VOLUME 56, NUMBER 1, WINTER 2015

# Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age

Marko Milanovic*

## INTRODUCTION

The 2013 revelations by Edward Snowden of the scope and magnitude of electronic surveillance programs run by the U.S. National Security Agency (NSA) and some of its partners, chief among them the UK Government Communications Headquarters (GCHQ), have provoked intense public debate regarding the proper limits of such intelligence activities. Privacy activists decry such programs, especially those involving the mass collection of the data or communications of ordinary individuals across the globe, arguing that they create an inhibiting surveillance climate that diminishes basic freedoms, while government officials justify them as necessary to prevent terrorism. Snowden's disclosures proved especially damaging for U.S. foreign policy interests when it was revealed that the United States and some of its "Five Eyes" partners[1] spied on the leaders of allied governments, including Germany, Mexico, Brazil, and Indonesia.[2]

* Associate Professor, University of Nottingham School of Law; Visiting Professor, University of Michigan Law School, Fall 2013; Secretary-General, European Society of International Law. E-mail: marko.milanovic@nottingham.ac.uk. I am grateful for their most helpful comments to Gerry Neuman, Peter Margulies, the participants of the Roundtable on Protecting Human Rights in the Age of Surveillance, organized by the Center for Democracy and Technology and the American University Washington College of Law in January 2014, and the participants of the seminar on the Right to Privacy in the Digital Age organized at the United Nations headquarters in Geneva in February 2014. This is a fast-moving topic, and the article takes into account developments as of March 2014. This article incorporates much of the text of a blog series I wrote on the topic from November 25–29, 2013 on *EJIL: Talk!* at http://www.ejiltalk.org/foreign-surveillance-and-human-rights-introduction/, but in a revised and more developed form.

1. The "Five Eyes" is an alliance of five English-speaking countries—the United States, the United Kingdom, Australia, Canada, and New Zealand, focusing mainly on cooperating in the domain of signals intelligence. *See generally* Carly Nyst, *The Five Eyes Fact Sheet*, PRIVACY INT'L (Nov. 26, 2013), https://www.privacyinternational.org/blog/the-five-eyes-fact-sheet; Paul Farrell, *History of 5-Eyes—Explainer,* THE GUARDIAN (Dec. 2, 2013, 12:30 AM), http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

2. *See* Jacob Appelbaum et al., *Berlin Complains: Did U.S. Tap Chancellor Merkel's Mobile Phone?*, SPIEGEL ONLINE (Oct. 23, 2013, 8:20 PM), http://www.spiegel.de/international/world/merkel-calls-obama-over-suspicions-us-tapped-her-mobile-phone-a-929642.html; *Brazil and Mexico Probe Claims U.S. Spied on Presidents*, BBC NEWS (Sept. 2, 2013), http://www.bbc.co.uk/news/world-latin-america-23938909; Ewen MacAskill & Lenore Taylor, *Australia's Spy Agencies Targeted Indonesian President's Mobile Phone*, THE GUARDIAN (Nov. 17, 2013, 7:58 PM), http://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone.

The political fallout of the Snowden disclosures has undoubtedly been very significant. They revealed the sheer technological capacity of the NSA and other signals intelligence agencies to collect personal data on a vast scale and to subvert and intercept communication over the Internet. The public scrutiny of the work of these agencies has been unprecedented, and discussions are ongoing in government and policy circles on how to regulate and reform such activities. Thus, for instance, President Obama appointed a Review Group on Intelligence and Communications Technologies to advise him on possible options for reform, which the Review Group did in an extensive report.[3] The President responded with a series of reform proposals.[4] The U.S. Congress, the European Parliament, and other legislative bodies have held or will be holding committee hearings on the various mass data collection programs.

The purpose of this article, however, is not to assess the general propriety or usefulness of surveillance programs, or their compliance with relevant domestic law. I will not argue that electronic surveillance programs, whether targeted or done on mass scale, are *per se* illegal, ineffective, or unjustifiable. Rather, I will look at how the legality of such programs would be debated and assessed within the framework of international human rights law, specifically under the major human rights treaties to which the "Five Eyes" and other states with sophisticated technological capabilities, such as Germany, France, and Russia, are parties: the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR).[5] Both of these treaties protect the right to privacy. Drawing almost verbatim on Article 12 of the Universal Declaration of Human Rights (UDHR),[6] Article 17 of the ICCPR provides that

3. The President's Review Grp. on Intelligence & Comm'ns Techs., Office of the Dir. of Nat'l Intelligence, Liberty and Security in a Changing World (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter *Review Group Report*].

4. *See infra* notes 55–56 and relevant text.

5. International Covenant on Civil and Political Rights, *adopted* Dec. 16, 1966, S. Exec. Rep. 102–23, 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) [hereinafter ICCPR]; Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Nov. 4, 1950, 213 U.N.T.S. 222 (entered into force Sept. 3, 1953). Australia ratified the ICCPR on August 13,1980; Canada on May 19, 1976; France on November 4, 1980; New Zealand on December 28, 1978; Russia on October 16, 1973; the United Kingdom on May 20, 1976; the United States on June 8, 1992. China signed the ICCPR on October 5, 1998 but has not yet become a party. *See* United Nations, Status of International Covenant on Civil and Political Rights, United Nations Treaty Collection, *available at* https://treaties.un.org/Pages/ViewDetails.aspx?mtdsg_no=iv-4&chapter=4&lang=en. The U.K., France, and Russia are also parties to the ECHR and subject to the compulsory jurisdiction of the European Court of Human Rights. *See* Council of Europe, Status of Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Eur. Treaty Off., *available at* http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=005&CM=8&DF=08/02/2014&CL=ENG.

6. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

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

Article 8 of the ECHR, on the other hand, stipulates that

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

These provisions are broad and vague.[7] They are also coupled with the preliminary threshold question of whether they would apply at all to *extraterritorial* surveillance. But while there are many uncertainties regarding the application of human rights treaties to intelligence gathering, these questions are not insurmountable. Indeed, it is inevitable that human rights language and fora will be used to challenge the legality of electronic surveillance programs, as is already being done by privacy activists.[8] Special rapporteurs of the U.N. Human Rights Council have already started examining the impact of counter-terrorism measures on the right to privacy.[9]

7. Similarly, Article V of the American Declaration of the Rights and Duties of Man provides that "[e]very person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life." American Declaration of the Rights and Duties of Man, OEA/Ser.L./V.II.23, doc. 21, rev. 6 (1948), *reprinted in* Basic Documents Pertaining to Human Rights in the Inter-American System, OEA/Ser.L.V./II.82, doc. 6, rev. 1 at 17. American Convention on Human Rights art. 11, Nov. 21, 1969, 1144 U.N.T.S. 143 is modelled on the text of the UDHR/ICCPR, while also incorporating some of the language of Article V of the American Declaration. The Organization of African Unity, African Charter on Human and Peoples' Rights (Banjul Charter), *adopted on* June 27, 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58, *available at* http://www.refworld.org/docid/3ae6b3630.html, does not explicitly protect the right to privacy.

8. *See International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY & PROPORTIONATE (May 2014), https://en.necessaryandproportionate.org/text (a set of 13 principles drawn from human rights law that would apply to both domestic and extraterritorial surveillance, drafted by numerous civil society organizations in a comprehensive process led by Privacy International, Access, and the Electronic Frontier Foundation).

9. *See* Special Rapporteur on the Promotion and Protection of Human Rights, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009) (by Martin Scheinin); Special Rapporteur on the Promotion and Protection of Human Rights, *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, U.N. Doc. A/HRC/14/46 (May 17, 2010) (by Martin Scheinin); Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) (by Frank La Rue).

Litigation already is or soon will be pending, either before domestic courts in states where human rights treaties are directly applicable, or before international judicial and quasi-judicial bodies. Some of these cases are likely to proceed to an examination of the merits, particularly in Europe, where standing, state secrets and political question doctrines are either non-existent or are not as onerous for applicants to overcome as they are in the United States.[10] GCHQ has long been aware that, if exposed, its mass surveillance programs may be subject to "damaging public debate" and legal challenge on privacy grounds under the ECHR.[11] Indeed, one case before the European Court of Human Rights dealing with GCHQ interception of external communications has already been communicated to the U.K. government, with the Court moving at an almost unprecedented speed in dealing with the case.[12]

Crucially, human rights language has also been used at a purely intergovernmental level. Prompted by allegations of U.S. spying on their leaders, in October 2013 Brazil and Germany submitted a draft resolution entitled "The Right to Privacy in the Digital Age" to the Third Committee of the United Nations General Assembly ("UNGA").[13] After pushback by the United States and its "Five Eyes" allies and the usual diplomatic wrangling (much of it based on arguments that the right to privacy does not apply extraterritorially)[14] the draft underwent revision, obtained more sponsors, and cleared the Third Committee;[15] it was adopted without a vote by the Assembly itself a few weeks later.[16] The revisions were mainly stylistic, toning down, for example, some of the more emphatic references to violations of

10. *Compare* Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013) (holding by 5 votes to 4 that a real likelihood that individuals would be subjected to surveillance measures, rather than proof that such measures were actually taken, was not sufficient for standing, which could not be speculative) *with* Klass v. Germany (Judgment), App. No. 5029/71, 28 Eur. Ct. H.R. (ser. A) (1978), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-73538 (allowing for precisely this kind of speculative standing).

11. *See* James Ball, *Leaked Memos Reveal GCHQ Efforts to Keep Mass Surveillance Secret*, THE GUARDIAN (Oct. 25, 2013, 1:45 PM), http://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden.

12. Big Brother Watch v. United Kingdom (Communicated Case), App. No. 58170/13, Eur. Ct. H.R. (2013). Similarly, a domestic U.K. case was filed before the Investigatory Powers Tribunal by Privacy International. *See Privacy International Files Legal Challenge Against UK Government Over Mass Surveillance Programmes*, PRIVACY INT'L (July 8, 2013), https://www.privacyinternational.org/press-releases/privacy-international-files-legal-challenge-against-uk-government-over-mass.

13. Colum Lynch et al., *Exclusive: Germany, Brazil Turn to U.N. to Restrain American Spies*, FOREIGN POLICY (Oct. 24, 2013, 4:18 PM), http://thecable.foreignpolicy.com/posts/2013/10/24/exclusive_germany_brazil_turn_to_un_to_restrain_american_spies. United Nations General Assembly, Third Comm., The Right to Privacy in the Digital Age, U.N. Doc. A/C.3/68/L.45 (Nov. 1, 2013).

14. Colum Lynch, *Exclusive: Inside America's Plan to Kill Online Privacy Rights Everywhere*, FOREIGN POLICY (Nov. 20, 2013, 1:10 PM), http://thecable.foreignpolicy.com/posts/2013/11/20/exclusive_inside_americas_plan_to_kill_online_privacy_rights_everywhere.

15. United Nations General Assembly, Third Comm., The Right to Privacy in the Digital Age, U.N. Doc. A/C.3/68/L.45/Rev.1 (Nov. 1, 2013).

16. Resolution on the Right to Privacy in the Digital Age, G.A. Res 68/167, U.N. Doc. A/RES/68/167 (Jan. 21, 2014).

or attacks against privacy. But together with the caveats they expressed in the Third Committee, the revisions allowed the resolution to be sufficiently acceptable to the United States and its closest allies.[17]

On any assessment, the Assembly's resolution on the right to privacy in the digital age represents a major development. It firmly puts the issue of electronic surveillance within the framework of international human rights law and directly invokes both Article 12 of the UDHR and Article 17 of the ICCPR. In the preamble, the Assembly expresses its deep concern "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."[18] Operative paragraph three affirms "that the same rights that people have offline must also be protected online, including the right to privacy," while operative paragraph four calls upon states "to respect and protect the right to privacy, including in the context of digital communication"—the reference to the obligation to protect being especially significant since it requires states to regulate the conduct of non-state actors, such as telecommunications companies.[19]

But the most important aspect of the resolution is that it initiates a process, a conversation, on the application of human rights norms to surveillance, interception, and data collection activities, even when such activities are conducted by a state outside its borders. Operative paragraph five of the resolution states:

> *Requests* the United Nations High Commissioner for Human Rights to present a report on the protection and promotion of the

17. The U.S. representative to the U.N. Economic and Social Council, Elizabeth Cousens, explained U.S. support for the revised draft by saying that that the United States understands "this resolution to be focused on State action and consistent with longstanding U.S. views regarding the ICCPR, including Articles 2, 17, and 19." This appropriately subtle diplomatic reference to longstanding U.S. views regarding Article 2 ICCPR allowed the U.S. to seemingly join the consensus on protecting the right to privacy in a digital age while in fact denying that the right to privacy as protected by the ICCPR applies extraterritorially. I will be examining this position in more detail in Part II below. For the full text of Ambassador Cousens' remarks, *see* Ambassador Elizabeth Cousens, U.S. Rep. to the U.N. Econ. & Soc. Council, Explanation of Position for the Third Committee Resolution on the Right to Privacy in the Digital Age (Nov. 26, 2013), http://usun.state.gov/briefing/statements/218078.htm.

18. G.A. Res. 68/167, *supra* note 16 (emphasis added).

19. *Id.* Op. para. 4 also calls upon states

(b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(c) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data.

> right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States.

Numerous meetings, expert seminars, and similar events will of course inform the report, although the report itself will not be the end of the story. Electronic surveillance and related activities will remain on the agenda of U.N. bodies for years to come, especially since the political relevance of the topic shows no signs of abating. The discussion has just started, and it will continue at least partly in *human rights* terms, focusing on the rights and interests of the affected *individuals*, rather than solely on the interests and sovereignty of *states*.[20] It is because of their equal, inherent human dignity that *all* individuals are deserving of some protection for their privacy, not simply because two states made reciprocal arrangements not to spy on each other's citizens.

