. I then present the way this debate is reflected in a groundbreaking case, currently pending, before the ECtHR surrounding the Government Communications Headquarters (GCHQ) and NSA joint global mass surveillance programs.

In Section III of this Article, I shift the focus to various arguments that have been raised in the literature to justify a differentiation in legal treatment between surveillance at home and surveillance abroad. I will first examine claims raised by the political right that seem to suggest that privacy in the digital age has no intrinsic value of its own and should not be obligatorily applied in an extraterritorial setting. I will challenge these positions to reaffirm the international right to privacy. I will then address claims from commentators on the political left, who have erroneously focused their attention solely on historical biases to discredit the differentiation. I will propose, instead, three new arguments in defense of the need to establish different legal regimes for domestic and foreign surveillance: (1) disparity in the political-jurisdictional reach of state agencies, (2) disparity in the technological reach of state agencies, and (3) disparity in harms from a potential abuse of power.

Having established that setting different human rights regimes for domestic and foreign surveillance is something that states not only do, but something that they *can't not do*, the final Section of this Article will offer a proposal for a new

human rights framework for foreign surveillance. I will particularly point out areas where one could anticipate divergence from existing ECtHR jurisprudence on domestic surveillance. This framework is aimed at beginning a conversation, and by no means ending it, which I hope will help bridge the gap between the practice of state surveillance agencies and the deep-seated commitments of human rights experts and organizations.

II. THE OPERATIONAL CODE AND MYTH SYSTEM OF FOREIGN SURVEILLANCE

Cold War CIA analyst James Jesus Angleton masterfully described the labyrinthine world of espionage as a "wilderness of mirrors."[16] Indeed, intelligence gathering is an area of human behavior where regulators must accept, perhaps even welcome, some form of *lex imperfecta* and *lex simulata* as inevitable.[17] It is a field of study where one should routinely ascertain which is the law-in-the-books and which is the law-in-practice.[18] This is especially true in the light of the influence that technology has on the continuous evolution of the field. As new technologies are introduced into the work of surveillance agencies they lead to changes "on the order of our sensory lives."[19]

This conceptualization, common to the literature of the New Haven School of International Law, has been a feature in the writing of Professor W. Michael

---

16 For further reading, see DAVID C. MARTIN, WILDERNESS OF MIRRORS 10 (1980).

17 Professor W. Michael Reisman identifies the concept of *lex imperfecta* as "laws without teeth," laws devised so that no remedy or sanction may be invoked following their violation. W. MICHAEL REISMAN, FOLDED LIES: BRIBERY, CRUSADES, AND REFORMS 29 (1979). Reisman explains that a common purpose of the *lex imperfecta* as a legal construct is an "elite design for dealing with aggravated myth system and operational code discrepancies." *Id.* The *lex simulata* serves a similar purpose but in a more nuanced way. It is a "statutory instrument apparently operable, but one that neither prescribers, those charged with its administration, nor the putative target audience ever intend to be applied." *Id.* at 31. By doing so, the *lex simulata* helps to "reaffirm on the ideological level that component of the myth, to reassure peripheral constituent groups of the continuing vigor of the myth . . . ." *Id.* at 31–32.

18 *See* Roscoe Pound, *Law in Books and Law in Action*, 44 AM. L. REV. 12, 12–13 (1910):

> When tradition prescribed case-knives for tasks for which pickaxes were better adapted, it seemed better to our forefathers, after a little vain struggle with case-knives, to adhere to principle—but use the pickaxe. They granted that law ought not to change. Changes in law were full of danger. But, on the other hand, it was highly inconvenient to use case-knives. And so the law has always managed to get a pickaxe in its hands, though it steadfastly demanded a case-knife, and to wield it in the virtuous belief that it was using the approved instrument.

19 MARSHALL MCLUHAN & QUENTIN FIORE, WAR AND PEACE IN THE GLOBAL VILLAGE 4 (1968) (continuing, the quote explains: "It is the shift in this order, altering the images that we make of ourselves and our world, that guarantees that every major technical innovation will so disturb our inner lives that wars necessarily result as misbegotten efforts to recover the old images.").

Reisman. Reisman has noted that "in law things are not always what they seem,"[20] further highlighting the existence of "two 'relevant' normative systems: one which is supposed to apply and which continues to enjoy lip service among elites and one which is actually applied."[21] He has coined them the "myth system" and the "operational code." It is important to note in this regard, as Reisman clarifies, the difference between a "myth system" and pure legal fiction:

> [T]he myth system is *not* widely appreciated as consciously false. It does not express values that are obsolete. On the contrary: it affirms values that continue to be important socially and personally. Although not applied in the "jurisdiction" of the operational code, the myth system may yet influence decision-making.
>
> Precisely because discrepancies between myth system and operational code can erode the credibility of the myth system, maintenance of belief in the myth system is a dynamic process requiring ongoing contributions from many. By contrast, those who practise the operational code try to obscure it from the general public. But there is an almost symbiotic relationship between myth system and operational code, with the latter providing a degree of suppleness and practicality that the myth system could not achieve without changing much of its content and procedure of application.[22]

It is in the context of this "dynamic process" and "symbiotic relationship" that we must understand the universal nature of privacy protections and the practice of mass foreign surveillance by states. In this Section, I wish to lay out the distinction between the myth and the code, not in an attempt to undervalue the myth, but rather in the hope of bringing the code closer to it (as it has seemed to have strayed away too far).

A. The Operational Code

On March 19, 2015, French Prime Minister Manuel Valls introduced a controversial "Intelligence Act" as a reaction to the Charlie Hebdo shooting, and the bill was made into law on July 24, 2015.[23] On November 30, 2015, the French Government adopted a second law, the "International Intelligence Act," as an addendum to the original legislation, focusing solely on foreign surveillance.[24] In

---

20 REISMAN, FOLDED LIES, *supra* note 17, at 7.

21 W. Michael Reisman, *Myth System and Operational Code*, 3 YALE STUD. WORLD PUB. ORD. 229, 230 (1977) (footnote omitted).

22 W. Michael Reisman, *On the Causes of Uncertainty and Volatility in International Law*, *in* THE SHIFTING ALLOCATION OF AUTHORITY IN INTERNATIONAL LAW: CONSIDERING SOVEREIGNTY, SUPREMACY AND SUBSIDIARITY 44–45 (Tomer Broude & Yuval Shany eds., 2008) (emphasis in original).

23 Loi 2015-912 du 24 juillet 2015 relative au renseignement [Law 2015-912 of July 24, 2015 relating to Intelligence], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July 26, 2015, p. 12735 [hereinafter Intelligence Act].

24 Loi 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications

addition to reaffirming existing regulations and practices, which were already substantively permissive, the new legislation extended even more powers to the French intelligence and security community. In particular, it institutionalized two different legal regimes, with different standards of privacy protections for domestic and foreign surveillance.

For example, whereas the content of domestic communications could now be stored for up to thirty days, and their metadata for up to four years,[25] the content of foreign communications could now be stored for up to twelve months, and their metadata for up to six years.[26] Similarly, foreign encrypted information could be stored for up to eight years, instead of the six mandated under the domestic regulation.[27] Even more startling is that, in accordance with the new Intelligence Act, spying on parliamentarians, judges, lawyers, and journalists within France would now be dependent on a prior consultation in a mandatory plenary session[28] with an independent oversight body known as "CNCTR."[29] The

électroniques internationales [Law 2015-1556 of Nov. 20, 2015 relating to Surveillance Measures of International Electronic Communications], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Dec. 1, 2015, p. 22185 [hereinafter International Intelligence Act]. The International Intelligence Act was originally a section of the intelligence bill, however, on July 23, 2015, the Constitutional Court of France struck that section out of the law. The Court found that the conditions established in that section were ill-defined (namely because the original bill referenced the collection of "information which originated from outside of French territory," a term which the Court found to be ambiguous in the age of internet communications). *See* Conseil constitutionnel [CC] [Constitutional Court] decision No. 2015-713 DC, July 23, 2015, J.O. 12751. The new International Intelligence Act was thus a reaffirmation of the original section with only minor alterations. In this regard, the new law now applies to the monitoring of communications that are "sent or received abroad," which entails that their "communications subscription number, or identifiers" are not traceable to the national territory of France. Art. L. 854-1. As is clarified in Art. L. 854-8, in case it is later discovered that information collected under the "international intelligence law" provisions involves wholly domestic communications, those must immediately be subjected to the safeguards listed in the Intelligence Act. S*ee* Intelligence Act, *supra* note 23, at Arts. L. 852-1, 822-2, 822-4.

25 *See* Intelligence Act, *supra* note 23, at Art. L. 822-2. Note that the law distinguishes between information intercepted from regular communication operations and information intercepted through special operations involving the installment of recording devices and cameras in private vehicles or premises. Such information may be collected for a period of up to 120 days. *Id.*

26 *See* International Intelligence Act, *supra* note 24, at Art. L. 854-5. For information on the retention periods in French laws in English, see Félix Tréguer, *Internet Surveillance in France's Intelligence Act*, HAL ARCHIVES OUVERTES (Oct. 2016), https://perma.cc/E4CQ-99NZ.

27 *Id.* For encrypted materials periods start after decyption.

28 *See* Intelligence Act, *supra* note 23, at Art. L. 821-7.

29 The National Commission for the Control of Intelligence Techniques (Commission Nationale de Contrôle des Techniques de Renseignement, CNCTR) (previously known as the The National Commission for the Control of Security Interceptions, La Commission Nationale de Contrôle des Interceptions de Sécurité, CNCIS), is the primary oversight body over France's intelligence agencies. *See* CODE DE LA SÉCURITÉ INTÉRIEURE (CODE OF INTERNAL SECURITY) Art. L243-8–L243-12 (Fr.) (introducing CNCIS). The CNCTR is comprised of nine members: (a) two deputies

International Intelligence Act, on the other hand, did not establish a similar consultation process, thus allowing for the surveillance of foreign officeholders outside of France without requiring any independent *ex ante* review of the request.[30]

France is not alone, as the Washington-based Center for Democracy and Technology had concluded in a 2013 report: "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."[31] From the U.S. to Russia, from

---

and two senators designated respectively for the duration of their term by the National Assembly and Senate respectively, ensuring a "pluralistic representation of parliament"; (b) two members of the State Council appointed by the Vice President of the State Council; (c) two judges outside of the hierarchy of the Cour de Cassation, appointed jointly by the President and by the Attorney General of the Cour de Cassation, and (d) a person qualified for his knowledge in electronic communications, appointed on the proposal of President of the Regulatory Authority for Electronic Communications and Postal (La Autorité de Régulation des Communications Électroniques et des Postes). CODE DE LA SÉCURITÉ INTÉRIEURE, *supra*, at Art. L831-1. The chairperson of the CNCTR is appointed by the President of France for a period of six years. *Id.* In the context of domestic surveillance, the CNCTR may issue opinions prior to the authorization of communications interception made by the Prime Minister. *Id.* at Art. L821-1; for foreign surveillance operations, including with regards to intelligence gathering techniques not the subject of a specific request or authorization, the Commission should be granted access to all relevant information necessary for the accomplishment of its mission. Excluded are intelligence communicated by foreign agencies or by international organizations, or which "could inform the Commission, directly or indirectly, of the identity" of specific intelligence sources. *Id.* at Art. L833-2. The Commission may additionally review complaints submitted by persons with "direct and personal interest." *Id.* at Art. L243-9. For more information on the effectiveness of the CNCTR, see Jacques Follorou, *Un An après Sa Création, la Commission chargée du Contrôle du Renseignement Affirme Son Indépendance*, LE MONDE (Dec. 13, 2016), http://www.lemonde.fr/societe/article/2016/12/13/premier-bilan-de-la-commission-chargee-du-controle-du-renseignement_5047987_3224.html.

30 For more on the French foreign surveillance legislation, as well as the laws in the U.K. and Germany, see Asaf Lubin, *A New Era of Mass Surveillance is Emerging across Europe*, JUST SECURITY (Jan. 9, 2017), http://perma.cc/N7HK-CTH2.

31 Ira Rubinstein et al., *Systematic Government Access to Personal Data: A Comparative Analysis*, CTR. FOR DEMOCRACY AND TECH. 19–20 (Nov. 13, 2013), http://perma.cc/QW2S-ED5B. Of course this statement should be qualified in two regards. First, and contrary to traditional wisdom, not all countries engage in interstate espionage. Consider the Central European microstate of Liechtenstein, which does not even hold an intelligence agency and which security is maintained through the work of a small national police force (Landespolizei) comprised of 80 officers and roughly 40 civilian staff. *The Principality*, LIECHTENTEIN, https://perma.cc/H6DH-JBMV (last visited Nov. 18, 2017). Likewise, the island country of Grenada does not run its own intelligence apparatus, let alone a regular military force, which perhaps explains why the country's national bird is the Grenada dove. In both these scenarios there is no lax foreign surveillance regulation, simply because there is no foreign surveillance to begin with. Moreover, there are countries that do not distinguish between their foreign and domestic surveillance because their domestic surveillance regulation is already permissive enough, setting, if any, minimal restrictions, safeguards, and oversight. In such a scenario there is simply no need to set different, more lenient, procedures for foreign surveillance. As the report noted, in this regard, "China and India stand out due to almost total lack of protection and oversight in both law enforcement and national security." *Id.* at 17.