The primary purpose of this article is to advance this conversation by looking at one specific, threshold issue: whether human rights treaties such as the ICCPR and the ECHR even apply to foreign surveillance. I will use the term "foreign surveillance" loosely, as an umbrella term encompassing a wide range of activities conducted for the purpose of gathering intelligence, ranging from audio-visual observation or surveillance in a narrower sense, to the interception of communications, electronic and otherwise, to the collection, storage, processing, and transfer of personal data to third parties. Note also how the term *foreign surveillance* or *intelligence* can be understood in at least three different ways: as activities undertaken by a state that are directed against individuals who are officials, members or agents of *foreign governments or organizations*; as activities targeted against individuals who are *foreign nationals*; or as activities targeted against individuals who are located *outside the state territory*, who may or may not be its nationals.[21] We will see throughout the article how these three elements—agency, nationality, and location—frequently interact with one another in the regulation of surveillance activities. As states increasingly engage in mass extraterritorial surveillance,[22]

20. Consider, for example, the arbitral proceedings filed by Timor-Leste against Australia, which involve allegations of Australian espionage during treaty negotiations between the two states, as well as a related case filed afterwards before the ICJ. *See* Kate Mitchell & Dapo Akande, *Espionage & Good Faith in Treaty Negotiations: East Timor v Australia*, EJIL: TALK! (Jan. 20, 2014), http://www.ejiltalk.org/espionage-fraud-good-faith-in-treaty-negotiations-east-timor-v-australia-in-the-permanent-court-of-arbitration/.

21. Consider, for example, the definition of foreign intelligence in Exec. Order 12,333, 3 C.F.R. § 3.5(d) (1981), which demarcates the responsibilities of various U.S. intelligence agencies, as "information relating to the capabilities, intentions, and activities of foreign powers organizations or persons, but not including counterintelligence except for information on international terrorist activities."

22. *See* La Rue Report, *supra* note 9, para. 64 (noting that "a number of States have begun to adopt laws that purport to authorize them to conduct extra-territorial surveillance or to intercept communications in foreign jurisdictions. This raises serious concern with regard to the extra-territorial commission

clarifying the threshold question of applicability, as this article attempts to do, is a necessary first step in any human rights analysis of the topic.

The article proceeds in five parts. Part I looks briefly at whether citizenship should be the normative basis for fundamental rights, including the right to privacy. Part II interprets the text of the clauses of human rights treaties that define their territorial scope of application. It compares the jurisdiction clauses of the ECHR and the ICCPR, and critically evaluates the U.S. position on the extraterritorial application of the ICCPR. Part III examines the main strands of the case law of international human rights bodies with respect to the treaties' extraterritorial application, which conceptualize state jurisdiction in human rights treaties either as effective overall control of territories or areas, or as authority and control over individuals. Part IV will apply the different models of jurisdiction to a number of possible factual scenarios of foreign or extraterritorial surveillance. Finally, while the focus of this article is on the threshold question of applicability, that question is in practice inseparable from a substantive analysis on the merits. Part V will thus look at what the right to privacy might substantively entail in the extraterritorial context, if it is indeed found to apply.

The article will show that there is much uncertainty as to how existing case law on the jurisdictional threshold issues might apply to foreign surveillance. It will also argue that this uncertainty should not be overestimated—even if the uncertainty can and is being exploited. We will see how the inherent instability of the spatial and personal models of state jurisdiction in human rights treaties is the product of a balance between considerations of universality and effectiveness. The only truly coherent approach to the threshold question of applicability, I will argue, is that human rights treaties should apply to virtually all foreign surveillance activities. That the treaties apply to such activities, however, does not mean that such activities are necessarily *unlawful*. Rather, the lawfulness of a foreign surveillance program is subject to a fact-specific examination on the merits of its compliance with the right to privacy, and in that, I submit, foreign surveillance activities are no different from purely domestic ones.

## I. Do Foreigners Deserve Privacy?

### A. *Citizenship and the Social Contract*

Before looking at the ICCPR and the ECHR in detail, it is necessary to briefly deal with a prior question—who deserves privacy? One robust feature of U.S. discourse, for example, is a continuing emphasis on *citizenship* as

of human rights violations and the inability of individuals to know that they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance, or seek remedies. . . . These developments suggest an alarming trend towards the extension of surveillance powers beyond territorial borders, increasing the risk of cooperative agreements between State law enforcement and security agencies to enable the evasion of domestic legal restrictions.").

a basis for fundamental rights. This is true not only of case law, such as the U.S. Supreme Court's holding in *Verdugo-Urquidez*,[23] dealing with a search by U.S. agents of a Mexican national's property in Mexico, that non-resident aliens are not protected by the Fourth Amendment to the U.S. Constitution. It is also true of public debate more generally, which frequently starts from the assumption that citizens naturally have constitutional rights, whereas foreigners do not.[24]

While this type of citizenship discourse is especially prominent in the United States, it is by no means confined to it. Notably, the statutes regulating surveillance powers in the "Five Eyes" countries frequently make distinctions between eavesdropping on citizens (and permanent residents) versus non-citizens, as well as surveillance that takes place in or outside the state's territory.[25] Under these statutory frameworks non-citizens enjoy fewer protections than citizens, if they have any rights at all. For instance, some of the most far-reaching surveillance programs conducted by the NSA were authorized under Section 702 of the Foreign Intelligence Surveillance Act (FISA).[26] Section 702(b) of FISA explicitly limits such authorizations so as to prohibit surveillance of *any person* known to be located in the United States, and of any *U.S. person* (defined as a U.S. citizen or permanent resi-

23. United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

24. For example, when commenting on various Snowden disclosures, NSA spokespersons frequently say that the NSA respects the privacy of *U.S. persons*: "[a]ny implication that NSA's foreign intelligence collection is focused on the social media communications of everyday Americans is not true." Richard Esposito et al., *Snowden Docs Reveal British Spies Snooped on YouTube and Facebook*, NBC NEWS, Jan. 27, 2014, http://investigations.nbcnews.com/_news/2014/01/27/22469304-snowden-docs-reveal-british-spies-snooped-on-youtube-and-facebook?lite. Even the critics of expansive governmental counterterrorism policies invoke citizenship. *See, e.g.*, Letter from Anthony D. Romero, Exec. Dir., Am. Civil Liberties Union to the Editor, N.Y. TIMES (May 31, 2013), http://www.nytimes.com/2012/06/01/opinion/when-the-president-orders-a-killing.html?_r=0. ("If President Obama is allowed to execute American citizens without judicial review and outside the theater of war, that astonishing power will forever reside in the hands of future presidents.") *See also* Jennifer Granick, *Eight Questions PCLOB Should Ask About Section 702,* JUST SECURITY (Feb.11, 2014, 9:00 AM), http://justsecurity.org/2014/02/11/questions-pclob-section-702/.

25. For example, in Australia, §§ 8-9 and 15 of the Intelligence Services Act 2001 create various safeguards for Australian persons, defined as Australian citizens or permanent residents. *Intelligence Services Act 2001* §§ 8-9, 15. In New Zealand, § 14 of the Government Communications Security Bureau Act 2003 categorically prohibits the issuance of interception warrants for intelligence-gathering purposes with respect to New Zealand citizens or permanent residents, unless they act as an agent or representative for a foreign government, organization or person. *Government Communications Security Bureau Act 2003*. § 16 similarly protects New Zealand citizens and permanent residents from those interception powers that do not require a warrant. In Canada, § 273.64(2) of the National Defence Act requires intelligence-gathering measures not to be "directed at Canadians or any person in Canada," with Canadians being defined as Canadian citizens and permanent residents. National Defence Act, R.S.C. 1985, c. N-5. UK legislation, on the other hand, does not make distinctions on the basis of citizenship. Rather, § 8(4)-(5) of the Regulation of Investigatory Powers Act 2000 provides that interception warrants do *not* need to target a specific person, premises, or communication if the interception is directed against an "external communication." Investigatory Powers Act, (2000) § 8(4)-(5) CURRENT LAW. S. 20 RIPA further defines "external communication" as "a communication sent or received outside the British Islands." *Id.* This distinction between external and internal communications essentially allows for the bulk collection of any external communications under general warrants issued by a minister.

26. 50 U.S.C. § 1881 *et seq*.

dent) reasonably believed to be located outside the United States. In other words, while non-U.S. citizens and permanent residents will be protected against surveillance when they set foot on U.S. soil, unlike U.S. citizens and permanent residents they will enjoy no such protection when they are outside the United States. For FISA's drafters, therefore, the physical presence of an individual on U.S. territory, and his or her citizenship or residence status, were criteria of categorical normative relevance with regard to the enjoyment of the right to privacy. Like for the Supreme Court in *Verdugo-Urquidez*, a citizen is entitled to privacy no matter where he is located, but the same does not apply for an alien.

In order to assess the implications of a citizenship-oriented approach in international human rights law, we first need to look at its possible justifications. For example, when responding to the advocates of a global human right to privacy,[27] Orin Kerr pointed out that the citizenship-oriented approach stems from a conception of "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."[28] Kerr's statement is but an articulation of a long-standing tradition in American legal thought: an essentially contractarian conception of the Constitution, which sees it as the manifestation of a social compact.

But while social contract theories have a long pedigree, their application in this particular context and in this particular way is deeply problematic, both descriptively and normatively. First, there is quite a leap between the postulated, fictional social contract in Western political philosophy and the drafting and interpretation of positive legal instruments such as the U.S. Constitution. Second, the text of the relevant amendments to the Constitution generally does not differentiate between the rights of citizens and noncitizens, normally speaking of "persons."[29] Third, there is little if any historical evidence that the framers of the Constitution or of its subsequent amendments paid any attention to the question of the extraterritorial application of fundamental rights, or made such strong associations between citizenship and rights. Indeed, that same founding generation was steeped in natural law thinking, proudly declaring "these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness." Self-evident truths and unalienable rights do not mix well with citizenship.

27. *See, e.g.*, David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SECURITY (Oct. 29, 2013, 12:48 PM), http://justsecurity.org/2013/10/29/foreigners-nsa-spying-rights/; Kenneth Roth, *NSA: Our Analogue Spying Laws Must Catch Up with the Digital Era*, THE GUARDIAN (Nov. 10, 2013), http://www.theguardian.com/commentisfree/2013/nov/10/nsa-analogue-spying-laws-surveillance-digital-era.

28. Orin Kerr, *A Reply to David Cole on Rights of Foreigners Abroad*, LAWFARE (Nov. 2, 2013, 1:54 AM), www.lawfareblog.com/2013/11/a-reply-to-david-cole-on-rights-of-foreigners-abroad/.

29. The Fourth Amendment, for its part, speaks of the "people." U.S. Const. amend. IV.

Fourth, even if one accepts the general validity of social contract theories, as the Declaration of Independence does when it proclaims that "to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed," it does not follow from this alone that the contract protects only its parties and that others are completely excluded; that is, that only those who politically legitimated and continue to legitimate the social contract (say by having the rights to vote and to stand for office) are those who can benefit from it.[30] In other words, one can both believe that governments rest on the consent of the governed, derive their just powers therefrom, and are accountable to their citizens, *and* that governments owe certain basic duties toward non-citizens as well. The two are not necessarily incompatible.

While social compact thinking undoubtedly informed the U.S. Supreme Court's case law on the application of constitutional rights to foreigners and abroad, as in *Verdugo*, it would be a stretch to argue that the Court's jurisprudence flows from any coherent grand theory. Rather, the lack of specific textual guidance in the Constitution allowed the Court to make its approach up as it went along, and this is what it continues to do to this very day.[31] The Court's case law has never been consistent—it has oscillated between universalist impulses to protect fundamental rights of all persons and the fear that this protection would be unmanageable in practice, often leading it to resort to citizenship as a limiting principle.

Thus, for example, the majority of the Court in *Eisentrager*[32] held that non-U.S. nationals imprisoned by U.S. forces in occupied Germany were not constitutionally entitled to *habeas corpus*. Justice Jackson wrote for the Court, justifying the lack of protection for foreigners by saying that "[c]itizenship as a head of jurisdiction and a ground of protection was old when Paul invoked it in his appeal to Caesar. The years have not destroyed nor diminished the importance of citizenship, nor have they sapped the vitality of a citizen's claims upon his government for protection."[33] On the other hand, Justice Black wrote for the minority that

> Paul was fortunate enough to be a Roman citizen when he was made the victim of prejudicial charges; that privileged status afforded him an appeal to Rome, with a right to meet his "accusers face to face." Acts 25:16. But other martyrized disciples were not

30. If that were the case, then those classes of people who were historically denied the right the vote (e.g. women, African-Americans, or the poor) would also not be entitled to constitutional protection. On the other hand, through most of American history voting rights were not inextricably tied to citizenship and most U.S. states have experience with alien suffrage. *See generally* Jamin B. Raskin, *Legal Aliens, Local Citizens: The Historical, Constitutional and Theoretical Meanings of Alien Suffrage*, 141 U. PA. L. REV. 1391 (1993).

31. *Cf.* Boumediene v. Bush, 553 U.S. 723 (2008) (5-4 decision) (holding that non-U.S. nationals imprisoned in Guantanamo have a constitutional right to habeas corpus).

32. Johnson v. Eisentrager, 339 U.S. 763 (1950).

33. *Id.* at 769.

> so fortunate. Our Constitution has led people everywhere to hope and believe that, wherever our laws control, all people, whether our citizens or not, would have an equal chance before the bar of criminal justice . . . . Our nation proclaims a belief in the dignity of human beings as such, no matter what their nationality or where they happen to live.[34]

We can clearly see how the *Eisentrager* majority emphasized citizenship, even though its prime concern was a practical one, namely how *habeas corpus* could apply to thousands of foreign prisoners of war. For its part, the minority spoke the language of universality, invoking "the dignity of human beings as such, no matter what their nationality," and *Eisentrager* was not the only case showing a deep disagreement among the justices on the normative justification for fundamental rights. As was shown so clearly by the works of Kal Raustiala[35] and Gerald Neuman,[36] the Supreme Court's case law has ebbed and flowed between many different ideologies and policy considerations. Its decisions on the Constitution's applicability to foreigners and nationals both within and outside U.S. territory are not set in stone, but need to be critically and continually reassessed.

In that regard, grounding fundamental rights in citizenship is open to critiques of moral arbitrariness.[37] In the vast majority of cases we acquire citizenship merely as an accident of birth, not because of any moral desert (for example, because we served in the armed forces, or made some other contribution to society). For example, consider the right to life—in the U.S. constitutional context the right not to have one's life taken without due process of law—and the debate regarding the use of drones for targeted killing of suspected terrorists. Compare the cases of Anwar al-Awlaki, the militant Islamic preacher killed by a U.S. drone strike in Yemen on September 30, 2011,[38] and that of an undeniably innocent 10-year-old child also killed by a U.S. drone strike in Yemen on June 9, 2013.[39] One needs to seriously re-think any theory that argues that al-Awlaki, an avowed enemy of the United States who wanted nothing more than to destroy its social compact—but who just happened to have been born on U.S. soil—was con-

34. *Id.* at 798.

35. Kal Raustiala, Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law (2009).

36. Gerald L. Neuman, *Whose Constitution?*, 100 Yale L.J. 909 (1991); Gerald L. Neuman, *The Extraterritorial Constitution after* Boumediene v. Bush, 82 S. Cal. L. Rev. 259 (2009). *See also* Gerald L. Neuman, Strangers to the Constitution: Immigrants, Borders, and Fundamental Law (1996).

37. *See, e.g.*, David Cole, Enemy Aliens: Double Standards and Constitutional Freedoms in the War on Terrorism (2003).

38. Martin Chulov, *Al-Qaida Cleric Anwar al-Awlaki is Dead, says Yemen*, The Guardian (Sept. 30, 2011), http://www.theguardian.com/world/2011/sep/30/anwar-al-awlaki-dead.

39. Sarah Knuckey, *Anonymous U.S. Officials Admit CIA Accidentally Killed a Yemeni Child in a Drone Strike*, Just Security (Nov. 18, 2013), http://justsecurity.org/2013/11/18/anonymous-officials-admit-cia-accidentally-killed-yemeni-child-drone-strike/.

stitutionally entitled not to have his life taken without due process of law, whereas the perfectly innocent but non-citizen child had no such entitlement. And it was precisely on the basis of such a theory that the strike against al-Awlaki was conducted.[40]

The plausibility of the contractarian, citizenship account is not helped by its manifest inconsistency. Note how even among ardent contractarians it is routinely accepted that foreigners have constitutional rights *once they are on U.S. territory*. This is simply *obvious*. But the obviousness is rarely explained, other than by arguing to tradition—it has always been like this—which is of course normatively neither here nor there.[41] In other words, if one is entitled to fundamental rights because one is a citizen and hence a member of the social contract, it is not at all clear why one would become a member deserving of protection merely by touching one atom of American soil, like some modern-day Antaeus.

In *Eisentrager,* Justice Jackson tried to explain this inconsistency by saying that a foreigner's "[m]ere lawful presence in the country creates an implied assurance of safe conduct and gives him certain rights."[42] It seems no less dubious for fundamental rights to depend on a *stamp* in one's passport than on the passport itself. To disprove this theory one need only point to aliens present in the country *unlawfully*, who in the United States number in the millions, whose basic rights are unquestionably deserving of protection, but who have no such "implied assurance of safe conduct." From a purely contractarian perspective territorial sovereignty cannot possess some magical protective quality for the foreigner—a consistent contractarian would have to accept, at the very least, that illegal aliens enjoy no constitutional rights whatsoever.[43]

---

40. *See* Eric Holder, Att'y Gen., U.S. Dept. of Justice, Attorney General Eric Holder Speaks at Northwestern University School of Law (Mar. 5, 2012), *available at* http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html. Attorney General Holder stated inter alia that "the government must take into account all relevant constitutional considerations with respect to United States citizens—even those who are leading efforts to kill innocent Americans. Of these, the most relevant is the Fifth Amendment's Due Process Clause, which says that the government may not deprive a citizen of his or her life without due process of law." Note that the Due Process Clause actually says that "no *person* . . . shall be deprived of life, liberty, or property, without due process of law." It makes no mention of citizenship—but the Attorney General then went on to articulate what due process would require under the circumstances (e.g. imminence of threat and no feasibility of capture), limitations on the use of lethal force that would in his view not apply to non-citizens.

41. For one defense of the various distinctions drawn in the U.S. context, see Andrew Kent, *Citizenship and Protection*, 82 Fordham L. Rev. 101 (2014); *A Textual and Historical Case Against a Global Constitution*, 95 Geo. L.J. 463 (2007).

42. *Eisentrager*, 339 U.S. at 770.

43. Needless to say, this is not the position in U.S. law. *See, e.g.*, Zadvydas v. Davis, 533 U.S. 678, 693 (2001) ("[T]he Due Process Clause applies to all 'persons' within the United States, including aliens, whether their presence here is lawful, unlawful, temporary, or permanent."); Plyler v. Doe, 457 U.S. 202, 210 (1982) (holding that "[w]hatever his status under the immigration laws, an alien is surely a 'person' in any ordinary sense of that term. Aliens, even aliens whose presence in this country is unlawful, have long been recognized as 'persons' guaranteed due process of law by the Fifth and Fourteenth Amendments"); Wong Wing v. United States, 163 U.S. 228, 238 (1896) (holding that "it must be concluded that all persons within the territory of the United States are entitled to the protection guaranteed by [the

In other words, it is normatively incoherent to say that before being killed by the U.S. government (1) a U.S. national on U.S. soil is entitled to due process; (2) a non-U.S. national lawfully on U.S. soil (e.g. a tourist) is entitled to due process; (3) a non-U.S. national *unlawfully* on U.S. soil is entitled to due process; (4) a U.S. national *outside* U.S. soil is also entitled to due process; but that *only* (5) a non-U.S. national outside U.S. territory has no entitlement to due process. It seems impossible to identify a principle whereby (5) can truly be distinguished from (1)-(4), and I have never seen it persuasively explained why this should be the case—this distinction is all too often assumed rather than argued, and even when it is argued this is usually done in a perfunctory way.[44]

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 compact." Their rationale is far more prosaic: one not grounded in moral theory, principle, or philosophy, but in political expediency.[45] 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 neighbor with whom we will empathize (even if he is an illegal alien), drones in Pakistan are a different story. 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.

My point in making this rather substantial digression into U.S. constitutional law is that the question of its extraterritorial application, to citizens as well as to aliens, was not predetermined by the Constitution's Framers. Rather, it is, and has always been, a moral choice. It is ultimately for U.S. lawyers, officials, courts, and the general public to make this choice. They

---

Fifth and Sixth] amendments"); Yick Wo v. Hopkins, 118 U.S. 356, 369 (1886) (holding that the "fourteenth amendment to the constitution is not confined to the protection of citizens. . . . These provisions are universal in their application, to all persons within the territorial jurisdiction, without regard to any differences of race, of color, or of nationality; and the equal protection of the laws is a pledge of the protection of equal laws.").

44. *See* Review Group Report, *supra* note 3, at 152 (demonstrating a similar argument applied in the surveillance context).

45. *Cf.* Samuel Issacharoff & Richard H. Pildes, *Drones and the Dilemma of Modern Warfare*, *in* Drone Wars: The Transformation of Armed Conflict and the Promise of Law (Peter Bergen & Daniel Rothenberg, eds., forthcoming 2014) (draft at 18–19), *available at* http://papers.ssrn.com/abstract=2268596 ("Differentiating the treatment of threats coming from citizens as opposed to non-citizens is a deeply controversial matter, both in theory and in international law. Particularly when force can be used only once the enemy 'target' is highly individuated, in terms of his specific actions, it is not at all clear why, in principle, an American citizen in the same overseas location who poses the identical threat as a non-American should have greater legal protection. As a matter of domestic politics, perhaps, one can understand why political leaders would want to ensure their own citizens that they receive special protection against the exceptional circumstance of their own government using lethal force against them. But as a matter of law, why should governments have the power to kill non-citizens who could otherwise be captured but not kill citizens in that circumstance?").

may do so consistently, or not.[46] And the contours of that choice may well evolve over time, as circumstances change.

### B. *The Decline of Citizenship*

Indeed, that process of evolution may currently be underway. In the targeted killing context, for example, even though his Attorney General[47] and the Department of Justice[48] argued that outside U.S. territory only citizens are constitutionally entitled not to be killed without due process of law, in a May 2013 speech on U.S. counterterrorism strategy President Obama articulated a somewhat different sentiment:

> Of course, the targeting of any American raises constitutional issues that are not present in other strikes—which is why my administration submitted information about Awlaki to the Department of Justice months before Awlaki was killed, and briefed the Congress before this strike as well. But the high threshold that we've set for taking lethal action applies to all potential terrorist targets, regardless of whether or not they are American citizens. This threshold respects the inherent dignity of every human life.[49]

The standards the President referred to ostensibly include a near-certainty that no civilians will be killed or injured, and the infeasibility of capture of the targeted individual. While it is clear that the President was articulating standards of policy, rather than advocating a shift in the constitutional position, he was still saying that his administration will treat citizens and non-citizens alike in the targeted killings context.[50] The substantive standard would thus be the same—whether it is high enough, or is actually enforced, is a different matter. And the reason the President gave for applying the same standard was one very much grounded in a universalist conception of

46. *See also* Marko Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy 67–83 (2011).

47. *See* Holder, *supra* note 40.

48. U.S. Dep't of Justice, *Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who Is a Senior Operational Leader of al-Qa'ida or An Associated Force*, *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf.

49. Barack Obama, President of the United States, Remarks by the President at the National Defense University (May 23, 2013) (transcript available at http://www.whitehouse.gov/photos-and-video/video/2013/05/23/president-obama-speaks-us-counterterrorism-strategy#transcript).

50. Simultaneously with the speech the administration released a policy guidance. *See* Press Release, The White House, Office of the Press Sec'y, Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations outside the United States and Areas of Active Hostilities (May 23, 2013) *available at* http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism. The substantive standards do not distinguish between citizens and non-citizens but do say that "[i]f the United States considers an operation against a terrorist identified as a U.S. person, the Department of Justice will conduct an additional legal analysis to ensure that such action may be conducted against the individual consistent with the Constitution and laws of the United States." *Id.*

individual rights—the need to respect "the inherent dignity of every human life."

In the surveillance context we can observe a similar development. When discussing Section 702 of the FISA, which is directed against non-U.S. persons located outside U.S. territory, the President's Review Group noted in its report the need to safeguard the legitimate privacy interests of foreigners, while simultaneously justifying the distinctions drawn by the FISA in the following terms:

> FISA's especially strict limitations on government surveillance of United States persons reflects not only a respect for individual privacy, but also—and fundamentally—a deep concern about potential government abuse *within our own political system*. The special protections for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system. In light of that history and those concerns, there is good reason for every nation to enact *special* restrictions on government surveillance of those persons who participate directly in its own system of self-governance.[51]

This reasoning is unpersuasive. It is certainly true that the surveillance of ordinary people on a mass scale will be detrimental to any free, democratic society, and has been the hallmark of many repressive regimes, but this does not *ipso facto* justify drawing categorical distinctions between citizens (or permanent residents) and foreigners, whose privacy interests are no less worthy of protection.

Indeed, the FISA itself does not actually draw distinctions in protection on the basis of direct participation in the U.S. system of self-governance. Section 702(b)(1) of the FISA provides that authorized surveillance measures "may not intentionally target *any person* known at the time of acquisition to be located in the United States."[52] In other words, an ordinary tourist or visitor to the United States would be equally protected by the FISA as a U.S. citizen or permanent resident, as would be the case with the Fourth Amendment. And such persons certainly do *not* directly participate in the American system of self-governance. Neither do U.S. permanent residents, who only have the potential for such participation once they acquire citizenship, yet are (unlike non-nationals or residents) protected by Section 7(b)(3) of the FISA even when they are abroad. It is hard to see how affording greater protections to, for example, a U.S. citizen who has been living in France for

51. Review Group Report, *supra* note 3, at 154. Somewhat cynically the Report proceeds to add that affording greater protection to U.S. persons as opposed to non-U.S. persons has the potential to promote democratic accountability and ideals abroad, essentially because other states would be shown how to enact greater protections for their own nationals or residents and would emulate the United States. *Id.*

52. Foreign Intelligence Surveillance Act, 50 U.S.C. ch. 36 (emphasis added).

the past 30 years and does not vote in any U.S. elections, as opposed to an ordinary French citizen also living in France, can be justified on the basis of the need to protect American democratic self-government.

Be that as it may, the Review Group went on to note that "there are sound, indeed, compelling reasons to treat the citizens of other nations with dignity and respect" and that failing to do so can have numerous adverse consequences on U.S. interests.[53] But perhaps the most compelling reason for protecting the privacy of foreigners, in the Review Group's view,

> is the simple and fundamental issue of respect for personal privacy and human dignity—wherever people may reside. The right of privacy has been recognized as a basic human right that all nations should respect. Both Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights proclaim that "No one shall be subjected to arbitrary or unlawful interference with his privacy. . . ." Although that declaration provides little guidance about what is meant by "arbitrary or unlawful interference," the aspiration is clear. The United States should be a leader in championing the protection by all nations of fundamental human rights, including the right of privacy, which is central to human dignity.[54]

The Review Group is here not only speaking the language of human rights and human dignity, but is directly invoking the UDHR and the ICCPR in the foreign surveillance context. President Obama also took up the dignity/universality theme in his response to the Review Group's report. While his major speech on the topic was mainly geared toward domestic audiences, the President nonetheless noted that the "bottom line is that people around the world, regardless of their nationality, should know that the United States is not spying on ordinary people who don't threaten our national security, and that we take their privacy concerns into account in our policies and procedures. This applies to foreign leaders as well."[55] In his policy directive, however, the President was even more explicit:

---

53. Review Group Report, *supra* note 3, at 155.

54. *Id.* at 155–56.