Germany to the United Kingdom, from Canada to Australia, internal legislation seems to denote two separate legal regimes, one for those within the borders of the country, and another for foreigners.[32] In fact, certain countries, like Israel and Egypt, for example, have even gone a step further by only regulating, through primary legislation, the domestic surveillance activities of their intelligence agencies. Foreign surveillance is thus authorized through confidential executive orders and secret internal guidelines, naturally allowing for even greater flexibility and leniency.[33]

B. The Myth System

Despite this prevalent state practice, U.N. experts, human rights treaty bodies, and privacy NGOs have been adamant about protecting the myth of a singular and universal right to privacy. By doing so, they seem to "abet the deception, avoiding the truth like someone pulling blankets over his head to avoid the cold reality of dawn."[34] Let us review a few examples of this peculiar behavior from recent years. In 2014, the U.N. Office of the High Commissioner for Human Rights issued a report following a General Assembly Resolution on the *Right to Privacy in the Digital Age*. In that report, Commissioner Pillay addressed the foreign-domestic surveillance debate and noted the following:

> [There exist] ongoing discussions on whether "foreigners" and "citizens" should have equal access to privacy protections within national security

Other examples might include Pakistan and Namibia. *See, for example*, *State of Privacy: Pakistan*, PRIVACY INT'L (June 28, 2017), http://perma.cc/K9XZ-24E6; Privacy Int'l, Namibia: Submission to the Universal Periodic Review of the 24th Sess. (June 2015), http://perma.cc/N4Q8-HCAF. In a similar manner, not all countries opt to regulate their intelligence activities through primary legislation. In those cases, both domestic and foreign surveillance are equally subjected to undisclosed executive orders and internal guidelines, which by their nature allow significant leeway to intelligence agencies operating under a cloak of secrecy.

32 *See* Rubinstein et al., *supra* note 31, at 3 ("Statutory frameworks for surveillance tend to be geographically focused and draw distinctions between communications that are wholly domestic and communications with one or both communicants on foreign soil. Moreover, statutory frameworks, as far as we can tell, often draw a distinction between the collection activities that an intelligence service performs on its own soil and the activities that it conducts extraterritorially."). This report surveyed legislation in thirteen countries including Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the U.K., and the U.S. For a particular focus on legislation in the Five Eyes member states, see Rep. of the Off. of the U.N. High Comm'r for Hum. Rts., The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, n.30 (June 30, 2014) [hereinafter OHCHR Report]; Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81, 88–89 (2015).

33 For more information on Egyptian surveillance regulation, see *State of Privacy: Egypt*, PRIVACY INT'L (Mar. 14, 2017), http://perma.cc/5Q39-VUVV. For more information on Israeli regulation, see Ze'ev Segal, *A Legal Framework for the Mossad*, HAARETZ (Mar. 1, 2010), http://perma.cc/LK77-7LH4.

34 Reisman, *Myth System*, *supra* note 21, at 237.

> surveillance oversight regimes. Several legal regimes distinguish between the obligations owed to nationals or those within a State's territories, and non-nationals and those outside, or otherwise provide foreign or external communications with lower levels of protection. If there is uncertainty around whether data are foreign or domestic, intelligence agencies will often treat the data as foreign (since digital communications regularly pass "off-shore" at some point) and thus allow them to be collected and retained. The result is significantly weaker—or even non-existent—privacy protection for foreigners and non-citizens, as compared with those of citizens.
>
> International human rights law is explicit with regard to the principle of non-discrimination. Article 26 of the International Covenant on Civil and Political Rights [(ICCPR)] provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law" and, further, that "in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." These provisions are to be read together with articles 17, which provides that "no one shall be subjected to arbitrary interference with his privacy" and that "everyone has the right to the protection of the law against such interference or attacks," as well as with article 2, paragraph 1.[35]

That very year, the Special Rapporteur on Counter Terrorism, Ben Emmerson, issued his own analysis of the human rights implications of mass digital surveillance. In that report, Emmerson reiterated the significance of Article 26 of the ICCPR and concluded: "States are legally obliged to afford the same privacy protection for nationals and non-nationals and for those within and outside their jurisdiction. Asymmetrical privacy protection regimes are a clear violation of the requirements of the Covenant."[36]

---

35 OHCHR Report, *supra* note 32, at ¶¶ 35–36 (footnote omitted).

36 Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, *Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, ¶ 62, U.N. Doc. A/69/397 (Sept. 23, 2014). The Special Rapporteur reiterated this position in her 2017 report to the Human Rights Council, noting that:

> > [There are] serious and continuing concerns around extraterritorial mass surveillance programmes, and proliferation of laws that authorize asymmetrical protection regimes for nationals and non-nationals. Such laws exist in Germany, France, and the United States. The Special Rapporteur recalls that differential treatment of nationals and non-nationals, and of those within or outside a State's jurisdiction, is incompatible with the principle of non-discrimination, which is a key constituent of any proportionality assessment.
>
> Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, *Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, ¶ 33, U.N. Doc. A/HRC/34/61 (Feb. 21, 2017) (internal citations omitted).

The Human Rights Committee has similarly echoed this position, hammering, in both its List of Issues to reviewed states and Concluding Observations, the claim that safeguards against arbitrary interference with the right to privacy must be guaranteed to "all individuals, regardless of nationality and physical location when intercepted."[37]

In his inaugural report to the General Assembly, issued in August 2016, the Special Rapporteur on the Right to Privacy, Joseph Cannataci, had also joined the choir. Criticizing the German Draft Law on the Federal Intelligence Service (the Bundesnachrichtendienst, or BND), the Special Rapporteur stated:

> [W]hat is the true value of laws that discriminate between nationals and non-nationals? Especially since, in terms of article 17 of the International Covenant on Civil and Political Rights, everybody enjoys a right to privacy irrespective of nationality or citizenship, so one must ask how useful and appropriate, never mind legal, such types of provisions may be . . . . [The German] interpretation is as unacceptable as any claim in the laws of other countries that fundamental human rights protection is only restricted to its own citizens or residents.[38]

Human rights scholars have also taken up this approach. The most decisive of them was Douwe Korff, who submitted an expert opinion for the Committee of Inquiry of the Bundestag into the Five Eyes Global Surveillance Systems.[39] In his opinion he writes:

> In simple terms: the prohibition of discrimination in international human rights law is absolutely fundamental to that already fundamental area of law. Any state laws or practices that appear *prima facie* to be in violation of that

---

37 U.N. Hum. Rts. Comm., List of Issues in Relation to the Initial Rep. of S. Afr., ¶ 26, U.N. Doc. CCPR/C/ZAF/Q/1 (Aug. 19, 2015); U.N. Hum. Rts. Comm., Concluding Observations on the Seventh Periodic Rep. of the United Kingdom of Great Britain and Northern Ireland, ¶ 24, U.N. Doc. CCPR/C/GBR/CO/7 (Aug. 17, 2015) [hereinafter Concluding Observations on U.K.] ("[M]easures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance."); U.N. Hum. Rts. Comm., Concluding Observations on the Fourth Periodic Rep. of the United States of America, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014) [hereinafter Concluding Observations on U.S.].

38 Joseph Cannataci (Special Rapporteur on the Right to Privacy), *Rep. of the Special Rapporteur on the Right to Privacy*, ¶ 36, U.N. Doc. A/71/368 (Aug. 30, 2016). The Special Rapporteur concluded by noting that:

> The new draft German law [which continues to make distinctions between German and non-German citizens] loses out on a precious opportunity to clarify that the right to privacy and related safeguards applies to individuals irrespective of nationality, citizenship or location, or indeed whether the surveillance is carried out inside or outside Germany.

Id.

39 Douwe Korff, Expert Opinion Prepared for the Committee of Inquiry of the Bundestag into the "5EYES" Global Surveillance Systems Revealed by Edward Snowden, Committee Hearing (June 3, 2014), http://perma.cc/ZWC4-XU77.

> principle must be subject to the most rigorous assessment as to the necessity of the apparent distinctions . . . [T]he mere fact that a person who is to be spied upon is a "foreigner," or that the communications that are to be intercepted occur outside the spying state's territory, can in my opinion not be sufficient reason to make such a distinction.
>
> In other words, historical laws that contain such distinctions (often at their very heart) must be fundamentally rewritten. This must be done in and by Germany as much as in and by the states accused of having established a global surveillance system.[40]

In a groundbreaking case currently pending before the European Court of Human Rights, ten human rights NGOs are attempting to trumpet this privacy universality agenda.[41] The NGOs are challenging GCHQ's mass surveillance programs and intelligence sharing arrangements, in part because of prima facie discrimination.[42] The Regulation of Investigatory Powers Act (RIPA), which has since been overhauled by the British Parliament in 2016, distinguished between external and internal communications, and set different degrees of protections for each.[43] The NGOs are claiming that this distinction violates Article 14 of the European Convention on Human Rights (ECHR) (the equivalent of Article 26 of the ICCPR).[44]

This would be the first time that the ECtHR, let alone any international court, could expressly decide the question of whether distinctions between

---

40 *Id.* at 26. See also arguments raised by Milanovic:

> [I]f human rights treaties do apply to a particular interception (or other surveillance activity), and the intercepting state draws distinctions on the basis of nationality (as many do), this potentially implicates not only the privacy guarantees in the treaties, but also their provisions on equality and non-discrimination. A nationality-based distinction would be justified only if it pursues a legitimate aim (such as the protection of national security) and the measures taken serve that aim and are proportionate. If the rationale for protecting privacy interests is the value of the autonomy and independence of individuals—of enabling them to lead their lives without state intrusion—then distinctions based on nationality alone would seem hard to justify . . . .
>
> In sum, one cannot escape the conclusion that under the moral logic of human rights law, citizens and non-citizens are equally deserving of protections of their rights generally, and privacy specifically.

Milanovic, *Human Rights Treaties*, *supra* note 32, at 99–101. *See also* David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SECURITY (Oct. 29, 2013), http://perma.cc/89P2-TEVX.

41 *See* 10 Human Rights Orgs. v. United Kingdom, Applicants' Reply to Observations of the Government of the U.K., App. No. 24960/15, Eur. Ct. H.R., (Sept. 26, 2016), http://perma.cc/QF8M-A9YB [hereinafter Applicants' Reply].

42 *Id.* at ¶ 22.

43 This distinction between internal and external communications carried through into the 2016 Investigatory Powers Acts. For further analysis, see Lubin, *supra* note 30.

44 Applicants' Reply, *supra* note 41, at ¶¶ 262–71.

nationals and foreigners can ever be justified in foreign surveillance legislation.[45] In the following Section, I will be examining the arguments that have been raised both in the past, and in the context of this case, for and against such distinctions. The Section will try to show how the scholarly discourse has so far avoided the real issues that stand at the heart of the distinction.

III. DISTINGUISHING FOREIGN FROM DOMESTIC SURVEILLANCE

The topic of distinctions between nationals and foreigners in governmental policies and legislative acts is by no means a new one. As early as the Babylonian Talmud, we know that there existed conversations on the moral justifications for providing preferential treatment to one's own based on geopolitical lines.[46] This debate surfaces in conversations over nationalism and cosmopolitanism in the political philosophy of international distributive justice, and similarly over contractarian, rights-based, and goals-based models of cosmopolitanism.[47] The conversation also extends to the question of entitlements based on political membership in constitutional designs, for example as they relate to transnational migration flows.[48] This piece generally follows the above discourse, adopting a mild cosmopolitan approach that is willing to accept "nationalist concerns about viability" without undermining cosmopolitan moral standards.[49] In Reismanian terms, it means a willingness to acknowledge the core practical reasoning that undergirds the operational code without challenging the foundational values behind the myth system. In fact, if the myth system is to continue to offer individual agencies any "general guidelines for orientation and valuation" of their

---

45 Interestingly enough, this is not the first time that the European Court of Human Rights addressed legislation which purported to regulate foreign surveillance. *See* Weber v. Germany, 2006-XI Eur. Ct. H.R. 309 (June 29, 2006) [hereinafter *Weber*]. Indeed, in the *Weber* case, the legislation in dispute concerned the G 10 Act, which involved strategic monitoring of satellite links, *id.* at 334, which by nature involved the interception of non-German communications. Nonetheless, neither of the parties brought any arguments pertaining to Article 14 of the ECHR, and the Court never picked up the issue.

46 *See* BABYLONIAN TALMUD, *Baba Mezia* 71a (Soncino ed., H. Freedman trans. 1962) ("If thou lend money to any of my people that are poor by thee: this teaches, if the choice lies between a [Jew and a non-Jew], [a Jew] has preference; the poor or the rich—the poor takes precedence; thy poor [your relatives] and the general poor of thy town—thy, poor come first; the poor of thy city and the poor of another town—the poor of thine own town have prior rights.") (internal punctuation and footnotes omitted).

47 For a comprehensive literary review of the literature, see generally Simon Caney, *International Distributive Justice*, 49 POL. STUD. 974 (2001).

48 *See generally, for example*, SEYLA BENHABIB, THE RIGHTS OF OTHERS: ALIEN, RESIDENTS, AND CITIZENS (2000).

49 Caney, *supra* note 47, at 988.

environment, it must recognize that these "operators" are not "outsiders."[50] As Reisman notes:

> But operators are not necessarily outsiders. Phrases such as "you've got to be practical," "take a more realistic view," "in the real world" or "the nitty gritty" are usually signals of operators who identify with the myth but perform group functions according to a discrepant operational code. Obvious domestic examples in official behavior might include the activities of intelligence agencies and certain police functions . . . . To characterize activities by such agencies as "unlawful" would not be illogical yet somehow it would be imprecise and incongruous, for the activities are carried out by the minions of the law and may be routinely supported by judges charged with the supervision of criminal justice processes. They do indeed deviate from the myth system, and those who perform them defer to this fact by performing them in covert or "discreet" fashion. Of significance here is the fact that those who perform them view them as lawful under the operational code.[51]

This Section thus makes the case for a distinct human rights legal regime for foreign surveillance that is separate from the regime that applies to domestic surveillance. Given the controversial nature of my claim, and the potential of it being perceived as anti-liberal or nationalistic, I will begin by rejecting conservative arguments in favor of unfettered mass surveillance. I will then proceed to reject the liberal account against the distinction. Finally, the Section will offer an innovative analysis of the true justifications that are central to the differentiation between domestic and foreign surveillance.