55. Barack Obama, President of the United States, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) (transcript available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence). The President continued on to say that:

> Given the understandable attention that this issue has received, I have made clear to the intelligence community that unless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies. And I've instructed my national security team, as well as the intelligence community, to work with foreign counterparts to deepen our coordination and cooperation in ways that rebuild trust going forward.
>
> Now let me be clear: Our intelligence agencies will continue to gather information about the intentions of governments—as opposed to ordinary citizens—around the world, in the same way that the intelligence services of every other nation does. We will not apologize

> All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and 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.[56]

The appropriate safeguards under the directive include treating U.S. and non-U.S. persons equally with regard to the minimization procedures on the dissemination and retention of personal information, data security, access, and quality: "[t]o the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."[57]

One could criticize President Obama's reform as being largely cosmetic or rhetorical. The "national security" caveat allows for wiggle-room, and distinctions remain in U.S. law on surveillance on the basis of nationality or immigration status, for example in the FISA. Even so, the rhetoric itself still matters. The explicit recognition that foreigners have dignity and privacy interests deserving of respect is of great importance, and undermines the exclusionary social contractarian thinking that pervades much of the area. It is also consistent with a general diminishment of the importance of citizenship in a globalized world.[58]

This is not to say, however, that the United States has completely embraced a universalist vision of individual rights. The situation is very much one of flux, in a process that is both political and cultural and ultimately might not coalesce around the rights of foreigners or may pay them only lip service. Who knows, for example, what the next elections will bring, or whether what progress has already been made could become yet one more casualty of a possible major terrorist attack.

### *C. Citizenship and Human Rights*

The U.S. polity is in the process of deciding whether fundamental rights should be grounded in citizenship. But whatever that choice ultimately turns out to be within the United States, it has already been made in the international human rights system. By their very definition, *human* rights cannot turn on nationality alone. Human rights treaties are not social com-

---

simply because our services may be more effective. But heads of state and government with whom we work closely, and on whose cooperation we depend, should feel confident that we are treating them as real partners. And the changes I've ordered do just that.

56. Office of the White House Secretary, Presidential Policy Directive — Signals Intelligence Activities/PPD-28, White House (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

57. *Id.*

58. *See, e.g.*, Peter J. Spiro, *Sovereigntism's Twilight*, 31 BERKELEY J. INT'L L. 307 (2013).

pacts, nor can their applicability depend on morally arbitrary criteria such as the mere accident of birth; they are grounded in the idea that all human beings possess inherent dignity deserving of protection.[59] As well put by Ronald Dworkin, "[t]he domain of human rights has no place for passports."[60]

The idea of the universality of human rights was born out of bitter experience. History has long taught us that predicating fundamental rights upon citizenship allows for rights to be denied if citizenship is revoked or curtailed. I need only mention the disemancipation of the German Jews through the 1935 Nuremberg Laws,[61] or the stripping of the citizenship of South African blacks through the creation of the Bantustans and the passing of the 1970 Black States Citizenship Act.[62] Although there is no inevitable causal relationship between apartheid and genocide, and predicating rights upon citizenship, we do know where that road *in extremis* can take us. This is why human rights jurisprudence outside the relatively narrow areas of immigration and political rights has treated nationality as a potentially prohibited grounds of discrimination, allowing distinctions based upon citizenship only if they are objectively and reasonably justified.[63]

---

59. Note, in that regard, the UDHR's emphatic endorsement in its preamble of the idea that the "recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world" and the admonition of its Article 1 that "[a]ll human beings are born free and equal in dignity and rights."

60. RONALD DWORKIN, IS DEMOCRACY POSSIBLE HERE? 48 (2006).

61. *See generally* HENRY FRIEDLANDER, THE ORIGINS OF NAZI GENOCIDE: FROM EUTHANASIA TO THE FINAL SOLUTION 24–25 (1995).

62. *See generally* JOHN DUGARD, HUMAN RIGHTS AND THE SOUTH AFRICAN LEGAL ORDER (1978); JAMES CRAWFORD, THE CREATION OF STATES IN INTERNATIONAL LAW 338–348 (2nd ed. 2007).

63. *See, e.g.*, Gaygusuz v. Austria (Judgment), App. No. 17371/90, 1996-IV Eur. Ct. H.R. para. 42, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58060 (holding that "very weighty reasons would have to be put forward before the Court could regard a difference of treatment based exclusively on the ground of nationality as compatible with the Convention"). The holding in *Gaygusuz* was affirmed, for example, in *Andrejeva v. Latvia* (Judgment), App. No. 55707/00, Eur. Ct. H.R. (2009), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91388; U.N. Human Rights Comm., *General Comment No. 15: The Position of Aliens Under the Covenant* (1986), para. 2, *available at* http://www.refworld.org/docid/45139acfc.html ("[T]he general rule is that each one of the rights of the Covenant must be guaranteed without discrimination between citizens and aliens. Aliens receive the benefit of the general requirement of non-discrimination in respect of the rights guaranteed in the Covenant, as provided for in article 2 thereof. This guarantee applies to aliens and citizens alike. Exceptionally, some of the rights recognized in the Covenant are expressly applicable only to citizens (art. 25), while article 13 applies only to aliens.") and para. 7 ("Aliens thus have an inherent right to life, protected by law, and may not be arbitrarily deprived of life. . . . They may not be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. . . . Aliens are entitled to equal protection by the law. There shall be no discrimination between aliens and citizens in the application of these rights. These rights of aliens may be qualified only by such limitations as may be lawfully imposed under the Covenant."); U.N. Human Rights Comm., *General Comment No. 31: Nature of the General Legal Obligation on States Parties to the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004) [hereinafter *General Comment No. 31*] ("As indicated in General Comment 15 adopted at the twenty-seventh session (1986), the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons, who may find themselves in the territory or subject to the jurisdiction of the State Party."); U.N. Comm. on the Elimination of Racial Discrimination, *Gen. Recommendation No. 30: Discrimination Against Non-Citizens*, U.N. Doc. CERD/C/64/Misc.11/rev.3 (2004).

Accordingly, we can draw two basic lessons from the preceding discussion for the applicability of human rights treaties to foreign surveillance programs:

First, the threshold question of whether individuals enjoy human rights generally, and the right to privacy specifically, vis-à-vis a particular state should in principle not depend on whether they have that state's nationality. When it comes to the interpretation of the jurisdiction clauses in human rights treaties, which I will address below, an individual cannot be within the jurisdiction of a state party merely because he or she is a national of that state.[64] In other words, if the United Kingdom simultaneously intercepts the electronic communication of one U.K. national and one non-U.K. national living outside the country, either both or neither have human rights vis-à-vis the United Kingdom. The citizen must not be treated preferentially.

Second, if 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.[65] 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.[66] This is particularly so because it simply cannot reasonably be argued that non-citizens *as a class are* inherently more dangerous to the security of a state than its own citizens or permanent residents (viz. the July 7, 2005 London tube terrorist bombings, conducted by U.K. nationals, the November 5, 2009 mass shootings at Fort Hood, Texas, by Nidal Hasan, a U.S. national and then a major in the U.S. Army, or the April 15, 2013 Boston Marathon bombings, perpetrated by the Tsarnaev brothers, one of whom was a U.S. citizen and the other a U.S. permanent resident).[67]

64. As a formal matter, this is so because the concept of state jurisdiction in human rights treaties is not the same as that of a state's jurisdiction to prescribe the rules of its own domestic law, under which nationality is a recognized head of jurisdiction. That, for example, the United States can pass penal laws criminalizing murder if committed by one of its own citizens abroad, or tax legislation requiring its citizens living abroad to pay taxes to the U.S. government (both of which are exercises of prescriptive jurisdiction), does not mean that an American in Paris who commits a murder or fails to pay his U.S. taxes is ipso facto subject to the U.S. jurisdiction in the sense of Art. 2(1) of ICCPR. *See generally* Milanovic, *supra* note 46, at 19–41.

65. *See supra* text accompanying note 63.

66. *Cf.* the discussion in the Review Group Report, *supra* note 3, at 156–57, on how some distinctions would be "warranted by the *special* obligation the United States Government owes to 'the people' of the United States."

67. *See also* Sandra Laville, *MI5 Chief Says 34 UK Terror Plots Disrupted Since 7/7 Attacks*, The Guardian (Nov. 7, 2013), http://www.theguardian.com/uk-news/2013/nov/07/mi5-chief-34-uk-terror-plots-disrupted (reporting on the testimony of the chief of the UK Security Service (MI5) before the Intelligence

This is not to say, on the other hand, that no distinctions may be drawn at all on the basis of the location or type of surveillance or other individual characteristic of the target. But it would be difficult for the United Kingdom to justify, for example, having one surveillance regime for its own citizens living in the country, and another for foreign nationals who are also in the country, or to treat citizens and non-citizens radically differently in an extraterritorial context.[68] Thus, for instance, in the *Belmarsh* case the House of Lords struck down the U.K. government's post-9/11 order derogating from Article 5 of the ECHR, which allowed for the preventive security detention of foreign nationals, on the grounds that distinguishing between nationals and foreigners in the counter-terrorism context was disproportionate, discriminatory, and irrational.[69] This was also the conclusion of a unanimous Grand Chamber of the European Court of Human Rights, despite the fact that it was prepared to pay the United Kingdom significant deference in determining whether an emergency threatening the life of the nation in the sense of Article 15 of the ECHR existed and what measures were appropriate to deal with that emergency:

> The choice by the Government and Parliament of an immigration measure to address what was essentially a security issue had the result of failing adequately to address the problem, while imposing a disproportionate and discriminatory burden of indefinite detention on one group of suspected terrorists. As the House of Lords found, there was no significant difference in the potential adverse impact of detention without charge on a national or on a non-national who in practice could not leave the country because of fear of torture abroad. . . . [T]he Court notes that the national courts, including SIAC, which saw both the open and the closed material, were not convinced that the threat from non-nationals was more serious than that from nationals. In conclusion, therefore, the Court, like the House of Lords, and contrary to the Government's contention, finds that the derogating measures were disproportionate in that they discriminated unjustifiably between nationals and non-nationals.[70]

In sum, one cannot escape the conclusion that under the moral logic of human rights law, citizens and non-citizens are equally deserving of protec-

---

and Security Committee of Parliament, stating that "[t]here are several thousands of individuals in this country who I would describe as supporting violent extremism or engaged in it in some way that we are aware of, and the terrorist plots that we have dealt with have almost all come from those people").

68. The United Kingdom, unlike the United States, does not discriminate on the basis of nationality, with RIPA distinguishing only between external and internal communications. *See supra* note 25.

69. A. v. Sec'y of State for the Home Dep't, [2004] UKHL 56, [2005] 2 A.C. 68 (H.L.) [43] (appeal taken from Eng.).

70. A. v. United Kingdom (Judgment), App. No. 3455/05, Eur. Ct. H.R. paras. 186–90 (2009), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91403.

tion of their rights generally, and privacy specifically. In the counterterrorism and surveillance context, non-citizens neither inherently pose a greater threat to a state's security than its citizens, nor is their private information of inherently greater value or interest to the state.[71] If citizenship is normatively irrelevant for the threshold question of whether a human rights treaty applies to a particular act of surveillance, and may be relevant only for the substantive merits question of whether the right to privacy or the prohibition of discrimination have been violated, then the truly critical question becomes the territorial scope of human rights treaties on the basis of *the location of the individual and/or the interference with his rights*, regardless of that person's nationality. With this in mind, let us look at whether the text of the ICCPR allows for its extraterritorial application.

## II. Interpreting the ICCPR

### A. *Comparing the ICCPR and the ECHR*

The scope of many human rights treaties is at least partly determined by how we interpret their jurisdiction clauses, and here we can observe some important differences. I will limit this analysis solely to the ICCPR and the ECHR—the former because most states engaging in overseas surveillance are parties to it (like the United States) and the latter because of the relative strength and influence of its enforcement mechanism and the European Court of Human Rights' extensive (and conflicting) jurisprudence on questions of territorial application.[72] This section will deal specifically with the ICCPR, the most widely ratified human rights treaty protecting the right to privacy, with 168 states parties as of the time of writing,[73] and the text of which poses unique interpretative problems that we do not find in other human rights treaties. I will also address in the section the categorical position against the extraterritorial application of the ICCPR that has been espoused by the United States, as the state with most sophisticated electronic surveillance capabilities.

Article 2(1) of the ICCPR provides that "[e]ach State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant," whereas Article 1 of the ECHR stipulates that the "High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention." The main difference between the two provisions is the ICCPR's mention of territory. The ICCPR also explicitly distinguishes between the obligations to respect and to ensure

71. If anything, the value of the information of the people living within the state, most of whom would be its citizens, would be greater due to the increased potential that these individuals have to harm the state when present in its own territory, as was for instance the case with the 9/11 hijackers.

72. *See generally* Milanovic, *supra* note 46.

73. Status of ICCPR, *supra* note 5.

human rights, while the ECHR speaks of the obligation to respect in the heading of Article 1, but only of the obligation to secure in the actual text.[74]

The magic word in both texts is (state) "jurisdiction," but the question arises whether the ICCPR's seemingly conjunctive reference to territory admits of *any* extraterritorial application, i.e. whether an individual who is subject to the jurisdiction but not within the territory of the state can be protected by the ICCPR. If the ICCPR can in principle apply extraterritorially, a further question is whether the interpretations of the ICCPR and the ECHR in that regard should align or not, bearing in mind the differences between the two texts.

### *B. The U.S. Position on the ICCPR*

The United States has argued that the Covenant's text precludes any kind of extraterritorial application, i.e. that an individual who is not located in a territory over which the state has sovereign title can never have rights under the treaty vis-à-vis that state. But the U.S. views on the extraterritorial application of the ICCPR have not been as clear, long-standing or principled as some claim.[75] It is true that during the drafting of the Covenant the United States proposed to modify the original language of what was to become Article 2(1)—"within its jurisdiction," the formula that was taken up by the drafters of the ECHR[76]—so that it became "within its *territory and subject to* its jurisdiction."[77] Much was later made of this drafting change by the George W. Bush administration in the context of the "war on terror", as well as by Michael Dennis writing in the *American Journal of International Law*.[78] Yet not only are the *travaux* much more ambiguous than the U.S. government has claimed, but it is simply factually wrong to insist on a supposed half-century of continuity in the U.S. position. Indeed, the story of the ICCPR's drafting and adoption is riddled with interruptions and de-

74. On positive obligations in the ECHR and the ICCPR, *see generally* PIETER VAN DIJK ET AL., THEORY AND PRACTICE OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 13 (4th ed. 2006); MANFRED NOWAK, UN COVENANT ON CIVIL AND POLITICAL RIGHTS: CCPR COMMENTARY 37–41 (2d ed. 2005). I will return to the distinction between positive and negative obligations below.