---

50 Reisman, *Myth System*, *supra* note 21, at 239.

51 *Id.* at 239–40 (footnotes omitted).

A. Rejecting the Conservative Account

As a starting point I vehemently oppose the *teatro de la comedia* that engulfs the anarchic arguments still being raised by a number of countries[52] and scholars[53] in support of a territorially constrained conception of human rights. It has been firmly established now that states must respect and ensure human rights to all individuals subject to their jurisdiction, regardless of whether those individuals are situated within that state's territory.[54] As Professor Milanovic has framed it, this is

---

52 *See, for example*, U.N. Hum. Rts. Comm., 53d Sess., 1405th mtg., ¶ 20, U.N. Doc. CCPR/C/SR.1405 (Mar. 31, 1995) (statement of Conrad Harper, Legal Advisor, U.S. Dep't of State) (emphasis added):

> The Covenant was not regarded as having extraterritorial application. In general, where the scope of application of a treaty was not specified, it was *presumed to apply only within a party's territory*. Article 2 of the Covenant expressly stated that each State party undertook to respect and ensure the rights recognized "to all individuals within its territory and subject to its jurisdiction." That dual requirement restricted the scope of the Covenant to persons under United States jurisdiction and within United States territory. During the negotiating history, the words "within its territory" had been debated and were added by vote, with the clear understanding that such wording would limit the obligations to within a Party's territory.

Cf. Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights (Oct. 19, 2010), http://perma.cc/CYD7-CMHE (suggesting that the traditional U.S. position on the territorial scope of the ICCPR is becoming increasingly untenable and proposing his own model for the extraterritorial application of the treaty); Replies of the Government of Israel to the List of Issues to Be Taken up in Connection with the Consideration of the Third Periodic Report of Israel, 3, U.N. Doc. CCPR/C/ISR/Q/3/Add.1 (July 12, 2010) ("[T]he Convention, which is a territorially bound Convention, does not apply, nor was it intended to apply, to areas outside its national territory."); Replies of the Government of the Netherlands to the Concerns Expressed by the Human Rights Committee in Its Concluding Observations, ¶ 7, U.N. Doc. CCPR/CO/72/NET/Add.1 (Apr. 9, 2003) ("Article 2 of the Covenant clearly states that each State party undertakes to respect and to ensure to all individuals 'within its territory and subject to its jurisdiction' the rights recognized in the Covenant . . . . It goes without saying that the citizens of Sebrenica, vis-à-vis the Netherlands do not come within the scope of that provision."); Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Geor. v. Russ.), Verbatim Record, at 40 (Sept. 8, 2008, 3:00 p.m.) ("The general rule continues to be that treaties, including human rights treaties, in line with Article 29 of the Vienna Convention only bind States with regard to their own territory.").

53 *See, for example*, Eric A. Posner, Statement before the Privacy and Civil Liberties Oversight Board 2, 2 n.2 (Mar. 14, 2014), http://perma.cc/7C39-JSHS; Michael J. Dennis, *Non-Application of Civil and Political Rights Treaties Extraterritorially during Times of International Armed Conflict*, 40 ISR. L. REV. 453, 461–81 (2007); Michael J. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflicts and Military Occupation*, 99 AM. J. INT'L L. 119, 122–27 (2005); Dietrich Schindler, *Human Rights and Humanitarian Law: Interrelationship of the Laws*, 31 AM. U. L. REV. 935, 938–39 (1982).

54 *See, for example*, U.N. Hum. Rts. Comm., 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 (May 26, 2004):

> States Parties are required by Article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all

indeed part and parcel of the "moral logic of human rights law,"[55] which prompts states' human rights obligations wherever they purport to exercise a certain degree of control. In this respect it is important to distinguish between mass surveillance and other forms of extraterritorial human rights interferences (such as, for example, extraordinary rendition, military detention, or drone strikes).

Foreign surveillance programs involve a series of actions, which form part of the intelligence cycle, that are being taken by public authorities of the state within its own territory and subject to its effective control.[56] Consider, for

---

> persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party. . . . This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained.

See also, for example, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J Rep. 136, ¶¶ 107–13 (July 9):

> The Court would observe that, while the jurisdiction of States is primarily territorial, it may sometimes be exercised outside the national territory. Considering the object and purpose of the International Covenant on Civil and Political Rights, it would seem natural that, even when such is the case, States parties to the Covenant should be bound to comply with its provisions. . . . The *travaux préparatoires* of the Covenant confirm . . . the drafters of the Covenant did not intend to allow States to escape from their obligations when they exercise jurisdiction outside their national territory.

For further analysis, see generally MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY (2011).

55 Milanovic, *supra* note 32, at 100.

56 Lowenthal defines the intelligence cycle, which he refers to as the "intelligence process," as the "steps or stages in intelligence, from policy makers perceiving a need for information to the community's delivery of an analytical intelligence product to them." MARK M. LOWENTHAL, INTELLIGENCE: FROM SECRETS TO POLICY 70 (6th ed., 2015). Lowenthal maps out seven steps common to these cycles: (1) identification of requirements; (2) interception and collection of intelligence information; (3) initial extraction, processing and exploitation of said information (the process of decoding, decrypting, translating, and reorganizing the information in a way that makes it accessible to the analysts); (4) filtering, storage, collation, analysis and production of intelligence products; (5) dissemination of products; (6) consumption of products by policy makers; and (7) feedback, which leads to identification of new requirements and the wheel goes round. *Id.* Any signal intelligence gathering operation that involves one of the above activities being conducted within the territory of the state, would qualify to meet the "effective control" standard. Moreover, in the information era, controlling one's data, in any of the above capacities, would be akin to controlling one's person, and should be treated the same for triggering the applicability of human rights treaties' jurisdictional clauses. This analysis holds true irrespective of the question of the physical location where the interception took place or the means by which the data was intercepted. *See* Vivian Ng & Daragh Murray, *Extraterritorial Human Rights Obligations in the Context of State Surveillance Activities?*, UNIV. OF ESSEX HUM. RTS. CTR. BLOG (Aug. 2, 2016), http://perma.cc/9PBW-4UWM:

> It has been established that the interception of the content of communications and/or of communications data is an exercise of authority and control over an

example, the PRISM program, which involves the collection of Internet communications from at least nine major U.S. internet companies.[57] The collection, retention, analysis, and, later, the dissemination of information, as part of this program, are all conducted by U.S. governmental officials, in U.S. governmental facilities, subject to the U.S. government's effective control.[58] This is perhaps the reason why.[59] It is noteworthy that despite the general U.S. rejection of the extraterritorial application of human rights treaties, the U.S. has never explicitly argued that its foreign surveillance programs did not trigger its human rights obligations. Quite the opposite, Presidential Policy Directive 28 seems to denote a tacit recognition of some limited privacy obligations associated with NSA's foreign surveillance operations.[60]

The approach that the international human rights treaty corpus may be triggered by extraterritorial foreign surveillance operation has been reaffirmed, albeit not in so many words, by the United Nations General Assembly,[61] the U.N.

> individual's right to privacy, capable of giving rise to extraterritorial jurisdiction. Indeed, if extraterritorial jurisdiction is not established, there is a risk that intelligence agencies may exploit this gap to circumvent Convention protections through the use of intelligence sharing arrangements. Effectively, if extraterritorial jurisdictional obligations do not apply, and as a result international human rights safeguards are not in place, it circumvents existing limits on domestic surveillance and renders affected individuals without an avenue of redress.

57 PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 7 (July 2, 2014), http://perma.cc/AT7T-75UK.

58 *See id.*

59 The Privacy and Civil Liberties Oversight Board, for example, has left the matter unresolved. *See id.* at 98–100.

60 President Barack Obama, *Presidential Policy Directive/PPD-28—Signals Intelligence Activities* (Jan. 17, 2014), http://perma.cc/2SZA-FZAH:

> [O]ur signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information . . . . U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.

61 G.A. Res. 68/167, The Right to Privacy in the Digital Age, at 2 (Dec. 18, 2013) ("Deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights.").

Human Rights Committee,[62] the Venice Commission,[63] and the Court of Justice of the European Union.[64] More interestingly, and perhaps unsurprisingly, in the *10 Human Rights Organizations* case (which directly concerns the legality under international human rights law of global mass surveillance programs, including in the context of Tempora, PRISM, and Upstream), the U.K. Government did not even challenge the extraterritorial applicability of the ECHR.[65] Instead, both the Applicants and the Respondent ignored the issue altogether (tacitly accepting that

---

62 *See, for example*, U.N. Hum. Rts. Comm., Concluding Observations on the Seventh Periodic Report of Poland, ¶ 39, U.N. Doc. CCPR/C/POL/CO/7 (Nov. 23, 2016) ("The Committee is concerned about the surveillance and interception powers of the Polish intelligence and law enforcement authorities . . . The Committee is particularly concerned about: . . . the targeting of foreign nationals and application of different legal criteria to them."); U.N. Hum. Rts. Comm., Concluding Observations on the Sixth Periodic Report of New Zealand, ¶ 16, U.N. Doc. CCPR/C/NZL/CO/6 (Apr. 28, 2016) ("The State Party should take all appropriate measures to ensure that . . . [s]ufficient judicial safeguards are implemented, regardless of the nationality or location of affected persons, in terms of interception of communications and metadata collection, processing and sharing"); U.N. Hum. Rts. Comm., Concluding Observations on the Fifth Periodic Report of France, ¶ 12, U.N. Doc. CCPR/C/FRA/CO/5 (Aug. 17, 2015) ("The State Party should take all necessary steps to guarantee that its surveillance activities within and outside its territory are in conformity with its obligations under the Covenant, in particular, article 17."); Concluding Observations on U.K., *supra* note 37, at ¶ 24; Concluding Observations on U.S., *supra* note 37, at ¶ 22(a) ("[M]easures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality, and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance.").

63 European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, ¶ 6, CDL-AD(2015)006, Study No. 719/2013 (Apr. 7, 2015):

> The collection of signals intelligence may legitimately take place on the territory of another state with its consent, but might still fall under the jurisdiction of the collecting state from the view point of human rights obligations under the ECHR. At any rate, the processing, analysis and communication of this material clearly falls under the jurisdiction of the collecting State and is governed by both national law and the applicable human rights standards. There may be competition or even incompatibility between obligations imposed on telecommunications companies by the collecting state and data protection obligations in the territorial state; minimum international standards on privacy protection appear all the more necessary.

64 Case C-362/14, Schrems v. Data Prot. Comm'r, ECJ Judgment (Grand Chamber), ¶ 94 (Oct. 6, 2015), https://perma.cc/S96P-LRXT [hereinafter *Schrems*] ("[L]egislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter."). The *Schrems* case concerned the transfer of data from European data centers to American data centers, specifically from Facebook Ireland to its facilities in the U.S., in light of the alleged involvement of American companies, such as Facebook, in the PRISM mass surveillance program.

65 *See generally* Applicants' Reply, *supra* note 41.

the obligation to respect and ensure the right to privacy, under ECHR Article 8, was triggered by the nature and scope of the disputed programs).[66]

Similarly, this paper does not take the view, championed more recently by Professor Eric Posner, that the right to privacy has no intrinsic value of its own and that, therefore, espionage alone cannot be said to harm a person's human dignity. He argues:

> Suppose that the NSA collects the emails of foreigners and conducts searches of them for keywords. Occasionally a false positive turns up, and an analyst reads someone's email to his lover, therapist, or doctor, ascertains that the email contains no information that identifies terrorists or other security threats, and deletes it. The writer of the email never finds out, and the analyst of course has no idea who this person is. Has a human right been violated? It is hard to identify an affront to human dignity, or even a harm, any more than if a police officer overhears a snatch of personal conversation on the bus.[67]

Setting aside the empirical question of whether covert mass surveillance breeds fear and self-censorship, corrodes democratic institutions and reverses their basic tenets (such as the presumption of innocence),[68] stifles creativity and dissent, and hampers friendly relations amongst nations (in other words directly inflicting a whole canopy of potential harms),[69] Posner's critique should be dismissed solely

---

66 It could be that the decision to ignore the extraterritoriality question was a strategic move by all parties. For the human rights NGOs, the interest is clear, as ignoring the issue avoids the potential hurdle of preliminary admissibility questions. For the U.K. Government, it could be that the lawyers of the state are so confident at their ability to win following the *Kennedy* decision, which also looked at RIPA, *see* Kennedy v. United Kingdom, App. No. 26839/05, Eur. Ct. H.R., Judgment (May 18, 2010), that they would rather have a victory on the merits than a dismissal of the case on admissibility arguments.

67 *See* Posner, *supra* note 53, at 4–5.

68 *See, for example*, 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. P7_TA(2014)0230, ¶ 12 (Mar. 12, 2014):

> > [The European Parliament] [s]ees the surveillance programmes as yet another step towards the establishment of a fully-fledged preventive state, changing the established paradigm of criminal law in democratic societies whereby any interference with suspects' fundamental rights has to be authorised by a judge or prosecutor on the basis of a reasonable suspicion and must be regulated by law, promoting instead a mix of law enforcement and intelligence activities with blurred and weakened legal safeguards, often not in line with democratic checks and balances and fundamental rights, especially the presumption of innocence.