75. *See, e.g.*, Cable from the Permanent Mission of the United States to the United Nations in Geneva, *UN Human Rights Committee – USG July 17018 Public Hearing*, http://www.state.gov/documents/organization/131739.pdf, para. 12 (noting the opposition of members of the Human Rights Committee to the United States' "long-standing and principled legal interpretation" that the ICCPR is not applicable to activities of States Parties outside of their territory); Ashley Deeks, *Does the ICCPR Establish an Extraterritorial Right to Privacy?*, LAWFARE (Nov. 14, 2013), http://www.lawfareblog.com/2013/11/does-the-iccpr-establish-an-extraterritorial-right-to-privacy/ (noting the United States' position that the scope of the ICCPR limits its application to U.S. Government activity within U.S. territory only).

76. *See* 3 COLLECTED EDITION OF THE "TRAVAUX PRÉPARATOIRES" OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 260 (1976).

77. *See* MARC BOSSUYT, GUIDE TO THE "TRAVAUX PRÉPARATOIRES" OF THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 49 (1987).

78. *See* Michael J. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation*, 99 AM. J. INT'L L. 119 (2005).

lays.[79] The principal drafting of the text was mostly done from 1947 to 1954; the United States actively took part. But the ideological divisions brought about by the Cold War made it impossible for states to agree to what was then a single human rights Covenant. After much wrangling, a political decision was made to split the Covenant into two, followed by further deliberations and the adoption of the texts and the opening for signature of the ICCPR and the International Covenant on Economic, Social and Cultural Rights (ICESCR) in 1966. The two Covenants entered into force ten years later, in 1976. The United States did not even sign the two Covenants until October 5, 1977, under the Carter administration.[80] It ultimately ratified the ICCPR only in 1992, under the George H.W. Bush administration, and never ratified the ICESCR.[81]

Rather than having a consistent position against the extraterritorial application of the ICCPR, during most of this extended period neither the United States nor other states expressed any kind of clear view, let alone agreement, on the Covenant's territorial scope. A deeper look at the *travaux* in the main drafting stages in particular shows the complete lack of conceptual coherence among the drafters. Territorial scope was but one of many issues they were considering, and while some states were concerned about the application of the Covenant to *specific problems* (notably that the Covenant should not require them to *protect* their nationals abroad against third states, or *legislate* for the people of occupied Germany), the preparatory work is remarkably unhelpful when it comes to any first principles regarding the interpretation of Article 2(1).[82] The *travaux* certainly do not express a clear sentiment by the drafters that the Covenant should never apply extraterritorially. This was indeed the International Court of Justice (ICJ)'s conclusion upon looking at the *travaux* in the *Wall* case,[83] and is also the conclusion of a number of other detailed examinations.[84]

79. On the course of the drafting of the Covenant see, e.g., BOSSUYT, *supra* note 77; KAREN DA COSTA, THE EXTRATERRITORIAL APPLICATION OF SELECTED HUMAN RIGHTS TREATIES 17–40 (2012); MICHAL GONDEK, THE REACH OF HUMAN RIGHTS IN A GLOBALISING WORLD: EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES 75–120 (2009).

80. *See* Status of ICCPR, *supra* note 5 (detailing signing and ratification status of the ICCPR by U.N. member states); *see also* Id., https://treaties.un.org/Pages/ViewDetails.aspx?mtdsg_no=iv-3&chapter=4&lang=en. (detailing signing and ratification status of ICESCR by U.N. member states).

81. *Id.*

82. *See* MILANOVIC, *supra* note 45, at 222–27.

83. *See* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, 179 (July 9), *available at* http://www.icj-cij.org/docket/files/131/1671.pdf (stating that "the *travaux préparatoires* of the Covenant confirm the [Human Rights] Committee's interpretation of Article 2 of that instrument. These show that, in adopting the wording chosen, the drafters of the Covenant did not intend to allow States to escape from their obligations when they exercise jurisdiction outside their national territory. They only intended to prevent persons residing abroad from asserting, vis-à-vis their State of origin, rights that do not fall within the competence of that State, but of that of the State of residence.").

84. *See* da Costa, *supra* note 78, at 40; Gondek, *supra* note 78, at 118–19; Noam Lubell, Extraterritorial Use of Force Against Non-State Actors 195 (2010); Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORD. L. REV. 2137 (2014); Nigel

After the adoption of the text of the ICCPR came several decades of silence during which the issue of the ICCPR's extraterritorial application was simply not on anybody's agenda. When the first Bush administration reinitiated the ratification process in the U.S. Senate, no mention was made of the question of the ICCPR's extraterritorial application.[85] Nor was the issue raised in the U.S. initial report to the Human Rights Committee,[86] even though the Committee's first cases deciding that the Covenant can apply extraterritorially predated both the report and the U.S. ratification.[87]

The first time the U.S. government clearly articulated the position that the ICCPR cannot apply extraterritorially *tout court* was when its initial report was discussed before the Committee in March 1995, and it did so in response to a question by a member of the Committee:

> Mr. Klein had asked whether the United States took the view that the Covenant did not apply to government actions outside the United States. 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.[88]

Note how the U.S. representative made three arguments against the extraterritorial application of the ICCPR: (1) the existence of a default presumption against extraterritorial application; (2) the ordinary meaning of "within its territory" coupled with a conjunctive "and"; (3) the "clear understanding" to that effect from the preparatory work. Of these three arguments only

---

Rodley, *The Extraterritorial Reach and Applicability in Armed Conflict of the International Covenant on Civil and Political Rights*, 5 EUR. HUM. RTS. L. REV. 628 (2009); Margaret Satterthwaite, *Rendered Meaningless: Extraordinary Rendition and the Rule of Law*, 75 GEO. WASH. L. REV. 1333, 1361 (2007); Beth Van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations*, 90 INT'L L. STUD. 20 (2014).

85. The Senate certainly made no declarations or understandings in that regard. *See* S. EXEC. REP. NO. 102–23 (1992), *available at* http://sitemaker.umich.edu/drwcasebook/files/senate_committee_on_foreign_relations_report_on_the_iccpr.pdf.

86. U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, U.N. Doc. CCPR/C/81/Add.4 (Aug. 24, 1994).

87. *See, e.g.*, U.N. Human Rights Comm., Lopez v. Uruguay, Comm. No. R.12/52, paras. 12.1–12.3, U.N. Doc. Supp. No. 40 (A/36/40) at 176 (1981); U.N. Human Rights Comm., Montero v. Uruguay, Comm. No. 106/1981, para. 5, U.N. Doc. CCPR/C/OP/2.

88. U.N. Human Rights. Comm., Summary Record of the 1405th Meeting, para. 20. U.N. Doc. CCPR/C/SR (Mar. 31, 1995).

(2) has real merit, and I will come to it momentarily. As already noted with regard to (3), there most certainly was no *clear* understanding among the drafters regarding the ICCPR's extraterritorial application—indeed there was little understanding of any kind. As for (1), it at least is manifestly wrong. Presumptions against the extraterritorial applications of *statutes* are creatures of domestic law; in the law of treaties the default rule in Article 29 of the VCLT is that a treaty applies to the state's entire territory, rather than merely parts thereof, but that default rule has nothing to say about extraterritorial application.[89]

In short, the 1995 U.S. statement before the Human Rights Committee was not the reiteration of some long-standing, consistently held position, but was made there and then, within the contemporary political context, particularly the 1994-1995 intervention in Haiti. Indeed, it was precisely with regard to Haiti that Theodor Meron wrote an influential 1995 piece in the *American Journal of International Law* on the extraterritoriality of human rights treaties, one of the earliest academic treatments of the topic.[90] The Clinton administration's position was inevitably informed by the practical difficulties the ICCPR could pose in its present and future foreign interventions, as was its similar position against the extraterritorial application of the Refugee Convention in the 1993 *Sale* case before the U.S. Supreme Court,[91] again with regard to the crisis in Haiti.[92]

Faced with the "global war on terror," the George W. Bush administration was happy to follow the Clinton administration's lead. Its consolidated second and third periodic report to the Human Rights Committee contained a somewhat more extended argument against the extraterritorial application of the Covenant.[93] While dropping argument (1) above regarding a supposed default presumption against extraterritoriality, the report again argued that the conjunctive language of Article 2(1) was clear and that the impossibility of the ICCPR's extraterritorial application was supported by the drafting history.

This rigid position was rejected by the Human Rights Committee in its case law[94] and in General Comment No. 31,[95] as well as by the ICJ[96] and

89. For an extended discussion see Marko Milanovic, *The Spatial Dimension: Treaties and Territory*, in Research Handbook on the Law of Treaties (Christian Tams et al. eds., forthcoming 2014), *available at* http://ssrn.com/abstract=2180597. *See also* Milanovic, *supra* note 46, at 9–11.

90. Theodor Meron, *Extraterritoriality of Human Rights Treaties*, 89 Am. J. Int'l L. 78 (1995).

91. Sale v. Haitian Ctrs. Council, 509 U.S. 155 (1993).

92. *See also* UNHCR, Advisory Opinion on the Extraterritorial Application of *Non-Refoulement* Obligations Under the 1951 Convention Relating to the Status of Refugees and its 1967 Protocol (Jan. 26, 2007), *available at* http://www.refworld.org/docid/45f17a1a4.html.

93. U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant: Third Periodic Report, Annex I, U.N. Doc. CCPR/C/USA/3 (Nov. 28, 2005).

94. *See, e.g.*, works cited in *supra* note 87.

95. *Supra* note 63, para. 10.

96. On the ICJ's case law on the extraterritorial application of human rights treaties, see generally Ralph Wilde, *Human Rights Beyond Borders at the World Court: The Significance of the International Court of*

most academic commentary.[97] But the Bush administration did not budge. The Obama administration, on the other hand, seemed to be somewhat more flexible. In its fourth periodic report to the Committee, the United States did *not* reaffirm its previous position, but merely noted that position and its rejection by the Committee and the ICJ:

> The United States in its prior appearances before the Committee has articulated the position that article 2(1) would apply only to individuals who were both within the territory of a State Party and within that State Party's jurisdiction. The United States is mindful that in General Comment 31 (2004) the Committee presented the view that "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 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." The United States is also aware of the jurisprudence of the International Court of Justice ("ICJ"), which has found the ICCPR "applicable in respect of acts done by a State in the exercise of its jurisdiction outside its own territory," as well as positions taken by other States Parties.[98]

The administration thus left open the possibility of modifying the previous categorical position. Anxious to accelerate this process, the Committee tried to press the administration further in its list of issues, but the administration remained coy in its response, merely referring the Committee back to the fourth U.S. report.[99]

We now know that the administration's coyness was due to internal disputes about the appropriateness of abandoning the categorical position. A week before the U.S. delegation was to present its fourth report to the Committee in March 2014, two internal memoranda written by Harold Koh, then the legal adviser to the State Department, were leaked to and published by the New York Times.[100] The first memo is on the extraterritorial applica-

*Justice's Jurisprudence on the Extraterritorial Application of International Human Rights Law Treaties*, 12 CHINESE J. INT'L L. 639 (2013).

97. *See, e.g.*, works cited in *supra* note 84.

98. U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant: Fourth Periodic Report, para. 505, U.N. Doc. CCPR/C/USA/4 (May 22, 2012).

99. *See* U.N. Human Rights Comm., List of Issues in Relation to the Fourth Periodic Report of the United States of America Adopted by the Committee at its 107th Session, para. 2., U.N. Doc. CCPR/C/USA/Q/4/Add.1 (Sept. 13, 2013).

100. *See* Charlie Savage, *U.S. Seems Unlikely to Accept That Rights Treaty Applies to Its Actions Abroad*, N.Y. TIMES, Mar. 7, 2014, at A6, *available at* http://www.nytimes.com/2014/03/07/world/us-seems-unlikely-to-accept-that-rights-treaty-applies-to-its-actions-abroad.html.

tion of the ICCPR and dates from 2010,[101] while the second is on the geographic scope of application of the Convention against Torture and dates from 2013.[102]

The first opinion, which is of most interest to us here, forcefully argues that the U.S. categorical opposition to the extraterritorial application of the ICCPR is fundamentally flawed and should be abandoned. In particular, Koh agrees with the critics of the U.S. position that the language of the ICCPR is not clear and is open to several possible interpretations,[103] and that reading that language to categorically disallow extraterritorial application would be contrary to the treaty's object and purpose.[104] Similarly, after conducting a thorough and extensive review of U.S. governmental materials, Koh confirms that the United States adopted the categorical position only in 1995 in the hearings before the Committee, where it was "first asserted in a conclusory fashion."[105]

However, despite the many strengths of his opinion, Koh was unable to persuade the other relevant stakeholders within the administration to change the position, since there were concerns that doing so might require significant alterations to existing U.S. policies, for example with regard to extraterritorial targeting or detention of suspected terrorists.[106] Whoever leaked the two memos to the New York Times did so precisely in order to undermine the credibility of the U.S. position as it was about to be reasserted in the hearings before the Committee.[107] And when the position was in fact reasserted, it was understandably met with considerable scepticism on the part of the Committee members.[108] In its concluding observations, the Committee thus expressed regret at the U.S. maintenance of its previous position, and recommended its reconsideration.[109]

---

101. U.S. Dep't of State, Office of the Legal Advisor, Memorandum Opinion on the Geographic Scope of the International Covenant on Civil and Political Rights (Oct. 19, 2010), *available at* http://justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf [hereinafter Koh ICCPR Opinion].

102. U.S. Dep't of State, Office of the Legal Advisor, Memorandum Opinion on the Geographic Scope of Application of the Convention Against Torture and Its Application in Situations of Armed Conflict (Jan. 21, 2013), *available at* http://justsecurity.org/wp-content/uploads/2014/03/state-department-cat-memo.pdf.

103. *See* Koh ICCPR Opinion, *supra* note 101, at 7–8.

104. *Id.* at 12–13.

105. *Id.* at 14; *see also id.* at 25–32.

106. *See* Savage, *supra* note 100.

107. *See* Marko Milanovic, *Harold Koh's Legal Opinions on the US Position on the Extraterritorial Application of Human Rights Treaties*, Just Security (Mar. 7, 2014, 5:09 PM), http://justsecurity.org/2014/03/07/harold-kohs-legal-opinions-position-extraterritorial-application-human-rights-treaties/.

108. *See* U.N. Human Rights Comm., *Human Rights Committee Considers Report of the United States* (Mar. 14, 2014), http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=14383&LangID=E.

109. *See* U.N. Human Rights Comm., Concluding Observations on the Fourth Report of the United States of America, advance unedited version, para. 4 (Mar. 26, 2014), *available at* http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf.

To conclude, the supposed consistency of the U.S. position on the ICCPR's extraterritorial application should not be overstated. Nor should we portray the U.S. position, which today is definitely in the minority internationally, as some kind of long-standing historical understanding of the Covenant that is today unjustifiably under threat from human rights and judicial activists, who are (yet again) trying to impose obligations on states without their consent. The U.S. position was contested from the moment it was articulated in 1995. What *is* true, as much as for the ECHR as for the ICCPR, is that until the 1990s very few people paid serious attention to the possibility of the extraterritorial application of human rights. This is not, I submit, because the states parties shared an *agreement* that the treaties do not apply outside their territories,[110] but rather because *culturally* the rights of others were largely beyond contemplation, especially during the Cold War. The process of human rights acculturation, through which the dignity and interests of others came to be seen as being worthy of protection, took its time. But while the extraterritorial application of human rights treaties, especially during armed conflict, may have been unthinkable for most of the treaties' lifetime, that is no longer the case today.[111]

### *C. The ICCPR's Text: Applying the Auschwitz Rule*

The U.S. position may well change in the future and embrace the current majority—whether this actually happens will depend on political developments that are difficult to predict. But what then of the text of Article 2(1) of the ICCPR and that annoying "and" in "all individuals within its territory and subject to its jurisdiction"? I should not be taken for arguing that the U.S. reading of the text is implausible—far from it, it probably is grammatically the most natural. But there are at least two more plausible readings of the text that would open the door to extraterritorial application: reading the "and" interchangeably with an "or," and reading the "within its territory and subject to its jurisdiction" limitation as being applicable only to the obligation to *ensure* human rights, but not to the obligation to *respect* them.

The second reading has not received much attention.[112] The first, however, was famously argued by Thomas Buergenthal in a classic 1981 arti-

110. Specifically, an agreement within the meaning of Art. 31(3)(a) VCLT, which would need to be taken into account when interpreting the treaty.

111. *See also* Milanovic, *supra* note 46, at 5.

112. *But see* John Cerone, *Jurisdiction and Power: The Intersection of Human Rights Law & the Law of Non-International Armed Conflict in an Extraterritorial Context*, 40 ISR. L. REV. 72, 124 (2007); Sarah H. Cleveland, *Embedded International Law and the Constitution Abroad*, 110 COLUM. L. REV. 225, 251–253 (2010); Rolf Künnemann, *Extraterritorial Application of the International Covenant on Economic, Social and Cultural Rights*, in EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES (Fons Coomans & Menno T. Kamminga, eds. 2004) 201, 227–29.

cle,[113] and was subsequently adopted by the Human Rights Committee in its General Comment No. 31, where it opined that states have the obligation "to respect and to ensure the Covenant rights to all persons who may be within their territory *and* to all persons subject to their jurisdiction."[114] The ICJ in the *Wall* case similarly thought that Article 2(1) could be interpreted both conjunctively and disjunctively, and preferred the latter option.[115]

One could object to this interpretation as being purely instrumental, but such an objection cannot be based on the supposed clarity of the text alone. Even in everyday usage "and" can be used interchangeably with "or" or to indicate both a conjunction and a disjunction. If I ask you whether you would like milk and sugar with your coffee, I am not only offering you *both* or *neither*. You will know that my "and" was really an "and/or" not from the grammatical context or the semantic meaning of the utterance, but from the *social context* in which it takes place, i.e. from the fact that plenty of people drink only milk or only sugar in their coffee, and not just both or neither, and that it is polite to offer all of these options to one's guests. Such ambiguities are not resolvable on the basis of grammatical interpretation alone.[116] Similarly, in legal usage, courts (and lawyers more generally) frequently read "and" and "or" interchangeably, depending on the context and their appraisal of the intent or purpose of the legislator which can operate at varying levels of specificity or generality.[117]

It is precisely this kind of interpretative exercise that we need to engage in to determine the effect of the "and" in Article 2(1) of the ICCPR. Indeed, article 31(1) of the VCLT requires us to interpret a treaty "in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose." At the very least this means that when we have several plausible readings of a text we should prefer the one that more accords with the treaty's object and purpose. And this is precisely where the universalist normative foundation of human rights comes in: an interpretation that values all human beings equally and

113. Thomas Buergenthal, *To Respect and to Ensure: State Obligations and Permissible Derogations*, in THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS (Louis Henkin ed. 1981).

114. General Comment No. 31, *supra* note 63, para. 10 (emphasis added).

115. Wall, *supra* note 83, paras. 108, 111 ("This provision can be interpreted as covering only individuals who are both present within a State's territory and subject to that State's jurisdiction. It can also be construed as covering both individuals present within a State's territory and those outside that territory but subject to that State's jurisdiction. . . . the Court considers that the International Covenant on Civil and Political Rights is applicable in respect of acts done by a State in the exercise of its jurisdiction outside its own territory.").

116. *See* Milanovic, *supra* note 46, at 223.

117. *See, e.g.*, United States v. Fisk, 70 U.S. 445, 447 (1865) ("[i]n the construction of statutes, it is the duty of the court to ascertain the clear intention of the legislature. In order to do this, courts are often compelled to construe 'or' as meaning 'and,' and again 'and' as meaning 'or'"); N.J. SINGER, 1A STATUTES AND STATUTORY CONSTRUCTION (6th ed., 2002), para. 21:14.

is respectful of their individual dignity is inherently more preferable than one that does not.[118]

Instead of looking at the object and purpose of the ICCPR at a general level one could also inquire into the *intentions of the parties* as to the specific problem of extraterritorial application. Put aside for a moment the fact that we are actually unable to determine this with much confidence from the *travaux*, or the methodological dubiousness of assuming what the text's drafters would have wanted if they were to decide a particular hypothetical problem. I am happy to concede that if we could today resurrect the drafters of the ICCPR and the ECHR, educate them about emails, the Internet, and smartphones, and ask them whether their treaties should apply to overseas espionage and mass surveillance programs of the kind run by the NSA and GCHQ, their answer would likely be no.

But the appeal of the argument that the representatives of the ICCPR's states parties could not possibly have agreed to outlaw foreign surveillance through the extraterritorial application of the right to privacy is only superficial. Like any presumptive intentionalist argument, it can be easily defeated. Surely these same drafters, crafting the Covenant largely in response to the horrors of the Second World War and the Holocaust, could not have intended to create a human rights treaty which would not be violated by the deliberate extermination of a million Jews in Auschwitz.[119] Make no mistake: this would indeed be the consequence of the absolutist position—that the ICCPR can *never* apply extraterritorially, not even to death camps in Nazi-occupied Poland.

In short, if one thinks that human rights treaties should be interpreted by establishing (or speculating on) how its drafters intended it or expected it to apply to *specific problems*, then one cannot escape what I will call the Auschwitz rule of interpretation: that in case there are two plausible interpretations of the text of a human rights treaty, one should favour that interpretation under which Auschwitz would be considered a human rights violation.

Whichever way one turns it, the position that the ICCPR should *never* apply extraterritorially seems untenable. It is rendered even more unpersuasive by not being supported by any normative theory as to why, exactly, human rights should categorically stop at the border (or I am yet to see one).[120] This is precisely why the U.S. government is finding its position increasingly difficult to sustain: it can offer nothing but a formalist invoca-

118. *See also* Wall, *supra* note 83, para. 109 ("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.").

119. *See* Milanovic, *supra* note 46, at 226.

120. This is not to deny that states may have concerns about the practical difficulties that they may face in applying human rights treaties beyond their borders. However legitimate these concerns might

tion of the text itself, regardless of its object and purpose, while pretending that the text allows no room for ambiguity.

In sum, the ICCPR must apply extraterritorially at least in some situations—the question is *when* and *how*. I will now look at the several possible models of extraterritorial application. In doing so, I argue that the rules and principles governing the application of the ICCPR and the ECHR should broadly be the same, despite the textual differences in the two jurisdiction clauses.

## III. Models of Extraterritorial Application

### A. Generally

This part will provide a brief outline of the (often conflicting and confusing) case law on the meaning of the concept of state jurisdiction in human rights treaties. I will first examine the spatial model of jurisdiction, which conceptualizes it as effective overall control of an area, then the personal model of jurisdiction as authority and control over individuals, and finally a third model that distinguishes between the positive and negative obligations of states under human rights treaties. Part IV will proceed to apply these models to several possible factual scenarios of overseas surveillance.

The European Court has produced by far the most case law on extraterritorial application, both in quantity and in variety. No case that I am aware of, however, in the European Court or elsewhere, deals directly with the question of extraterritorial application of human rights treaties to foreign searches, interceptions, or surveillance.[121] The issue is thus one of first impression. The jurisprudence of the Human Rights Committee on the extraterritorial application of the ICCPR, on the other hand, is not as conflicting or contradictory, even if it is less varied. The Committee has also tended to be more generous toward applicants than the European Court. Unless I am mistaken, there is not a single case in which the Committee rejected the communication of a person who made an arguable claim that his or her rights were violated extraterritorially, on the grounds that this person was not subject to the jurisdiction of the relevant state.[122]

---

be, they cannot warrant a categorical rule disallowing extraterritorial application. Rather, they should be taken into account when looking at the merits of any given case.

121. *But see infra* notes 189 and 192 and accompanying text.

122. The Committee's generosity can be explained, in my view, by the fact that it does not necessarily need to live with the consequences of an expansive approach in the same way as the Strasbourg Court, where the stakes are higher because of the greater robustness of the regime and the binding nature of the Court's decisions.

### *B. The Spatial Model*

The spatial model of jurisdiction as *de facto* effective control over areas is the least controversial. The European Court famously articulated it in the *Loizidou* case dealing with Northern Cyprus.[123] The Human Rights Committee similarly applied it to the occupation of the Palestinian territories by Israel,[124] and the ICJ likewise found the ICCPR to apply during occupation in the *Wall*[125] and *Congo v. Uganda* cases.[126] Under this model, an individual who is located in a territory under a state's *control* (but not necessarily its *sovereignty*) has human rights vis-à-vis that state. This approach makes intuitive sense: if a state exercises control over the territory of another state that in many respects replicates the extent of control that it has over its own territory, then it is only appropriate for it to have human rights obligations towards the territory's inhabitants. As the European Court held in *Loizidou*, what matters is the *fact* of such control, regardless of whether it was obtained lawfully or unlawfully (i.e. in violation of the territorial state's sovereignty).[127]

The benefit of this conception of jurisdiction is its clarity. There will always be difficult or borderline cases,[128] but the test itself is workable and provides some limits on states' obligations. But the test's benefit is also its

123. Loizidou v. Turkey (Judgment), App. No. 15318/89, 310 Eur. Ct. H.R. (ser. A), para. 62 (1995), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57920 ("Bearing in mind the object and purpose of the Convention, the responsibility of a Contracting Party may also arise when as a consequence of military action—whether lawful or unlawful—it exercises effective control of an area outside its national territory. The obligation to secure, in such an area, the rights and freedoms set out in the Convention, derives from the fact of such control whether it be exercised directly, through its armed forces, or through a subordinate local administration.").

124. *See* U.N. Human Rights Comm., 63d Sess., Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant: Concluding Observations: Israel, Jul. 15-28, 1998, para. 10, U.N. Doc. CCPR/C/79/Add.93 (Aug. 18, 1998) ("[T]he Covenant must be held applicable to the occupied territories and those areas . . . where Israel exercises effective control."); *see also* Comm. on Econ., Soc. & Cultural Rights, 19th Sess., Consideration of Reports Submitted by States Under Articles 16 and 17 of the Covenant: Concluding Observations: Israel, para. 8, U.N. Doc. E/C.12/1/Add.27 (Dec. 4, 1998) ("The Committee is of the view that the State's obligations under the Covenant apply to all territories and populations under its effective control."); Comm. on the Rights of the Child, 31st Sess., Consideration of Reports Submitted by States Parties Under Article 44 of the Convention: Concluding Observations: Israel, paras. 2, 5, 57–58, U.N. Doc. CRC/C/15/Add.195 (Oct. 4, 2002); Comm. Against Torture, 33d Sess., Consideration of Reports Submitted by States Parties Under Article 19 of the Convention: Conclusions and Recommendations: United Kingdom of Great Britain and Northern Ireland, Crown Dependencies and Overseas Territories, Nov. 15–26, 2004, para. 4(b), U.N. Doc. CAT/C/CR/33/3 (Dec. 10, 2004).

125. Wall, *supra* note 83.

126. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168 (Dec. 19).

127. For extended discussions of the spatial model, see, e.g., Ralph Wilde, *Triggering State Obligations Extraterritorially: The Spatial Test in Certain Human Rights Treaties*, 40 ISR. L. REV. 503 (2007).