69 *See generally, for example*, Jonathan W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117 (2016); PEN AM. CENTER, GLOBAL CHILLING: THE IMPACT OF MASS SURVEILLANCE ON INTERNATIONAL WRITERS (2015), http://perma.cc/9M7P-4TC9; HUMAN RIGHTS WATCH, WITH LIBERTY TO MONITOR ALL: HOW LARGE-SCALE US SURVEILLANCE IS HARMING JOURNALISM, LAW AND AMERICAN DEMOCRACY (2014), http://perma.cc/8VAH-XC3H. For analysis of Penney's study, see Tim Cushing, *The Chilling Effect of Mass Surveillance Quantified*, TECHDIRT (May 2, 2016), http://perma.cc/NZM3-XVKA and Glenn Greenwald, *New*

on the grounds of his false analogy. To compare foreign mass surveillance to a police officer overhearing a snippet of a conversation on a bus misses the mark twice. First, the issue is not the anecdotal situation police officers may find themselves in, listening in to a private conversation while incidentally taking the bus. The crux of the concern with mass surveillance is the government's intention to metaphorically place a police officer on every single bus so that they can record every single conversation. Moreover, the concern is exacerbated in the context of foreign mass surveillance, as country A is purporting to place an infinite number of its own metaphorical police officers on the busses of Country B. The real question is, therefore, whether one state can decide clandestinely on a balance between liberty and security, and then impose that balance on the nationals of a foreign sovereign without their knowledge, let alone consent.

Additionally, Posner suggests that if a victim is unaware of the infringement of his privacy, and the particular snooper is unable to explicitly utilize the information against him, then there is no human rights violation. The argument echoes the statement made by former U.S. House Intelligence Committee Chairman Mike Rogers, who had contended, and has since retracted, that "you can't have your right to privacy violated, if you don't know your right to privacy has been violated."[70] This *circulus in probando* just doesn't hold true in reality. If you peek into the windows of the sorority house, and they don't notice you standing there, the police will still arrest you. Or, as Jon Stewart put it more humorously in one segment of the Daily Show, if you don't detect your testicular tumor, it doesn't mean that it can't nevertheless kill you.[71]

Study Shows Mass Surveillance Breeds Meekness, Fear, and Self-Censorship, INTERCEPT (Apr. 28, 2016), http://perma.cc/E4VQ-DDR7. This was further stressed in the Concurrent Opinion of Judge Pettiti in Malone v. United Kingdom, App. No. 8691/79, Eur. Ct. H.R., Judgment, at 41 (Aug. 2, 1984) (noting that the requirements of judicial control over covert surveillance activities is not solely a matter of the "philosophy of power and institutions"; it is about the necessities of democratic functioning and protecting private life); *see also Weber*, *supra* note 45, at 335–36:

> [S]ince the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred to the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

See also Kim Zetter, *Personal Privacy is Only One of the Costs of NSA Surveillance*, WIRED (July 29, 2014), http://perma.cc/776J-E24A.

70 *Mike Rogers' View of Privacy* (C-Span 3 television broadcast Oct. 29, 2013), https://www.c-span.org/video/?c4470916/mike-rogers-view-privacy.

71 Jon Stewart, *A Bugged Life—Plausible Deniability Scramble,* THE DAILY SHOW (Oct. 30, 2013), http://www.cc.com/video-clips/ufe497/the-daily-show-with-jon-stewart-a-bugged-life---plausible-deniability-scramble.

But even were we to accept, and we shouldn't, the notion that privacy has no intrinsic value of its own,[72] then the fact that it serves as a lynchpin to other indispensable individual values (such as, inter alia, personal autonomy, freedom of expression, freedom of association, and freedom of choice), is sufficient for accepting the need to set certain limitations on foreign surveillance. As others have put it, privacy is indeed the "canary in our technological coal mine."[73] With its demise, other fundamental rights and values are sure to be asphyxiated by the invisible toxin of unfettered surveillance.

As John le Carré has taught us, capitulating to Big Brother's omnipresence is practically innate to our very nature as a dormant society, and from there it is but a short path to a "collective submission to wholesale surveillance of dubious legality."[74] This paper thus accepts, as a basic premise, the importance of the right to privacy, its applicability in extraterritorial mass surveillance cases, and the need to protect it from the negative effects of unfettered interception, access, and dissemination. The limited, albeit controversial, goal of this piece is merely to propose a different set of potential privacy protections for foreign surveillance compared to its domestic counterpart.

B. Rejecting the Liberal Account

While Article 26 of the ICCPR generally prohibits any discrimination on grounds such as national or social origin, birth, or other status, the Human Rights Committee has nonetheless recognized in General Comment 18 that "not every differentiation of treatment will constitute discrimination, if the criteria for such differentiation are reasonable and objective and if the aim is to achieve a purpose which is legitimate under the Covenant."[75] The ECtHR case law similarly adopted this position, noting that:

---

72 *Cf.* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 961–78 (1989). Professor Daniel Solove summarizes Post's theory the following way:

> [P]rivacy is not merely a set of restraints on society's rules and norms. Instead, privacy constitutes a society's attempt to promote civility. Society protects privacy as a means of enforcing order in the community. Privacy isn't the trumpeting of the individual against society's interests but the protection of the individual based on society's own norms and values.

DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 50 (2011) (footnote omitted).

73 THERESA M. PAYTON & THEODORE CLAYPOOLE, PRIVACY IN THE AGE OF BIG DATA: RECOGNIZING THREATS, DEFENDING YOUR RIGHTS, AND PROTECTING YOUR FAMILY 1 (2014).

74 JOHN LE CARRÉ, THE PIGEON TUNNEL: STORIES FROM MY LIFE 19 (2016).

75 U.N. Hum. Rts. Comm., Thirty-Seventh Session, General Comment 18: Non-discrimination, Compilation of General Recommendations Adopted by the Human Rights Treaty Bodies, ¶ 13, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (Nov. 10, 1989).

> [A] difference in treatment is discriminatory if it lacks reasonable and objective justification, that is to say it does not pursue a legitimate aim or if there is no reasonable relationship of proportionality between the means employed and the aim pursued. There is a margin of appreciation for States in assessing whether and to what extent differences in otherwise similar situations justify a different treatment.[76]

To identify what might constitute such a "reasonable and objective justification" for statutory differentiation between domestic and foreign surveillance, the literature has so far focused on the wrong arguments. Korff, for example, has tried to identify the roots of the distinction in history, claiming that it is reflective of the origins of the intelligence agencies that were established as "frontline defenders," part of a broader "war effort against external military threats and foreign spies, *saboteurs* and infiltrators." Suspending certain protections afforded to aliens and foreigners therefore made more sense in that historical context, and during that period.[77]

Korff is of course correct; going all the way back to the sixteenth century, to the days of the father of modern intelligence agencies, Sir Francis Walsingham, spy networks were centered around surveilling aliens at home and foreign nationals abroad, who could pose a threat to the crown.[78] Dawson and Head go even further back in time:

> Since ancient times foreigners have been regarded with suspicion, if not fear, either due to their nonconforming religious and social customs, their assumed inferiority, or because they were considered potential spies and agents of

---

76 J.M. v. United Kingdom, App. No. 37060/06, Eur. Ct. H.R., Judgment, ¶ 54 (Sept. 28, 2010). This falls in line with the positions of Professors McDougal, Lasswell, and Chen as early as 1976 where they contended that:

> It must be conceded that the aggregate common interest of territorially organized communities may upon occasion require some limitation of this preferred policy of the utmost individual freedom of choice in state membership and complete equality in the treatment of aliens and nationals. Insofar as the characterizations of "nationality" made by states bear some rational relation to group membership in fact, it may be expedient for states to make appropriate differentiations for the sake of internal and external security and the optimal functioning of all internal value processes.

Myres S. McDougal, Harold D. Lasswell, & Lung-chu Chen, *The Protection of Aliens from Discrimination and World Public Order: Responsibility of States Conjoined with Human Rights*, 70 AM. J. INT'L. L. 432, 438 (1976).

77 Korff, *supra* note 39, at 25–26.

78 As I have written elsewhere: "Walsingham carefully devised and constructed a web of spy networks. He paid off travellers in the ports of Lyon and merchant adventurers in the bazaars of Hamburg. He contracted with Scottish exiles living in Italy and with English soldiers of fortune in the pay of the Dutch. He turned to low-level ships' captains from Prague and expatriate traders from Barbary, but also to Men of Letters, poets, scholars, and scientists right from the heart of London." Asaf Lubin, *Espionage as a Sovereign Right under International Law and its Limits*, 24 ILSA QUARTERLY No. 3 22, 24–25 (2016).

> other nations. Thus, the Romans refused aliens the benefits of the *jus civile*, thirteenth-century England limited their recourse to the ordinary courts of justice, and imperial Spain denied them trading rights in the New World.[79]

Korff is obviously also correct in suggesting that laws which base their distinctions solely on these historical fears, which have no evidential basis in modern political reality, must be "fundamentally rewritten."[80] A second, closely related argument found in the literature is that the justification for the distinction lies with the fact that aliens or foreigners, as a class of people, are "inherently more dangerous to the security of the State" than a state's own citizens. Yet the countless cases of homegrown terrorism suffice to pull the rug right out from under this argument.[81] Second-generation immigrants—Europeans who are often fluent in their home countries' languages—are behind the vast majority of ISIS-inspired terrorist attacks that have occurred on European soil over the course of the past few years.[82] Nationals and non-nationals may pose an equal threat to a state's national security and public order, and making any distinctions between foreign and domestic surveillance solely on the basis of this claim would be unpersuasive.

Kerr on the other hand rests the reasons for the distinction on a contractarian conceptualization of human rights law. Kerr sees "governments as having legitimacy because of the consent of the governed, which triggers rights and obligations to and from its citizens and those in its territorial borders."[83] If the French Government decides to adopt an International Intelligence Act, and surveil foreigners with fewer restrictions, they are absolutely entitled to do so, claims Kerr, because foreigners "don't have any rights vis-à-vis the French government," they can't "give the French authority" to do anything or have any valid claim to satisfy."[84] While Kerr's position might have a stronger basis in constitutional design, as far as international human rights law is concerned it is

---

79 FRANK GRIFFITH DAWSON & IVAN L. HEAD, INTERNATIONAL LAW, NATIONAL TRIBUNALS AND THE RIGHTS OF ALIENS xi (1971).

80 Korff, *supra* note 39, at 26.

81 Milanovic correctly does so. *See Human Rights Treaties*, *supra* note 32, at 99. This type of criticism also echoes recent arguments against President Trump's immigration ban as being based on unfounded fears of foreign terrorist threats. *See generally*, Scott Shane, *Immigration Ban is Unlikely to Reduce Terrorist Threat, Experts Say*, N.Y. TIMES (Jan. 28, 2017), https://www.nytimes.com/2017/01/28/us/politics/a-sweeping-order-unlikely-to-reduce-terrorist-threat.html; Uri Friedman, *Where America's Terrorists Actually Come From*, THE ATLANTIC (Jan. 30, 2017), https://perma.cc/A2K2-7GDH.

82 Olivier Roy, *Who are the New Jihadis?*, THE GUARDIAN (Apr. 13, 2017), https://perma.cc/2E7V-KQGN.

83 Orin Kerr, *A Reply to David Cole on Rights of Foreigners Abroad*, LAWFARE (Nov. 2, 2013), https://perma.cc/EA9A-YFBQ.

84 *Id.*

inconceivable. Accepting Kerr's logic for the distinction would throw the baby out with the bathwater, as it would entail a rejection of extraterritorial application altogether.[85] Given that I have already accepted, as a premise, the extraterritorial applicability of the right to privacy to foreign mass surveillance, I must reject Kerr's reasoning for the distinction as well.[86]

This is where the discussion often ends. Having discredited historical logic, social compact reasoning, and external threat arguments, human rights scholars and liberal thinkers are quick to conclude that there is no "reasonable and objective justification" for the distinction and that it therefore reflects nothing more than the xenophobic fears of constituencies and the political expediency of the legislators. Milanovic summarizes this point best:

> It is a basic feature of human nature that it is easier for us to discount the interests, emotions, and rights of those who are distant, different, and de-personalized. While our squeamishness and moral intuitions will not so easily allow us to disregard the rights of a neighbour with whom we will empathize . . . . Such is also the case with surveillance—we will naturally care more if it happens to us, or to people like us, than if it happens to nameless outsiders.[87]

C. Proposing a New Account for the Distinction

I do not reject the possibility that many who participated in the surveys conducted by Amnesty International and the Pew Research Center, mentioned above, exhibited some form of biased, "Some Other Bugger's Back Yard" (SOBBY) thinking that might have played a role in formulating their responses.

---

85 If we contend that the "consent of the governed" is what triggers international human rights obligations, then it would entail that when Israel occupies Gaza without the consent of those subject to its effective control, it has no human rights obligations and when the U.S. engages in targeted killings in Yemen, without the consent of those impacted by its policies, it has no human rights obligations. It is not surprising that those who reject the extraterritorial application of international human rights treaties cite back to social compact theories to prove that they are territorially bound. But as noted by Professors Shany and Ben-Naftali:

> The broad application of human rights standards is mandated by the principle of universality, a central tenant of modern IHR law. The idea that all individuals are entitled to fundamental human rights protections derives from a belief in the intrinsic worthiness of the human person. This ideology has consciously moved away from the social contract theories advanced by Locke, Rousseau and others.

Orna Ben-Naftali & Yuval Shany, *Living in Denial: The Application of Human Rights Treaties in the Occupied Territories*. 37 ISR. L. REV. 17, 61 (2003).