128. *Cf.* Catan v. Moldova (Judgment), App. No. 43370/04, 2012 Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-114082; Ilascu v. Moldova (Judgment), App. No. 48787/99, 2004-VII Eur. Ct. H.R. para. 392, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61886 (speaking of a "decisive influence" of Russia over a separatist part of Moldova as sufficing for jurisdiction).

drawback, since the spatial model may be *too* limiting. There are many situations in which a state is factually perfectly capable of violating the rights of individuals *without* controlling the actual area. For example, the whole point of using drones for targeted killing is that the state does *not* need to have troops on the ground. Similarly, the "enhanced interrogation" of high-value Al-Qaeda detainees after 9/11 was conducted at CIA black sites in third states, such as Lithuania and Poland, where U.S. agents were using facilities provided to them by the territorial state.[129] The more such cases keep occurring (and there have been plenty), the more morally arbitrary it seems to condition the state's obligations on territorial control when such control is entirely irrelevant to the substance of the violation, and the more unsatisfactory and unappealing the spatial model becomes.

One way of dealing with this problem is to *shrink the size of the area* that is the object of the effective overall control test. Northern Cyprus is surely such an area. But why also not Guantanamo Bay, even though it is much smaller? There have been a number of cases applying the spatial model to ever decreasing areas or *places* such as a British military prison in Iraq,[130] or man-made objects such as ships and aircraft.[131]

Yet the more one shrinks the size of the area, the more artificial and arbitrary the whole test seems. For instance, should the application of human rights treaties really depend on whether state agents control the *house* in which an individual was shot to death, a possibility mooted during the litigation before the English courts in *Al-Skeini*?[132] The more the size of the area shrinks, the more likely it is that the spatial model collapses into a conception of jurisdiction as control over *individuals*, rather than spaces.

---

129. Cases are currently pending before the European Court against Poland for allowing or failing to prevent the human rights abuses in the "black sites." *See, e.g.*, Al Nashiri v. Poland (Judgment), App. No. 2876/11, Eur. Ct. H.R. (2014), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-146044; Husayn (Abu Zubaydah) v. Poland (Judgment), App. No. 7511/13, Eur. Ct. H.R. (2014), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-146047.

130. Al-Saadoon v. United Kingdom (Judgment), App. No. 61498/08, 2010 Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-97575.

131. *See, e.g.*, Jamaa v. Italy (Judgment), App. No. 27765/09, 2012 Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109231; Medvedyev v. France (Judgment), App. No. 3394/03, 2010 Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-97979; Öcalan v. Turkey (Judgment), App. No. 46221/99, 2005-IV Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-69022; Rigopoulos v. Spain (Decision), App. No. 37388/97, 1999-II Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-5625; Freda v. Italy (Decision), App. No. 8916/80, 21 Eur. Comm'n H.R. 254 (1980), *available at* http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-74311; *see also* J.H.A. v. Spain, Comm. Against Torture, 41st Sess., Nov. 3–21, 2008, U.N. Doc. CAT/C/41/D/323/2007 (Nov. 21, 2008), *available at* http://www.refworld.org/docid/4a939d542.html; Comm. Against Torture, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment: General Comment No. 2: Implementation of Article 2 by States Parties, UN Doc. CAT/C/GC/2 (Jan. 24, 2008), *available at* http://www.refworld.org/docid/47ac78ce2.html.

132. Al-Skeini v. Sec'y of State for Def., para. 110, [2005] EWCA (Civ) 1609, [2007] QB 140 (Eng.), *available at* http://www.bailii.org/ew/cases/EWCA/Civ/2005/1609.html (referring to this argument as "sophisticated"—but not in a good way).

### C. The Personal Model

The idea that the word "jurisdiction" in human rights treaties denotes authority and control exercised by states over individuals, rather than over territories or areas, also has a long pedigree. This jurisdiction was first set out by the European Commission in one of the early interstate cases between Cyprus and Turkey,[133] but its biggest proponent has been the Human Rights Committee. In *Lopez-Burgos*, a case dealing with an abduction by Uruguayan agents of an individual on Argentine territory, the Committee held that:

> The reference in article 1 of the Optional Protocol to "individuals subject to its jurisdiction" does not affect the above conclusion because the reference in that article is not to the place where the violation occurred, *but rather to the relationship between the individual and the State in relation to a violation of any of the rights set forth in the Covenant, wherever they occurred*. . . . Article 2 (1) of the Covenant places an obligation upon a State party to respect and to ensure rights "to all individuals within its territory and subject to its jurisdiction," but does not imply that the State party concerned cannot be held accountable for violations of rights under the Covenant which its agents commit upon the territory of another State, whether with the acquiescence of the Government of that State or in opposition to it. . . . In line with this, *it would be unconscionable* to so interpret the responsibility under article 2 of the Covenant as to permit a State party to perpetrate violations of the Covenant on the territory of another State, *which violations it could not perpetrate on its own territory*.[134]

Note how the Committee is essentially making an appeal to the universality of human rights in order to justify the personal model. The Committee reiterated this approach in General Comment No. 31, when it held 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 . . . regardless of the circumstances in which such power or effective control was obtained."[135]

So articulated, the principle is broad enough to make any human rights lawyer happy. But the benefit is again also a drawback, since it seems im-

133. Cyprus v. Turkey, App. Nos. 6780/74 & 6950/75, 2 Eur. Comm'n H.R. Dec. & Rep. 125, para. 8 (1975), *available at* http://hudoc.echr.coe.int/webservices/content/pdf/001-74811.

134. Lopez-Burgos, *supra* note 87, paras. 12.2–12.3 (emphasis added).

135. General Comment No. 31, *supra* note 63, at para. 10. For similar decisions from the Inter-American system, see Decision on Request for Precautionary Measures: Detainees at Guantanamo Bay, Inter-Am. Comm'n H.R., Cuba, 41 I.L.M. 532 (2002); Coard v. United States, Case 10.951, Inter-Am. Comm'n H.R., Report No. 109/99, para. 37 (1999); Alejandre v. Cuba, Case 11.589, Inter-Am. Comm'n H.R., Report No. 86/99, para. 23 (1999); Saldaño v. Argentina P, Inter-Am. Comm'n H.R., Report No. 38/99, para. 15–23 (1999).

possible to limit this principle in a non-arbitrary way. If depriving an individual of liberty would constitute "authority and control" or "power and effective control" over that person, why would depriving that person of life not also qualify as authority, power, and control?[136] Is there any meaningful difference between detaining a person and then killing him, and just killing him outright, be that by a missile fired from a drone, in a commando raid by troops on the ground—as with the killing of Osama bin Laden by U.S. forces in Pakistan—or simply by poison in his soup?[137] And if killing an individual is an exercise of power over him, as it surely must be, why would not the same apply to destroying their property, or reading his emails?

In other words, applying the personal model consequentially would lead to human rights treaties governing *any* extraterritorial state action. While that may not overly concern the Human Rights Committee (yet), it was precisely this kind of fear—of possible overreach, lack of institutional competence, and all sorts of practical and political difficulties on the merits—that in the immediate wake of 9/11 led the European Court to render its *Banković* inadmissibility decision. The case dealt with the destruction of a TV station in central Belgrade in a NATO airstrike during the 1999 Kosovo intervention.[138] The *Banković* Court not only held that the victims of aerial bombardment were not within the jurisdiction of the NATO states—since without troops on the ground they lacked effective control over the actual area despite controlling its airspace—but did so on methodologically dubi-

136. One potential argument for saying that physical custody qualifies as authority and control over an individual, whereas killing them does not, is that custody allows for a broad spectrum of possible violations of an individual's rights, i.e. that the control exercised over the individual is more comprehensive. But while it is undeniably true that custody enables the state to do many different things to the individual (other than just killing them outright), why should such plenary control be necessary for the individual to have human rights vis-à-vis that state? Consider only a scenario in which state X has a person in custody, but allows the agents of state Y to interrogate and torture that individual. State Y is only allowed to do to that individual what state X permits it to do, but is it also not true that, by torturing that individual, state Y is still exercising authority/power/control over that individual to the sufficient extent that it would have the obligation not to torture him? There seems to be no sound reason why it should *only* be state X that should have human rights obligations in such a scenario. We can of course replace torture in this scenario with any other possible human rights violation (e.g. killing) to demonstrate that limiting the authority and control principle to physical custody would be arbitrary. Compare, in that regard, the U.S. Supreme Court's consideration of the meaning of the word "seizure" in the Fourth Amendment, which it does *not* limit only to establishing custody over that individual, but extends also to the use of lethal force. *See* Tennessee v. Garner, 471 U.S. 1, 7 (1985) ("While it is not always clear just when minimal police interference becomes a seizure . . . there can be no question that apprehension by the use of deadly force is a seizure subject to the reasonableness requirement of the Fourth Amendment."). The Court was unanimous on this point, *see id.* at 25 (O'Connor, J., dissenting) ("For purposes of Fourth Amendment analysis, I agree with the Court that Officer Hymon 'seized' Garner by shooting him.").

137. Compare the case of Alexander Litvinenko, a former Russian spy killed in London in November 2006 by radioactive poisoning, ostensibly at the hands of Russian agents. His widow filed an application against Russia before the European Court, which is still pending. *See Strasbourg Court Sets Deadline for Russia on Litvinenko Case*, Ria Novosti (Dec. 15, 2010), http://en.ria.ru/world/20101215/161786652.html.

138. Banković v. Belgium (Decision), App. No. 52207/99, 2001-XII Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-22099.

ous grounds while studiously ignoring the personal model of jurisdiction. It moreover explicitly held that the extraterritorial application of the ECHR can only be *exceptional* and is an all-or-nothing proposition, as Convention rights could not be divided and tailored to suit the circumstances of the particular extraterritorial act in question.[139] The reference to the exceptional nature of extraterritorial application was not to the simple and incontestable fact that states will generally act far more frequently on their own territory than outside it. Rather, the Court meant to send a message that it will only rarely be prepared to accept claims originating in an extraterritorial context.[140]

As the criticism of *Banković* mounted,[141] as its arbitrariness got more and more exposed in a succession of smaller cases,[142] and as the composition of the Court itself changed, the Court decided to systematically revisit the question of extraterritorial application in the *Al-Skeini* case.[143] *Al-Skeini* was a complex litigation with six applicants, which started in British courts and dealt with the application of the ECHR to U.K. forces in occupied Iraq. Five of the applicants were killed by British troops on patrol, in varying circumstances. The sixth, Baha Mousa, was detained by British troops and beaten to death on the premises of a U.K. military prison. The applicants complained of a lack of an effective investigation into the deaths that would be compliant with Article 2 of the ECHR.

The House of Lords found that the five applicants killed on patrol were not within the United Kingdom's jurisdiction on the grounds that the spatial model of jurisdiction could not apply outside the ECHR's *espace juridique*, the combined territory over which the ECHR's states parties had sovereignty, or alternatively because the United Kingdom did not in fact have effective control over Basra under the spatial model because of the strength and intensity of the insurgency. Baha Mousa, on the other hand, was held to be within the United Kingdom's jurisdiction because of the

139. *Id.* at para. 75.

140. *See* Wilde, *supra* note 96, at 670.

141. *See, e.g.*, Olivier De Schutter, *Globalization and Jurisdiction: Lessons from the European Convention on Human Rights*, 6 BALTIC Y.B. INT'L L. 183 (2006); Alexander Orakhelashvili, *Restrictive Interpretation of Human Rights Treaties in the Recent Jurisprudence of the European Court of Human Rights*, 14 EUR. J. INT'L L. 529 (2003); Erik Roxstrom, Mark Gibney & Terje Einarsen, *The NATO Bombing Case (*Banković et al. v. Belgium et al.*) and the Limits of Western Human Rights Protection*, 23 B.U. INT'L L.J. 55 (2005).

142. *See, e.g.*, Pad v. Turkey (Decision), App. No. 60167/00, Eur. Ct. H.R. (2007), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=002-2605; Isaak v. Turkey (Decision), App. No. 44587/98, Eur. Ct. H.R. (2006), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-77533; Issa v. Turkey (Judgment), App. No. 31821/96, Eur. Ct. H.R. (2004), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-67460.

143. Al-Skeini v. United Kingdom (Judgment), App. No. 55721/07, 2011 Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105606. Notably, of the 17 judges who sat on the *Al-Skeini* Grand Chamber, only three sat on the *Banković* Grand Chamber—Costa, Rozakis, and Casadevall, whereas Judge Costa, presiding over the *Al-Skeini* Grand Chamber, had also presided over the 2004 *Issa* Chamber which openly contradicted *Banković* while directly invoking the language of the Human Rights Committee in Lopez-Burgos; *see also Issa*, App. No. 31821/96, Eur. Ct. H.R.

purported special status of a military prison in international law, akin to that of an embassy.[144]

The decision was criticized not only because of its dubious reasoning regarding a supposed analogy between prisons and embassies, but also because of its excessive rigidity and reliance on the *espace juridique* concept while largely rejecting the personal model of jurisdiction as inconsistent with *Banković*.[145] I have similarly argued that the decision is best explained not by looking at what the House of Lords said, but by understanding that the universalist imperative which served to protect Baha Mousa, a defenseless prisoner beaten to death by his captors, did not manage to outweigh the practical concerns that would be raised by investigations into the patrol killings during military operations.[146]

The applicants appealed to the European Court, which took the opportunity to repair some of the damage done by the often-arbitrary distinctions drawn in its own conflicting case law as well as by the British courts which had tried faithfully to apply it. The Court reaffirmed the validity both of the spatial model[147] and the personal model as "state agent authority,"[148] concluding with regard to the latter that

> [i]t is clear that, whenever the State through its agents exercises control and authority over an individual, and thus jurisdiction, the State is under an obligation under Article 1 to secure to that individual the rights and freedoms under Section 1 of the Convention that are relevant to the situation of that individual. In this sense, therefore, the Convention rights can be "divided and tailored" (compare *Banković*, cited above, § 75).[149]

The Court thus not only defined "jurisdiction" as state "control and authority over an individual," but it also partly overruled (or, in its words, "compared") *Banković* by allowing for the dividing and tailoring of Convention rights, as opposed to the all-or-nothing *Banković* approach. But the Court was still aware that if it defined jurisdiction in such terms, then the Convention would apply *everywhere*, as again there is no normatively sound, non-arbitrary way of concluding, for instance, that physical custody qualifies as "control and authority," while killing (or the ability to kill) does not. Indeed, the Court held that the five applicants killed by British troops on

144. Al-Skeini v. Sec'y of State for Def., [2007] UKHL 26, [2008] A.C. (H.L.) 153 (appeal taken from Eng.).

145. *See, e.g.*, Tobias Thienel, *The ECHR in Iraq: The Judgment of the House of Lords in* R (Al-Skeini) v. Secretary of State for Defence, 6 J. INT'L CRIM. JUST. 115, 115 (2008); Ralph Wilde, *The "Legal Space" or "Espace Juridique" of the European Convention on Human Rights: Is It Relevant to Extraterritorial State Action?*, 10 EUR. HUM. RTS. L. REV. 115 (2005); Lubell, *supra* note 84, at 214–15.