86 Or as Milanovic eloquently put it: "The citizenship-based distinctions drawn in U.S. law, as well as in the laws of other states engaging in mass surveillance (or possible extraterritorial violations of individual rights more generally), thus cannot be justified merely by crying 'social contract.'" Milanovic, *Human Rights Treaties*, *supra* note 32, at 93.

87 *Id.*

Nonetheless, I argue that there are multiple objective justifications for the distinction, which have not been brought up and discussed in the literature. I will take up each of my three justifications in turn.

1. Political-Juridical Disparity

States have two different toolboxes when conducting investigations domestically and abroad. As the U.K. Government had contended in its submissions in the *10 Human Rights Organizations Case,* "the Government has a panoply of powers to investigate a person in Birmingham, which it does not have to investigate a person in Cairo."[88] For instance, the Security Service can, amongst other things, examine a target's information against internal data sets, conduct certain inquires and issue certain subpoenas with a local police station, compel the disclosure of information from service providers (such as financial and medical institutions, telephone and internet companies, and service providers), interview witnesses and acquaintances, analyze the feeds from closed-circuit television (CCTV) cameras, deploy visual surveillance against the person's address or place of work, and if necessary issue warrants for the seizure of assets and property and the arrest of persons.

Given the myriad options available to a state in conducting domestic investigations, the need to rely on covert communications interception, let alone in bulk form, is innately reduced. There are simply less intrusive means available to the state to achieve the same legitimate aim. This is why turning to such measures domestically should be a rare occurrence, and the law must establish strict limitations on when such interceptions can, if ever, be justified. On the other hand, the abilities of a state abroad are far more restricted, as a country may not extend its police and criminal jurisdiction powers into the territory of a foreign state without the latter's consent.[89] The only tools available to the state are mutual legal assistance schemes[90] and intelligence sharing arrangements (in the often

---

88 10 Human Rights Organizations v. United Kingdom, U.K.'s Observations on the Merits, App. No. 58170/13, Eur. Ct. H.R. at ¶ 8.13 (Apr. 26, 2016), https://perma.cc/E2MR-XBA4 [hereinafter *10 Human Rights Organizations*].

89 *See* S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 9 ("Now the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its powers in any form in the territory of another State."); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW IN THE UNITED STATES § 432(2) (1987) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."); INTERNATIONAL BAR ASSOCIATION, REPORT OF THE TASK FORCE ON EXTRATERRITORIAL JURISDICTION 10 (2009) (noting that a "state cannot investigate a crime, arrest a suspect, or enforce its judgment or judicial process in another state's territory without the latter state's permission").

90 In this context, it might be worth noting the well-recognized need for a significant reform in the MLAT process as it relates to cross-border data transfers of digital evidence. S*ee, for example*, Drew

unlikely scenario where the targeted state is willing and able to assist in the investigation), reliance on certain open source intelligence (OSINT) when available, and the gathering of information in the normal course of diplomatic relations.[91] The U.S. Second Circuit Court of Appeals' ruling in *Microsoft Corp. v. United States*[92] further exemplifies this limitation. In that case, the court found that an American search warrant stops at the border (in other words, the Government cannot turn to the courts to issue and enforce, against U.S.-based service providers, warrants for the seizure of a user's e-mail content that is stored

Mitnick, *The Urgent Need for MLAT Reform*, ACCESS NOW (Sept. 12, 2014), https://perma.cc/Y7WE-7F3Y; Jennifer Daskal & Andrew Keane Woods, *Cross-Border Data Requests: A Proposed Framework*, LAWFARE (Nov. 24, 2015), https://perma.cc/M7YE-PNXN; Albert Gidari, *MLAT Reform and the 80 Percent Solution*, JUST SECURITY (February 11, 2016) https://perma.cc/82U7-CF93.

91 As noted by Professor Chesterman:

> Diplomacy and intelligence gathering have always gone hand in hand. The emergence of modern diplomacy in Renaissance Italy underscored the importance of having agents to serve as negotiators with foreign powers, and a chief function of the resident ambassador soon became to ensure that "a continuous stream of foreign political news flow[ed] to his home government."

Simon Chesterman, *The Spy Who Came in From the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L. L. 1071, 1087 (2006) (citing GARRET MATTINGLY, RENAISSANCE DIPLOMACY 67 (1955)). Today the Vienna Convention on Diplomatic Relations, 23 U.S.T. 3227, 500 U.N.T.S. 95 (1961), establishes in Article 3 that one of "the functions of a diplomatic mission" consists of "ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State . . . ." Chesterman, *supra*, at 1087 (quoting Vienna Convention on Diplomatic Relations, *supra*, at art. 3(d)).

92 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 2017 WL 2869958 (Oct. 16, 2017).

exclusively on foreign servers).[93] The case is now pending before the U.S. Supreme Court.[94]

Espionage in its broadest sense, and electronic communications interception more specifically, therefore become an important additional element available to the state in protecting its national security and public order, and in achieving foreign policy interests.[95] Surely, these tools pose significant risks and must be used in moderation, but greater leniency should also be provided given the limited investigative resources at the states' disposal. To this, we might add that adversaries are continuously at work trying to circumvent foreign governments' surveillance activities. Counter-intelligence operations thus further complicate the ability of states to engage in these sorts of investigations abroad.

2. Technological Disparity

Directly linked to the first justification, states' technological capacities to engage in electronic communications surveillance domestically are far greater than they are abroad. This is owed in part to the sheer volume of communications and

---

93 *See Microsoft Corp.*, *supra* note 92. As explained by Microsoft's Chief Legal Officer, Brad Smith, Microsoft directly challenged the ability of the Government to "go around the world and hoover up emails pursuant to a search warrant. . . . It's in effect saying to the people of Ireland, their law doesn't matter." Andrew Orlowski, *Microsoft Wins Landmark Irish Data Slurp Warrant Case Against the US*, REG. (July 14, 2016), https://perma.cc/L8HV-35PS. *Cf.* Jennifer Daskal, *A Microsoft Ireland Fix: Time to Act is Now!*, JUST SECURITY (Apr. 14, 2017), https://perma.cc/M7YE-PNXN (referencing three magistrate cases—from the Eastern District of Pennsylvania, Eastern District of Wisconsin, and Middle District of Florida—where the Second Circuit's approach was rejected; further noting that "an eventual Circuit split seems like, [sic] leading to possible Supreme Court review"; and suggesting a legislative alternative by Congress).

More important is an August 2017 decision from the Northern District of California, also rejecting the Second Circuit's analysis, concerning a similar application from Google. *See* In the Matter of the Search of Content Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A, No. 16-mc-80263-RS, 2017 WL 347889 (N.D. Cal. Aug. 14, 2017) (order denying Google's motion for de novo determination of dispositive matter referred to magistrate judge). This decision is noteworthy given the fact that most tech companies are located within the jurisdiction of the Northern District of California. On June 23, 2017, the U.S. Government filed a petition for a writ of certiorari with the Supreme Court. On August 2, 2017 the Attorney Generals of 33 States plus Puerto Rico filed a bipartisan amicus brief urging the Court to grant cert. The Supreme Court has granted the DOJ's petition on October 16, 2017. For further reading see Andrew Keane Woods, *A Primer on Microsoft Ireland, the Supreme Court's Extraterritorial Warrant Case*, LAWFARE (Oct. 16, 2017), https://perma.cc/CU98-VGDE.

94 *See* Amy Howe, *Court Adds Four New Cases to Merits Docket*, SCOTUS BLOG (Oct. 16, 2017), https://perma.cc/4W4E-TND5 (noting the Supreme Court's grant of certiori for *United States v. Microsoft Corp.*).

95 In fact, as I have written elsewhere, it is the sovereign right of a nation, recognized under international law, to engage in interstate espionage in order to protect its national security, defend against any potential threats of uses of force against the state, and indeed ensure its very survival. *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, no. 2, 2017, https://perma.cc/9L6B-YJAP.

potential targets,[96] but also to the available means for interception.[97] In other words, whereas a country has full understanding, and oftentimes statutory access to, its internal communications grid for conducting warranted interceptions, and where it is capable of compelling telecommunication companies at home to provide it with additional access to their networks or to disclose certain user information from their databases,[98] these abilities simply do not transfer to the foreign surveillance plane. To develop an adequate signal intelligence surveillance program, and to ensure its continued effectiveness, from a technical perspective, requires years of planning and work, mapping out networks and systems, and formulating interception and extraction techniques. It involves significant

---

96 *See generally* Bhaskar Chakravorti, *More Data, More Problems: Surveillance and the Information Economy*, FOREIGN AFF. (July 7, 2015), https://perma.cc/4X2Z-VCV5.

97 In referencing interception, extraction, filtering, storage, analysis, and dissemination, I refer to the terminology as defined by Privacy International in preparation for the *10 Human Rights Organizations Case*. Interception involves the capturing of a signal, a stream of communications from the cable; extraction involves the copying of the stream, directing it into a storage space and reassembling the packets; filtering involves separating out information using algorithms which comb the data based on specific "selectors," for example an IP address or logging into a particular website; storage involves retaining information in databases for analysis; analysis involves querying, reading, examining, collating and data-mining information stored in the databases; finally, dissemination involves the distribution of the results of the analysis to other organizations, agencies, or policy makers. Chakravorti, *supra* note 96. For further reading see Scarlet Kim, *How Bulk Interception Works*, MEDIUM (Sept. 30, 2016), https://perma.cc/3YFU-HEEM.

98 *Cf.* Joined Cases C-293/12 & C-594/12, Digital Rts. Ireland Ltd. v. Minister for Commc'ns, 2014 E.C.R. I-238 (Apr. 8, 2014) (concluding that EU regulators had exceeded the limits of the principles of necessity and proportionality by demanding, through the EU Data Retention Directive, the retention of all traffic data of all users of all means of electronic communications). *See also*, Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v. Post-Och Telestyrelsen, and Sec'y of State for the Home Dep't v. Tom Watson, Judgment, 2016 E.C.R. 970, ¶¶ 110–11:

> [A]s regards the substantive conditions which must be satisfied by national legislation that authorises, in the context of fighting crime, the retention, as a preventive measure, of traffic and location data, if it is to be ensured that data retention is limited to what is strictly necessary, it must be observed that, while those conditions may vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime, the retention of data must continue nonetheless to meet objective criteria, that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected.
>
> As regards the setting of limits on such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences.

investments in money and human hours, and routine maintenance and monitoring.

Certain countries because of their unique geographical location (like Germany) or their competitive advantage in the internet service market (like the U.S.) might benefit from significant portions of the world's online communications naturally passing through their territory, thus making it technologically easier to engage in bulk foreign surveillance. Nonetheless, as a general rule, and certainly in the context of the most effective foreign surveillance programs, there involves significant planning and complex execution. These programs simply cannot be turned on and off on an *ad hoc* basis, as would be expected in a traditional warrant-like setting. Given that the means of interception, extraction, and filtering are different and far more complex, there is, once more, a need for greater leniency in statutory authorization.[99]

3. Disparity in Harms from Potential Abuse

While I have already contested some of Posner's claims above, let me nonetheless recognize one important aspect of his argument. In case a potential abuse of surveillance powers occurs, the victim is indeed likely to endure greater immediate harm at home than he is abroad. It is correct to suggest that foreigners are provided some form of (very) minimal protection "by national boundaries." That is because domestically gathered information against someone within the territory can quickly turn into uses of legal and physical force, from harassment to detention to deportation, whereas in the foreign context, "Chinese, French, and Russian intelligence agents do not have the time or inclination to harass random

---

[99] The technological limitations are further explained in the U.K. Government's observations to the *10 Human Rights Organizations* case, though they are used as a rationale for the utility of mass surveillance more broadly:

> [The intelligence service's] ability to understand what communications bearers those targets will use is limited, and their ability to access those bearers is not guaranteed . . . electronic communications do not traverse the internet by routes that can necessarily be predicted. Communications will not take the geographically shortest route between sender and recipient, but the route that is most efficient, as determined by factors such as the cost of transmission, and the volume of traffic passing over particular parts of the internet at particular times of day. So in order to obtain even a small proportion of the communications of known targets overseas, it is necessary for the Services to intercept a selection of bearers, and to scan the contents of all those bearers for the wanted communications . . . .
>
> [C]ommunications sent over the internet are broken down into small pieces, known as "packets," which are then transmitted separately, often through different routes, to the recipient, where the message is reassembled. It follows that in order to intercept a given communication that is travelling over the internet (say, an email), any intercepting agency will need to obtain all the packets associated with that communication, and reassemble them.

10 Human Rights Organizations, *supra* note 88, at ¶¶ 1.29–1.30.

Americans, nor the capability as long as Americans remain in the United States." Unchecked domestic surveillance, in this regard, poses a more urgent danger to fundamental civil liberties. [100]

One needs to be careful with this line of argument, though. In a globalized world, individuals do step outside the bounds of their state, thus willingly entering themselves into the spheres of control and influence of foreign countries. This does not have to be done only by means of travel. Having economic interests or romantic entanglements overseas could easily expose an individual to the potential powers of those foreign governments in question. Moreover, in an age of intelligence sharing, the information collected by one agency can easily find its way in the hands of another, thus furthering the level of exposure. In addition, it is crucial to note that different countries' "national boundaries" offer different levels of protection, depending on the country's international gravitas and political, economic, and military power. Finally, as I have already alluded to, mass foreign surveillance and privacy infringements do in fact inflict direct harms in their own right.[101] This is why this reason for the distinction between domestic and foreign surveillance cannot simply justify unfettered spying on foreigners, as Posner has argued. Nonetheless, it can form a further justification for a *degree* of differentiation in legal treatment between the two regimes.

***

In conclusion, the combination of political and jurisdictional limitations, technological disparities, and a divergence in potential risk and harm, all seem to denote a "reasonable and objective justification" for differentiation. This is why the ECtHR should reject the ten human rights NGOs' claim of a violation of Article 14 and recognize the logic behind the legal differentiation in treatment that formed part of RIPA (and indeed of most, if not all, foreign surveillance laws). It might be the inclination of the ECtHR to follow a universalist model, and simply

---

100 *See generally* Eric Posner, *Keep Spying on Foreigners*, *NSA*, SLATE (Nov. 14, 2013), https://perma.cc/8JS7-DAJH; *see also*, Charles C. W. Cooke, *An Overreach for the NSA's Critics*, NAT'L REV. (Jan. 13, 2014), https://perma.cc/SDG8-WP5E ("It should be self-evident that a foreign power's violating your privacy and your own government's doing so are by no means the same thing. For the vast majority of people, the practical importance of one's secrets being obtained by one's own government considerably outweigh the importance of their being obtained by a foreign power. The American federal government can and might do all sorts of immediate harm to me; the government of China, on the other hand, cannot. If a rogue official in the United States take exception to my politics, he can make my life hell: inviting the government to track my whereabouts, ordering frivolous arrests, tying me up in endless audits and frivolous bureaucracy, and even sending a SWAT team to my house. If the Chinese politburo finds me objectionable (and I certainly hope it does), it can do very little of practical importance. Moreover, and this I think is the key point, if China tries to actually hurt me, I have distance, borders, and the American government's considerable arsenal standing in the way. If someone at home tries to hurt me, I have little individual recourse.").

101 *See supra* note 69.

equate the standards of domestic and foreign surveillance, as it alluded to in obiter dictum in the *Liberty* judgment.[102] Nonetheless, it would be far more in line with the practicalities of the topic at hand for the court to follow its precedent in the *Uzun v. Germany* case, where in the context of GPS monitoring, the court was willing to step away from its "rather strict standards" on domestic surveillance and apply "more general principles on adequate protection against arbitrary interference with Article 8 rights."[103] This suggests that the court is tolerant of an argument that different forms of surveillance activities might justify different frameworks of privacy regulations. This is precisely what the above account attempts to suggest in the context of domestic versus foreign surveillance.

The court should further use this opportunity to discuss how a foreign surveillance regime might meet the standards of necessity and proportionality in line with both Articles 8 (Right to Privacy) and 14 (Non-Discrimination) of the ECHR. In this regard, the court is well positioned to introduce a more tailored human rights framework for foreign bulk surveillance, distinct from its previous surveillance jurisprudence. The next section will attempt to begin a preliminary conversation about what such a framework might look like.

IV. A TAILORED HUMAN RIGHTS FRAMEWORK FOR GLOBAL SURVEILLANCE

Three primary considerations should guide us in devising any human rights driven framework for foreign surveillance. First, we should always bear in mind the above justifications for the differentiation in legal treatment (political-jurisprudential limitations, technological disparities, and divergence in potential

---

102 *See* Liberty and Others v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. at ¶ 63 (2008). Citing to the *Weber* decision, its first ever foreign surveillance case, the Court noted:

> It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses . . . . However, the *Weber and Saravia* case was itself concerned with generalised "strategic monitoring," rather than the monitoring of individuals . . . . The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of communications, on the one hand, and more general programmes of surveillance, on the other.

Id.

103 Uzun v. Germany, App. No. 35623/05, Eur. Ct. H.R. at ¶ 66 (2010):

> While the Court is not barred from gaining inspiration from these principles, it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications . . . are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations . . . It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 rights.

harm). Second, we must recall the thinking of Hugo Grotius who had considered it "essential to make the status of the foreigner coincide as far as possible with that of the subject of the particular State."[104] Protecting, to the extent we can, the sanctity of the universal nature of human rights, we should aspire, to the best of our abilities, to ensure as few discrepancies between domestic and foreign surveillance legislation as is prudent and necessary in light of the above justifications. We have to avoid a scenario where we allow for rights to be "violated abroad in the name of preserving them at home,"[105] and so must scrutinize every decision to step away from the general jurisprudence on surveillance. I note in this regard, that while most concerning would be scenarios where we might ask to lower the level of protection or the degree of restriction for foreign surveillance purposes, we should also be mindful of cases where we might wish to increase the level of control beyond what is required in the domestic surveillance context. Either an increase or decrease in protection, indeed any move from the baseline, should be individually justified.

Finally, we should take into account the fact that any easing of control over foreign surveillance might incentivize states to engage in practices to circumvent the greater restrictions imposed on them in the context of domestic surveillance. For example, spying abroad in the hopes of sweeping in the communications of one's nationals, or allowing a foreign agency to spy on one's nationals (with lesser restrictions), and then sharing the information through an intelligence sharing arrangement.[106] This is the "revolving door" or "circular exchange" risk caused by

---

104 *Reprinted in* McDougal, Lasswell & Chen, *supra* note 76, at 440 (citing A. ROTH, THE MINIMUM STANDARD OF INTERNATIONAL LAW APPLIED TO ALIENS 28 (1949)).

105 Craig Forcese, *A Distinction with a Legal Difference: The Consequences of Non-Citizenship in the 'War on Terror'*, *in* HUMAN SECURITY AND NON-CITIZENS: LAW, POLICY, AND INTERNATIONAL AFFAIRS 421 (Alice Edwards & Carla Ferstman eds., 2010).

106 *See* HANS BORN ET AL., MAKING INTERNATIONAL INTELLIGENCE COOPERATION ACCOUNTABLE 48 (2015):

> Information sharing is the main area of international intelligence cooperation that risks bypassing national laws and safeguards on the collection of information—some intelligence services may engage in what has been labelled "collusion for circumvention." Consequently, there have long been suggestions that some services have used their relationships with foreign partners to access information that they either could not lawfully obtain themselves or would be difficult from [sic] them to obtain lawfully. This may be the case for a variety of reasons, including a would-be target's status as a citizen of the state concerned (in circumstances where a service is not permitted to gather information on its state's own citizens); the fact that the actions of a person of interest have not met a requisite threshold of suspicion; the activities in which a would-be target is involved cannot be investigated by the service under the relevant legislation governing the service; a would-be target's membership of a profession that is protected (e.g. a member of parliament); or legal restrictions on using particular methods to collect information. Faced with these difficulties, some intelligence services may turn to foreign partners to acquire the information sought.

See also OHCHR Report, *supra* note 32, at ¶ 30 (noting that there is "credible information to suggest

the introduction of greater allowances in the foreign surveillance context. Any development of rules for foreign surveillance under human rights law must address the revolving door problem head on.

Below, I propose eight suggestions for an initial mapping of a potential new human rights framework, which follows the three considerations above. This is by no means an exhaustive list, and indeed is merely an opening for a broader conversation aiming at more tailored human rights standards for foreign surveillance operations.

A. Legitimate Grounds for the Distinction

As noted above, the only basis for distinction is that surveillance legislation must be rooted in political-jurisprudential and technological limitations on the power of intelligence agencies. A number of countries, however, have based their standard for distinction on the nationality of the targeted individual, not his or her physical location. Such citizenship-based differentiation criteria cannot be rationalized. Aliens situated in the territory of a country, regardless of their legal status, should be provided exactly the same privacy protections as the nationals of that country. Otherwise, we are likely to revert back to the kind historical fears Korff warned us of.[107] Therefore, any foreign surveillance regulation that is based on the nationality of the target, as opposed to his or her location should, to use Korff's words, be fundamentally rewritten.

B. The Territoriality Presumption

A significant hurdle in establishing territorial bounds as the basis for any distinction criteria is the non-territoriality of data. As noted by the U.S. President's Review Group on Intelligence and Communications Technologies: "traditional distinctions between 'foreign' and 'domestic' are far less clear today than in the past, now that the same communications devices, software, and networks are used globally by friends and foes alike."[108] In other words, we are all foreigners in

---

that some Governments systematically have routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy. Reportedly, some Governments have operated a transnational network of intelligence agencies through interlocking legal loopholes, involving the coordination of surveillance practice to outflank the protections provided by domestic legal regimes.").

107 Korff, *supra* note 39.

108 Richard A. Clarke et. al, *Preface to* THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD (2014). This conceptual understanding of data was best described by Professor Jennifer Daskal:

> After all, territorial-based dividing lines are premised on two key assumptions: that objects have an identifiable and stable location, either within the territory or without; and that location matters—that it is, and should be, determinative

cyberspace, not only in the limited sense that we are all foreigners to another nation,[109] but in the broader sense that technology is incapable of distinguishing us. A random email address or IP address is insufficient in determining the exact location of a particular target, whether it is within or outside of the territory and jurisdictional reach of a state.

The only way to address this problem is to place the burden of proof on the intelligence agencies and revert their existing hypothesis from an assumption of foreignness to a presumption of territoriality. As was noted above, the U.N. Office of the High Commissioner for Human Rights criticized the practice whereby "intelligence agencies will often treat the data as foreign" whenever there is uncertainty as to whether data are foreign or domestic.[110]

> of the statutory and constitutional rules that apply. Data challenges both of these premises. First, the ease, speed, and unpredictability with which data flows across borders make its location an unstable and often arbitrary determinant of the rules that apply. Second, the physical disconnect between the location of data and the location of its user—with the user often having no idea where his or her data is stored at any given moment—undercuts the normative significance of data's location . . . . [T]he movement of data from place to place often happens in a seemingly arbitrary way, generally without the conscious choice—or even knowledge—of the data "user" (by which I mean the person with a reasonable expectation of privacy in the data, such as the user associated with a particular e-mail account). An e-mail sent from Germany, for example, may transit multiple nations, including the United States, before appearing on the recipient's device in neighbouring France. Contact books created and managed in New York may be stored in data centers in the Netherlands. A document saved to the cloud and accessed from Washington, D.C., may be temporarily stored in a data storage center in Ireland, and possibly even copied and held in multiple places at once. These unique features of data raise important questions about which "here" and "there" matter; they call into question the normative significance of longstanding distinctions between what is territorial and what is extraterritorial. Put bluntly, data is destabilizing territoriality doctrine.
>
> Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326, 329–30 (2015).

109 *See* ELLIOT D. COHEN, TECHNOLOGY OF OPPRESSION: PRESERVING FREEDOM AND DIGNITY IN AN AGE OF MASS WARRANTLESS SURVEILLANCE 78 (2014) ("This is why the world community needs to supplement the laws of their nations with other international constraints on surveillance in cyberspace that protect 'foreigners'—realizing that we are all foreigners to another nation."); Cole, *supra* note 40:

> It is understandable that Americans care more about their own rights than those of others. But we should not be so quick to dismiss the rights of the foreigner. First, the reality is that we are all foreigners from the standpoint of every other nation. And while at the moment the NSA may be at the forefront of technological surveillance capacity, other nations are not likely to be far behind. How would we feel if we had recently learned that France—or China—was collecting data on millions of Americans' communications, or directly monitoring President Obama's cell phone? If we extend no protection to other countries' nationals, why should we expect them to respect our privacy rights? Thus, it's in our own interest to identify some reciprocal principles to preserve privacy in the digital age.

110 OHCHR Report, *supra* note 32, at ¶ 23.

Instead we should adopt a presumption of territoriality standard, whereby the agency should treat all communications as domestic communications, unless proven otherwise. This approach mimics Daskal's *Presumptive Fourth Amendment*, and applies it more broadly.[111] It entails that agencies will have to show, prior to launching a particular program of intelligence interception and collection, and even more rigorously prior to accessing and reviewing communications intercepted by that program, that such intelligence gathering does not and will not involve "wholly domestic" communications. In other words, every foreign surveillance operation by the state must be necessary considering the three justifications above. In any case of doubt, the government must apply the higher standards of protection.

In the *10 Human Rights Organizations Case*, the Applicants raised a critique surrounding this very issue. The Applicants had suggested that it would be arbitrary for the government to "require a certificate whilst someone is in Britain" but not require it "once they are on holiday abroad."[112] I disagree. This approach clearly adopts a territoriality-based criterion and is in line with the above premises. On the other hand, I agree that the government should not be allowed to circumvent its statutory requirements for domestic surveillance, just because, for example, a citizen had travelled abroad, or because a lawful alien emailed her

---

111 *See* Daskal, *supra* note 108, at 383:

> A much more robust response—and the one I prefer—*presumes* that the Fourth Amendment applies regardless of whether the collection takes place inside or outside the United States, and regardless of whether the target is a U.S. person or not. The presumption can be rebutted if, and only if, the government establishes that *none* of the parties to the communication is a U.S. person. The presumption also applies regardless of whether the communication is in transit or not. In practice, this means that bulk collection, wherever it takes place, will fall within the Fourth Amendment's ambit; cross-border communications will be covered by the Fourth Amendment, irrespective of the identity of the particular target; and most foreign intelligence surveillance will also trigger a Fourth Amendment inquiry, as it will not be feasible in most cases to show that none of the parties to communication is a U.S. person. By contrast, the surveillance of North Korean diplomats in North Korea or the targeted collection on Al-Nusra Front leaders in Syria is unlikely to trigger the Fourth Amendment—although there may be policy reasons to expand protection to these circumstances.
>
> To be clear, this is not the same as saying that a warrant is required every time the government searches or seizes electronic communications for foreign intelligence purposes, or that all surveillance necessarily implicates the Fourth Amendment. There is, I believe, a legitimate foreign intelligence exception to the warrant requirement in some circumstances. Rather, my argument is that Fourth Amendment protections, however defined, ought to apply to U.S. person targets and non-U.S. person targets alike, absent clear and convincing evidence that collection does not encompass communications to or from a U.S. person or include other data (such as stored documents) that have been generated in whole or in part by a U.S. person.

112 *See* Applicants' Reply, *supra* note 41, at ¶ 271(7).

mother who is abroad, or because an unlawful immigrant phoned her husband who is abroad.[113] Under a presumption of territoriality, each of these half-domestic, half-foreign communications would be treated as wholly domestic, for the purposes of our international human rights law analysis. This would entail, however, that certain operations, when sufficient evidence is provided, will be treated as wholly foreign and thus subject to more relaxed restrictions. This will help bridge the existing gap between the myth of universality under international human rights law and the practice of foreign surveillance under domestic authorizations and will help further harmonize privacy regulations and protections.[114]

C. Locations with "Quasi Territorial Qualities"

Given that the basis for the differentiation is one directly linked to *ratione loci* jurisdiction, it should be evident that countries cannot treat the surveillance of individuals situated in "quasi-territorial" locations[115] as subject to foreign surveillance laws. In this regard, individuals who are located within a country's embassies abroad, who are on board a country's registered vessels or aircrafts abroad, who are detained in a country's detention facilities abroad, who are tried by military courts abroad, or who are living within territories occupied by a country abroad, should all be treated as being within the state's territory for the purposes of protections and safeguards in the case of surveillance. If the country can exercise jurisdiction politically, and has the means to engage in the surveillance technologically, there is no justification for the distinction. In other words, under

---

113 I stress once more that the issue is not the nationality of the target, but the target's location. The citizen, the lawful alien, and the unlawful immigrant are all located within the country, and therefore should be covered under domestic surveillance regulations.

114 In this regard, I believe I diverge from the position of David Cole, in the sense that I do not encourage a reform of American "domestic laws and transnational agreements." I only limit my analysis to the interpretation of the specific international human rights law treaty provisions so far discussed and ask that certain aspects of their interpretation be brought closer to the best practices of intelligence agencies engaged in foreign surveillance. *Cf.* Cole, *supra* note 40.

115 The phrase "a location with a 'quasi-territorial quality'" is taken from the judgment of the U.K. Divisional Court in Al-Skeini v. Sec'y of State for Def., [2004] EWHC (Admin) 2911 ¶ 270, [2004] WLR 1401 [270] (Eng.), which was brought up in the context of the extraterritorial application of international human rights law:

> Such instances [of extraterritorial human rights applicability] are ones where, albeit the alleged violation of Convention standards takes place outside the home territory of the respondent state, it occurs by reason of the exercise of state authority in or from a location which has a form of discrete quasi-territorial quality, or where the state agent's presence in a foreign state is consented to by that state and protected by international law: such as diplomatic and consular premises, or vessels or aircraft registered in the respondent state. Such a rationalisation could also encompass courts located in a foreign state but, by international treaty, manned by the respondent state's judges acting as such.

my analysis, there is no reason not to apply the same domestic surveillance standards in each of the above-listed scenarios.

D. The Principle of Legality

Any limitations to the right to privacy "must be provided for by law, and the law must be sufficiently accessible, clear, and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances."[116] There is no question that there are far fewer countries that have actually regulated their foreign surveillance activities through primary legislation, as opposed to regulation by means of secret executive orders. This ought to be altered.[117] It should be part and parcel of any human rights framework for foreign surveillance to insist on primary regulation, which is subjected to the scrutiny of political debate in parliament.

While the basic principle of legality must apply to all surveillance legislation, it might produce different effects in the context of a foreign surveillance framework. For example, "accessibility" might mean something entirely different when spying on foreigners. This is because the targets are not to be expected to know where to find the surveillance legislation of a foreign country purporting to spy on them, nor should they be assumed to be able to read the language in which that legislation is likely to have been written. If the usual standard for "accessibility" in the domestic surveillance context is merely the dissemination of the law "in a generally accessibly official publication" of the state,[118] that might

---

116 *See* OHCHR Report, *supra* note 32, at ¶ 23.

117 *Id.* at ¶ 29:

> [S]ecret rules and secret interpretations—even secret judicial interpretations—of law do not have the necessary qualities of "law." Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion . . . The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive—a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights.

118 *See* Rotaru v. Romania, App. No. 28341/95, Eur. Ct. H.R., Judgment, ¶ 54 (2000) ("As to the accessibility of the law, the Court regards that requirement as having been satisfied, seeing that Law no. 14/1992 was published in Romania's Official Gazette on March 3, 1992."); Roman Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H.R., Judgment, ¶ 239–42 (2015):

> The publication of the Order in the Ministry of Communications' official magazine SvyazInform, distributed through subscription, made it available only to communications specialists rather than to the public at large. At the same time, the Court notes that the text of the Order, with the addendums, can be accessed through a privately-maintained internet legal database, which

prove insufficient in the context of foreign surveillance. We might require states to translate their laws to multiple languages, advertise their legislation in particularly vulnerable countries and to particularly vulnerable groups, and make it accessible to specialized advocacy groups (such as digital rights NGOs who can further scrutinize and challenge the country's foreign surveillance practices). In this regard a human rights tailored framework for foreign surveillance might set a higher, not a lower, standard for "accessibility" than its domestic counterpart.

E. The *Weber* Six

In its case law on surveillance measures, most notably in *Weber and Saravia v. Germany*,[119] the ECtHR had developed six minimum safeguards that should be introduced into statutory legislation in order to avoid abuses of power. Each piece of surveillance legislation must thus enumerate the following:

> [1] the nature of the offences which may give rise to an interception order; [2] a definition of the categories of people liable to have their telephones tapped; [3] a limit on the duration of telephone tapping; [4] the procedure to be followed for examining, using and storing the data obtained; [5] the precautions to be taken when communicating the data to other parties; [6] and the circumstances in which recordings may or must be erased or the tapes destroyed.[120]

The *Weber* Six should certainly be part of any foreign surveillance framework. Nonetheless, one can easily imagine a number of different ways by which domestic and foreign surveillance legislation might diverge on the particularities of any of these general principles. In the context of the French International Intelligence Act, we in fact already witnessed how differentiation in storing requirements and other safeguards might be introduced by parliament.[121] Similarly, differentiations between lists of purposes, which may give rise to an interception order in the domestic and the foreign surveillance context, could be potentially envisioned.[122]

> reproduced it from the publication in SvyazInform . . . . The Court finds the lack of a generally accessible official publication of Order no. 70 regrettable. However, taking into account the fact that it has been published in an official ministerial magazine, combined with the fact that it can be accessed by the general public through an internet legal database, the Court does not find it necessary to pursue further the issue of the accessibility of domestic law.

119 *Weber*, *supra* note 45.

120 *Id.* at ¶ 95.

121 *See*, *supra* notes 23–30.

122 Currently the tendency of most States is to establish one all-encompassing list of categories that could potentially justify interception, and then apply it equally in both the domestic and the foreign surveillance context. The U.K.'s hotly debated Investigatory Powers Act contains the following list of "purposes" for which communications data might be obtained:

> (a) in the interest of national security, (b) for the purpose of preventing or

One particular issue I wish to tackle at greater length pertains to the need for specific warrants for foreign surveillance. In their submissions in the *10 Human Rights Organizations* case, the Applicants contended that there was no rational basis in suggesting that GCHQ would need a warrant or certificate to target "an NGO's London office" but they would not need it to target "the same NGO's German office."[123] Once again let me begin by stressing that the objective reason for the differentiation in treatment should be the location of the target and not its nature, and that subject to the territoriality presumption, the scenario described does not seem irrational or unreasonable.[124] More importantly, however, there is room to discuss what kind of prior authorizations might be required for launching foreign surveillance operations.

As was explained by Commissioner Pillay, an interference with the right to privacy already occurs at the point of interception.[125] The general standard is therefore that a judicial warrant must be obtained before interception occurs and that such a warrant should include an explanation of why the specific method of

> detecting crime or of preventing disorder, (c) in the interest of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security, (d) in the interests of public safety, (e) for the purposes of protecting public health, (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, (g) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health, (h) to assist investigations into alleged miscarriages of justice.

Investigatory Powers Bill, as Amended in Committee, HL Bill [62], cl. 53(7) (Eng). Similarly, the French legislation allows for interception for the purposes of "national security, safeguarding the essential elements [of] scientific and economic potential of France, or the prevention of terrorism, crime and organized crime." *Supra* note 23, at Art. L241-2. Both countries respectively apply their broad lists of purposes equally to their domestic and foreign surveillance operations. Questions relating to foreign espionage for the purposes of economic advancements or the promotion of foreign affairs, which is common to certain countries, could now be scrutinized further by the ECtHR, to determine their unique compatibility with ECHR as a category justifying interception. For further reading, see Lubin, *A New Era of Mass Surveillance*, *supra* note 30.

123 *See* Applicants' Reply, *supra* note 41, at ¶ 271(6).

124 Insofar as the NGO is registered in the U.K., and conducts most of its operations in the U.K., then it takes away many of the political and technical limitations that stood at the heart of the original differentiation in treatment. In such a case, under the presumption of territoriality, the German branch of the NGO should be treated in the same manner that we treat the London branch, unless the Government is able to furnish evidence to suggest that the differentiation in treatment is called for.

125 *See*, OHCHR Report, *supra* note 32, at ¶ 20:

> [A]ny capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.

interception is necessary, proportionate and the least intrusive means to identify the target's likely communication lines. In particular, the warrant should provide an assessment of all collateral intrusion that may occur as a result of the interception, and how such intrusions will be minimized.

However, we must recognize the unique technical limitations, above discussed, pertaining to the evolution of an effective foreign SIGINT collection apparatus. We should therefore be willing to accept, solely for the purposes of testing towards eventual collection (but never for access), certain forms of "bulk warrants" as opposed to specific warrants.[126] For example, we might allow for the temporary interception of and extraction from a limitedly broader scope of bearers (communication trunks) and against a limitedly broader category of targets, than we would usually require in a domestic context.[127]

Of course, once the route by which communications are sent and received from the target is identified, all other extractions under the warrant should immediately cease and any information gathered on the basis of such warrant that is not necessary for the particular investigation for which it was authorized should be discarded. Similarly, other obligations, for example a requirement for an individualized showing of a prior reasonable suspicion prior to accessing the information, or the minimization of the extraction and storing of collateral information, would have to be adapted accordingly.

These points must be stressed, as the formulation of a tailored human rights framework for foreign surveillance should not be seen as a façade for legalizing mass surveillance. Indeed mass surveillance, in the sense of unwarranted and indiscriminate collection and/or access to unnecessary and disproportionate volumes of personal communications and metadata is, and should continue to be,

---

126 In *Zakharov v. Russia*, *supra* note 118, the ECtHR was specifically critical of Russian courts which "sometimes grant interception authorizations which do not mention a specific person or telephone number to be tapped, but authorize interception of all telephone communications in the area where a criminal offence has been committed . . . The Court considers that such authorizations . . . grant a very wide discretion to the law-enforcement authorities as to which communications to intercept, and for how long." *Id.* at ¶ 265. This is precisely the kind of area where I contend that we should be stricter in the context of domestic surveillance when compared with foreign surveillance.

127 I recognize that justifying, in a limited sense, certain forms of "bulk warrants" might be perceived as too expansive. It opens the door for the kind of criticism raised by Judge Pinto de Albuquerque in Szabò & Vissy v. Hungary, App. No. 37138/14, Eur. Ct. H.R. (2016), where the Judge challenged those who believe that the only way to fight terrorism efficiently is through a "net widening, all inclusive" pool of information that is based on a "minimalist suspicion threshold." *Id.* at ¶ 20 (Albuquerque, J. concurring). Albuquerque notes that such an approach reflects "an illusory conviction that global surveillance is the *deus ex machine* capable of combatting the scourge of global terrorism." *Id.* Let me be clear, I do not endorse mass surveillance or the retention of enormous haystacks of data. I merely propose that in the process of testing and developing new capabilities and sources relating to the interception of communications (and only for that purpose), some limited leniency must be given.

regarded as a violation of international human rights law.[128] A system of issuing well-defined bulk warrants for the purposes of identifying relevant bearers and relevant targets, then engaging in targeted collection from those identified bearers and against those identified targets, by reliance on specifically tailored identifiers, will not constitute a program of unlawful mass surveillance. Of course, the devil is in the details and each individual program would have to be scrutinized to ensure these standards are complied with. This is where effective oversight and transparency become crucial.

F. Oversight and Transparency

There is absolutely no reason not to establish the same institutional oversight structures for both domestic and foreign surveillance. Going back to the French example, there is no objective and rational reason not to establish the same mandatory consultative process with the CNCIS prior to the surveillance of both domestic and foreign members of parliament or journalists. In fact, given the greater leniency already provided under this framework, the need for effective and independent review is specifically necessary to minimize potential harms and abuses.[129] But the CNCIS, as it is currently structured, is likely not sufficient.[130] Oversight of both domestic and foreign surveillance must be independent, effective, adequately resourced, and impartial.[131]

---

128 *See, for example*, G.A. Res. 68/167, The Right to Privacy in the Digital Age, 3, U.N. Doc. A/RES/69/166 (Dec. 18, 2014) (noting that the U.N. is "*[d]eeply concerned* at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights.") (emphasis in original); U.N. Hum. Rts. Comm., Concluding Observations on the Initial Report of South Africa, ¶ 43, U.N. Doc. CCPR/C/ZAF/CO/1 (2016) ("The State party should refrain from engaging in mass surveillance of private communications without prior judicial authorization."); OHCHR Report, *supra* note 32, at ¶ 25 ("Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or 'bulk' surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate"); Special Rapporteur on the Promotion and Protection of Human Rights, *supra* note 36, at ¶ 18; *Szabó*, *supra* note 127, at ¶¶ 68–69.

129 *See, for example*, Martin Scheinin (Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism), *Rep. on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, ¶¶ 51–53, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009).

130 For further reading, see Lubin, *supra* note 30.

131 *See, for example*, G.A. Res. 69/166, at ¶ 4 (Dec. 18, 2014); Rep. on the Promotion and Protection of

In his concurring opinion in *Escher et al. v. Brazil,*[132] Judge Sergio García Ramírez of the Inter-American Court of Human Rights described in strong terms the importance of transparency in surveillance operations:

> We reject the furtiveness with which the tyrant hides his intolerable arbitrariness. We condemn the secrecy that shrouds the symbols of authoritarianism. We censure opacity in the exercise of public authority. We demand—and we are achieving, step by step, based on the argument of human rights—transparency in the acts of Government and in the conduct of those who govern us.[133]

It is specifically crucial to insist on greater transparency on the part of the government in the context of foreign surveillance operations. Bringing these programs into the light is the only practical way of developing professional best practices and increasing the pace of norm internalization across intelligence agencies. In this context, particular importance should be given to the governments disclosing more information on their use of selectors, which as described above become the gatekeepers for data collection and access to data. In this context it is important to note a recent judgment of the German Constitutional Court which found that a list of keywords and search parameters (which the BND used to track millions of surveillance targets worldwide, and which were allegedly shared with the NSA) should not be disclosed to the German Parliament's Special Parliamentary Fact-Finding Commission (established following the Snowden revelations). The court's ruling was based on the conclusion that the confidentiality of the selectors list outweighed the public's right to know and the parliament's duty of oversight.[134] This is an unfortunate ruling in this regard.

G. Notification and Remedies

As a whole, the state enjoys a wide margin of appreciation in choosing which form of effective remedies (judicial, legislative, administrative, or a combination

---

Human Rights and Fundamental Freedoms, *supra* note 129, at ¶¶ 51–53; U.N. Hum. Rts. Comm., Concluding Observations on the Sixth Periodic Rep. of Canada, U.N. Doc CCPR/C/CAN/CO/6, ¶ 10 (2015); Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R, Judgment, ¶¶ 54–56 (Sept. 6, 1978).

132 Escher et al. v. Brazil, Preliminary Objections, Merits, Reparations, and Costs Judgment*,* Inter-Amer, Ct. of H.R., (ser. C) No. 200 (July 6, 2009) (Garcia Ramirez, J. concurring).

133 *Id.* at ¶ 6.

134 *See* Manasi Gopalakrishnan, *German Court's Ruling on Mass Spying is a Victory for the BND and NSA*, DW (Nov. 15, 2016), https://perma.cc/VCT8-55VJ. To begin with, oversight bodies, including parliamentary committees and commissions of inquiry, should be provided sufficient security clearances to gain access to all necessary confidential material to conduct their investigation. Moreover, the Government should find more creative ways to provide generalized and redacted information relating to these selector lists to the general public.

thereof) it wishes to offer for violations of privacy through digital surveillance. As Commissioner Pillay had noted, notice and standing become "critical issues in determining access to effective remedy."[135] These issues are even further intensified in the context of foreign surveillance, where both notification processes are hard to establish and where in many countries standing of foreign nationals is significantly limited. It could therefore be justified to limit states' margin of appreciation on issues of notification and remedy in the context of foreign surveillance. This would once again be an area where a tailored human rights framework could set higher, and not lower, standards of protection for the right to privacy.

H. Intelligence Sharing

Incidentally, the *10 Human Rights Organizations* case was also the first case in which the ECtHR was called to explicitly address whether intelligence sharing arrangements (in this case, GCHQ-NSA cooperation within the broader Five Eyes arrangement) must be prescribed by law that is both clear and precise, and must conform to tests of strict necessity and proportionality. In the field of monitoring bilateral and multilateral intelligence sharing arrangements, there has been particular inadequacy of oversight. These arrangements are most often confidential and not subject to public scrutiny, taking the form of secret memoranda of understanding directly between the agencies or the relevant ministries. Such "gentleman's gentlemen's agreements" often expressly state that they are not constructed to be legally binding instruments according to international law.[136] As such, the agreements avoid any need to be ratified under the constitutional procedures and domestic laws of each partner state, and are not required to be registered with the Secretariat of the United Nations in accordance with Article 102 of the U.N. Charter. The U.N. Special Rapporteur on Counter-Terrorism and Human Rights has stated in this regard that:

> The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority. Information concerning an individual's communications may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards . . . . Such practices make the operation of the surveillance

---

135 *See* OHCHR Report, *supra* note 32, at ¶¶ 40–41.

136 *See, for example*, Memorandum of Understanding Pertaining to Protection of U.S. Persons, U.S.-Isr., § I(d), https://perma.cc/KN9N-7D3V (noting that "[t]his agreement is not intended to create any legally enforceable rights and shall not be construed to be either an international agreement or a legally binding instrument according to international law").

> regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the Covenant.[137]

Intelligence Sharing arrangements cover an array of potential engagements between partnering agencies including, *inter alia*, information sharing, operational cooperation, the hosting and administrating of facilities and equipment, joint training and capacity building, and the provision of technical and financial support.[138] Within each of these categories the spectrum of potential involvement is also significantly wide. In the context of information sharing, for example, you may find minimal arrangements for the *ad hoc* sharing of minimized intelligence briefs subject to specific request and approval, as well as far more robust partnerships for the automated dissemination of raw intercepted communications as well as the joint management of databases.[139]

Beyond the revolving door concern, above discussed, sharing intelligence with regimes that are known for disrespecting international legal standards, including international human rights law, puts the populations of those countries at particular risk. Such regimes could, for example, use the intelligence received to engage in the persecution and interrogation of minority groups, immigrant populations, human rights defenders, and journalists.[140]

Moreover, intelligence sharing reduces accountability as agencies fail to scrutinize the source of the raw intelligence they receive in order to ensure "plausible deniability." If such information was collected illegally, through means of torture or mass surveillance, or was based on partial or inaccurate information, the receiving agency is incentivized not to inquire as to the source and the means by which the information was obtained.[141] What more, most intelligence sharing regimes adopt the "originator rule," which provides that the consent of the originator of the information is a prerequisite to any further disclosure of the

---

137 Special Rapporteur on the Promotion and Protection of Human Rights, *supra* note 36, at ¶ 44.

138 For further reading, see BORN, *supra* note 106, at 18–25.

139 For a review of intelligence sharing practices, particularly in the context of the highly-integrated relationship between the U.S. and the U.K. intelligence services, see Privacy Int'l v. Sec'y of State for Foreign and Commonwealth Aff. and the Gov't Commc'n Headquarters, Investigatory Powers Tribunal, Witness Statement of Eric King, IPT/13/92/CH, ¶¶ 70–90 (2014).

140 *See* David Kaye (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*, ¶ 59, U.N. Doc. A/HRC/29/32 (May 22, 2015); Inter-American Comm'n on Human Rights, Annual Rep. of the Office of the Special Rapporteur for Freedom of Expression, ¶ 150, U.N. Doc. OEA/Ser.L/V/II.149 (Dec. 31, 2013).

141 For further reading, see European Commission For Democracy Through Law (Venice Comm'n), Rep. on the Democratic Oversight of the Security Services, Study No. 388/2006 CDL-AD(2007)016, ¶¶ 115-21 (June 11, 2007).

intelligence beyond its immediate receiver, setting a further obstacle on the ability to engage meaningful due diligence and oversight.[142]

For all these reasons, it is quite important to stress that any allowances provided in the foreign surveillance context must only be examined in the context of stronger regulation on intelligence sharing both between agencies within the state[143] and between foreign surveillance agencies more broadly.[144]

V. CONCLUSION: LOSING THE BATTLE BUT WINNING THE WAR

In conclusion it might be worthwhile to compare two prosaic quotes, one from ICJ Judge Antônio Augusto Cançado Trindade, and the other from ICJ Judge ad hoc Ian Callinan, both producing contradictory opinions in the *Timor-Leste v. Australia*[145] case. Judge Trindade wrote:

> Six and a half decades ago (in 1949), in his last book, *Nineteen Eighty-Four*, George Orwell repeatedly warned: "Big Brother Is Watching You." Modern history is permeated with examples of the undue exercise of search and seizure, by those who felt powerful enough to exercise unreasonable surveillance of others. Modern history has also plenty of examples of the proper reaction of those who felt victimized by such exercise of search and seizure. In so reacting, the latter felt that, though lacking in factual power, they had law on their side, as all are equal before the law. If Orwell could rise from his tomb today, I imagine he would probably contemplate writing *Two Thousand Eighty-Four*, updating his perennial and topical warning, so as to encompass surveillance not only at *intra-State* level, but also at *inter-State* level; nowadays, "Big Brother Is Watching You" on a much wider geographical scale, and also in the relations across nations.[146]

Judge Callinan writes in his opinion, as if responding to Judge Trindade:

> All or most nations have, as Australia's pleadings show, intelligence organizations. They have them because they need them. Terrorists now

---

142 *See* European Commission For Democracy Through Law (Venice Comm'n), Update on the 2007 Rep. on the Democratic Oversight of the Security Services and Rep. on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006, ¶ 88 (April 7, 2015).

143 *See, generally*, Charlie Savage, *N.S.A Gets More Latitude to Share Intercepted Communications*, N.Y. TIMES (Jan. 12, 2017), https://perma.cc/689W-3AVT.

144 Privacy International had recently published a briefing mapping out a suggested human rights legal framework for trans-boundary intelligence sharing which offers a possible starting point for potential discussion on future regulation of the practice. *See Privacy International's preliminary views on cross-border* access to *data for intelligence/law enforcement purposes* (June 16, 2017) https://privacyinternational.org/sites/default/files/2017.06.16%20UN%20Counter-Terrorism%20Questionnaire%20-%20PI_0.pdf.

145 Questions Relating to the Seizure and Detention of Certain Documents and Data, Timor-Leste v. Austl., Provisional Measure, 2014 I.C.J. Rep. 167 (Mar. 3).

146 *Id.* at ¶ 51 (separate opinion by Judge Trindade, C.).

> operate within communities which shelter and have succoured them. International law must take cognizance of the painful realities of the vulnerabilities of the people in free nations. Any law or principle of it which does not do that may fail to command obedience as well as respect. It is difficult for those not the possessor of all the relevant information to know which piece of new, or further, or seemingly slight piece of information, will indicate an escalation of risk. Algorithms designed to process such pieces of information to identify risk and its heightening are now universally and ceaselessly employed. And a risk which can arise suddenly and dangerously is to the safety of a particular officer of [sic] officers of an intelligence organization, as well as to the security of the nation itself.[147]

The above exchange, in some respects, tells the story of the kind of binary split that characterizes the debates surrounding foreign mass surveillance. In paraphrasing the old saying, it would seem that intelligence agencies are from Mars and privacy experts are from Venus, and the two could never meet.

In this piece, I tried to argue that in fighting this absolutist war for a universal and unified standard of privacy, equally applicable to both domestic and foreign surveillance, the human rights community is losing the far bigger war. A new operational code has emerged, whereby few if any human rights protections are provided to foreigners' right to privacy. In this regard I completely concur with Professor Margo Schlanger who had noted that the relentless focus on a purist human rights discourse tends to "sweep under the rug" the messiness of civil liberties protection.[148]

This piece proposes recognizing the legitimacy behind certain limited legal differentiations in treatment for domestic and foreign surveillance. Such recognition, quite a concession on the part of the "Geneva echo chamber," would bring government agencies back to the table. It would allow us to begin a serious and long-awaited conversation on what arbitrary interference, necessity, and

---

147 *Id.* at ¶ 33 (dissenting opinion by Judge ad hoc Callinan, I.).

148 Margo Schlanger*, Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6. HARV. NAT'L. SEC. J. 112, 192 (2015); *id.* at 185 ("[R]ights talk hides the necessity of policy judgments and, by its purity, diverts attention from that messier field."). Elsewhere she writes:

> I have suggested that rights discourse tends to sweep under the rug the messiness of civil liberties protections—the policy issues that lie at the core of civil liberties interests. That messiness will be apparent in what follows; there are no magic bullets here. But a measure can be useful even if messy or compromised.

Id. at 192. *See also* Morton J. Horwitz, *Rights*, 23 HARV. C.R.-C.L. L. REV. 393, 403–04 (1988).

> [A] troubling aspect of rights discourse is that its focus on fundamental, inherent, inalienable or natural rights is a way of obscuring or distorting the reality of the social construction of rights and duties. It shifts discussion away from the always disputable issue of what is or is not socially desirable. Rights discourse . . . wishes us to believe instead that the recognition of rights is not a question of social choice at all, as if in the normative and constitutional realm rights have the same force as the law of gravity.

proportionality actually mean in the context of foreign surveillance. Stepping outside the bounds of the catch-all domestic surveillance jurisprudence of the ECtHR, we could begin developing a far more tailored human rights framework for extraterritorial bulk interception operations. This tailored human rights framework, far from introducing more "intelligence legalism" (which merely empowers lawyers to talk more),[149] would actually bridge the gap that already exists between two sets of particularly vocal lawyers, so that privacy protective policies could finally emerge.

[149] Schlanger, *supra* note 148, at 117, 173 (noting that "intelligence legalism brings lawyers' rule-of-law commitment into the realm of national security and surveillance," in part by empowering lawyers; then rejecting the conceptualization that "lawyers, empowered by legalism, turn out to be excellent good civil liberties guardians").