146. *See* MILANOVIC, *supra* note 46, at 116–17.

147. *Al-Skeini*, App. No. 55721/07, Eur. Ct. H.R. paras. 138–40.

148. *Id.*, paras. 133–37.

149. *Id.*, para. 137.

patrol in Basra were within the United Kingdom's jurisdiction precisely because the killing *was* with authority and control.[150] The Court hence felt compelled to find a limiting principle, and found one in the concept of "public powers" that it imported from the *Banković* analysis of the spatial model of jurisdiction—the killing of the applicants was thus an exercise of U.K. jurisdiction, but only because, due to the occupation of Iraq and relevant resolutions of the Security Council, the United Kingdom "assumed authority and responsibility for the maintenance of security in South East Iraq."[151]

In sum, *Al-Skeini* was a major attempt by the Court at fixing *Banković*, in which it was partly successful. But it would still not go all the way. In fact, it preserved the result of *Banković* and by using the nebulous concept of "public powers" managed to avoid the application of the ECHR to foreign military interventions *simpliciter*, as, for example, occurred recently in Libya. The use of drones in areas not under a state's control would likewise be outside the scope of the Convention per *Al-Skeini* and *Banković*. The uncertainties of *Al-Skeini* similarly left the door open for the United Kingdom to argue that it is confined to the specific facts of Iraq, and that the Convention largely does not apply to U.K. activities in Afghanistan.[152] The lines drawn by the judgment are better than those in *Banković*, but they remain arbitrary and uncertain—*Al-Skeini* will certainly not be the last word on the matter.[153]

### *D. A Third Model: Positive and Negative Obligations*

Just like the spatial model *in extremis* can collapse into the personal one, the more the area subject to jurisdiction shrinks in size, so does the personal model ultimately collapse, and the extraterritorial application of human rights treaties becomes limitless. The European Court's attempt to prop it up through the "public powers" concept may work for a while, but will increasingly be exposed as unstable.

I have hence argued in favor of a third model which would be based on the distinction between the overarching positive obligation of states to secure or ensure human rights, which extends even to preventing human rights violations by third parties, and the negative obligation of states to respect human rights, which only requires states to refrain from interfering

150. *Id.*, para. 149.

151. *Id.*, paras. 135, 149–50.

152. *See* Communication from the United Kingdom concerning the case of Al-Skeini and others against United Kingdom to the Committee of Ministers, (Council of Europe, DH–DD(2012)438 (May 2, 2012), *available at* https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2082643&SecMode=1&DocId=1885434&Usage=2 ("The UK considers that the Al Skeini judgment is set in the factual circumstances of UK's past operations in Iraq and that it has no implications for its current operations elsewhere, including in Afghanistan.").

153. *See* Marko Milanovic, Al-Skeini *and* Al-Jedda *in Strasbourg*, 23 EUR. J. INT'L L. 121 (2012) (analyzing *Al-Skeini* in detail).

with the rights of individuals without sufficient justification.[154] Under this model, "jurisdiction" would primarily mean effective overall control over areas, and the overarching positive obligation would be predicated on a state having such control over an area, because in the overwhelming majority of situations the state actually *needs* such control in order to be able to comply with this obligation.

On the other hand, the negative obligation to respect human rights would be territorially unlimited and not subject to any jurisdictional threshold, because any such threshold that was non-arbitrary would collapse anyway.[155] Textually, this would flow from Article 1 of the ECHR only referring to the obligation to *secure*, while Article 2(1) of the ICCPR could reasonably be read as attaching the jurisdiction threshold only to the obligation to *ensure*, but not the obligation to respect.[156] Alternatively, negative obligations could still be subject to the jurisdictional threshold under the personal model, but as we have seen this threshold actually collapses and the end result would be the same. The rationale for not limiting negative obligations is that states are *always* perfectly able to comply with them, since they remain in full control of their own organs and agents.[157]

The moral logic of universality is thus brought to its ultimate conclusion, while jurisdiction still serves as a limiting factor for the normally far more onerous positive obligations. I am not arguing that this model is perfect,[158] but I do claim that it is clear, predictable, precludes the vast majority of arbitrary outcomes, and provides a relatively stable balance between considerations of universality and effectiveness. Similarly, while I argue that this is how human rights treaties *should be* interpreted, I am not claiming that this is what human rights bodies or courts already are doing. Rather, I am saying that this model presents an equilibrium toward which the spatial and personal conceptions of jurisdiction will naturally tend to gravitate.

Having outlined these three models of jurisdiction, I will now proceed to apply them to several possible scenarios of overseas surveillance.

154. *See generally* MILANOVIC, *supra* note 46, at 209–22.

155. *Cf.* U.S. DEP'T OF STATE, *supra* note 101, at 4–5 (similarly relying on the distinction between the negative obligation to respect and the positive obligation to ensure human rights, but arguing that the obligation to respect should be limited to individuals subject to the authority and control of a state).

156. *See also supra* note 112.

157. *See* Van Schaack, *supra* note 84, at 49–52.

158. *See* Marko Milanovic, *Reply to Shany, Lowe and Papanicolopulu*, EJIL: TALK! (Dec. 5, 2011), http://www.ejiltalk.org/reply-to-shany-lowe-and-papanicolopulu/. *See also* Yuval Shany, *Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law*, 7 LAW & ETHICS HUM. RTS. 47 (2014).

## IV. Do Human Rights Treaties Apply to Extraterritorial Interferences with Privacy?

### A. Generally

The third model is the only one that provides easy, clear answers to whether human rights treaties apply to foreign surveillance. If the negative obligation to respect the right to privacy is territorially unlimited, then *any* interference with this right in *any* place in the world would implicate the ICCPR or the ECHR. This is not to say that such interferences, whether through a mass surveillance program or a targeted one, would necessarily be *illegal*. Rather, any such interference would need to be substantively *justified* within the analytical framework of human rights treaties (i.e. is the interference prescribed by law; does it serve a legitimate aim; is it proportionate to that aim). No threshold question of jurisdiction would arise, and just like with purely internal surveillance the analysis would need to be one on the merits. But again, this is also not to say that on the merits internal and external surveillance would need to be treated equally in every respect.[159]

The third model may provide a clear answer on the threshold question of applicability, but it is also one that is very broad and immediately leads to examination of the merits which carries with it its own uncertainties. This is precisely why the third model may not be appealing to those actors, be they governments, secret services, courts, or what have you, who would want to *avoid* the difficulties of a merits analysis or the constraints of human rights treaties altogether.

I will thus proceed to situate the following discussion within the confines of the more established spatial and personal models. But as soon as I do so, we will see how we run into uncertainty, complexity, and potential for arbitrariness. This is at least partly due to the fact that technological advances in obtaining information have rendered the exercise of manual, physical power over individuals unnecessary or at least less necessary. While privacy law in the information era frequently developed by analogy to old-school physical searches or interferences, whether in domestic systems (say under the Fourth Amendment to the U.S. Constitution)[160] or in international human rights law, there comes a point at which such analogies are no longer feasible or are outright misleading.

But such analogies can be a useful starting point.[161] I will now outline some scenarios of possible interferences with privacy through searches, inter-

159. *See infra* Part V.

160. *Cf.* United States v. Jones, 132 S. Ct. 949 (2012) (holding that attaching a GPS locator to a vehicle that enabled the movements of the vehicle to be tracked constituted a search under the Fourth Amendment, thus requiring a warrant); Kyllo v. United States, 533 U.S. 27 (2001) (holding that the use of an infrared thermal imaging device outside a house in order to detect lamps for growing marijuana within the house was a search for the purpose of the Fourth Amendment).

161. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005).

ception, or surveillance, starting with the more physical and ending with the most virtual. Under existing case law all of these actions by state agents against individuals could in principle count as interferences with their privacy rights under either the ECHR or the ICCPR if these actions were to occur on the state's own territory. The problem I want to address is *jurisdiction*: whether human rights treaties would apply in the first place if the state engaged in such conduct extraterritorially under either the spatial or the personal model, and whether distinctions should be made in terms of jurisdiction between the physical and the virtual methods of gathering information.

The scenarios include:

(1) Physical search of a person.
(2) Physical search of a person's property, or residence.
(3) Physical access to a person's computer system, phone, or an electronic telecommunications or data storage device.[162]
(4) Physical interference with a person's correspondence with another individual without the exercise of physical coercion against either individual (e.g. the opening and copying of a person's mail at the post office).[163]
(5) Audio-visual surveillance of a person.
(6) Audio-visual surveillance of a person's property or residence.
(7) Remote access to a person's computer system, phone, or electronic telecommunications or data storage device.[164]

---

162. Physically accessing a computer might at first glance seem a bit quaint. Note, however, that the most sensitive information held by governments and private enterprises is stored on computers not connected to the Internet, or to any internal network, precisely because of fears that such computers could be hacked and accessed remotely. Consider, in that regard, reports that the NSA has developed methods of accessing such "air-gapped" computers: "The technology, which the agency has used since at least 2008, relies on a covert channel of radio waves that can be transmitted from tiny circuit boards and USB cards inserted surreptitiously into the computers. In some cases, they are sent to a briefcase-size relay station that intelligence agencies can set up miles away from the target. . . . In most cases, the radio frequency hardware must be physically inserted by a spy, a manufacturer or an unwitting user." *See* David E. Sanger & Thom Shanker, *N.S.A. Devises Radio Pathway Into Computers,* N.Y. Times (Jan. 14, 2014), http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?hp&_r=0. The NSA's TAO unit is reported to be frequently deployed to the field, unlike most NSA operations, since its "ventures often require physical access to their targets." *Inside TAO: Documents Reveal Top NSA Hacking Unit*, Spiegel Online (Dec. 29, 2013, 9:18 AM), http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html; *see also* Jacob Appelbaum, Judith Horchert & Christian Stöcker, *Shopping for Spy Gear: Catalog Advertises NSA Toolbox*, Spiegel Online (Dec. 29, 2013, 9:19 AM), http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html (reporting on a variety of NSA hardware used to collect data from compromised computers, including rigged keyboards which log all keystrokes even without an Internet connection, and monitor cables which transmit images shown on the monitor).

163. Similarly, in a combination of scenarios (3) and (4), the NSA's Tailored Access Operations (TAO) unit is reported to engage in a program called "interdiction," which intercepts and diverts parcels of targeted parties, e.g. orders for new computers or accessories, in order to load malware onto them or install hardware components that would enable surveillance. *See Inside Tao*, *supra* note 162.

164. *See, e.g.*, *NSA Can Spy on Offline Computers Wirelessly, Says Security Expert*, CBS News (Dec. 30, 2013), http://www.cbsnews.com/news/nsa-can-spy-on-offline-computers-wirelessly-expert-jacob-apple-

(8) Interception of electronic communication midstream, without directly accessing the computer systems, phone, or other telecommunications devices of either the sender or the receiver.[165]
(9) Collection of metadata about the communication, rather than the content of the communication.
(10) Collection, storage, processing, transfer, and use of any other kind of personal data.[166]

Let us now try to apply the spatial and personal models of jurisdiction to some of these scenarios.

### *B. Spatial Model: Individual in an Area under the State's Control*

The application of the spatial model would be straightforward in principle. If an individual is located in an area under the state's control and the individual's privacy is interfered with by the agents of the state, the ICCPR and the ECHR would clearly apply. Thus, if Angela Merkel were in New York City visiting the United Nations, and a CIA agent searched her hotel room,[167] physically tampered with her phone or computer, or intercepted her communications remotely,[168] she would be subject to U.S. jurisdiction

baum-says/ (reporting inter alia on how malware uploaded onto an iPhone can allow remote access and turn it into a surveillance device); *Quantum Spying: GCHQ Used Fake LinkedIn Pages to Target Engineers,* SPIEGEL ONLINE (Nov. 11, 2013), http://www.spiegel.de/international/world/ghcq-targets-engineers-with-fake-linkedin-pages-a-932821.html (reporting on how the NSA and GCHQ can use fake LinkedIn pages to upload malware onto a target computer).

165. *See, e.g.*, *NSA Collects Millions of Text Messages Daily in "Untargeted" Global Sweep*, THE GUARDIAN (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (reporting on how the NSA's Dishfire program collects almost 200 million text messages daily from across the globe, and in addition to their contents extracts contacts, geolocational and financial information); Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (reporting on how the NSA's and GCHQ's joint MUSCULAR program allows them to collect at will content and metadata from hundreds of millions Google and Yahoo accounts).

166. The methods for acquiring such data are many and varied. *See, e.g.*, James Ball, *Angry Birds and "Leaky" Phone Apps Targeted by NSA and GCHQ for User Data*, THE GUARDIAN (Jan. 28, 2014, 2:51 PM), http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data (reporting on how vulnerable apps can be exploited to acquire personal data such as age, gender, ethnicity, location and sexual orientation, and quoting a leaked official document to the effect that "anyone using Google Maps on a smartphone is working in support of a GCHQ system").

167. It has been reported that GCHQ's "royal concierge" program is able to automatically identify and track potential hotel reservations for diplomats, so as to leave enough time to make the necessary technical preparations if the person in question is a valuable surveillance target so that the hotel room, its phone lines, and network can be bugged. *See* Laura Poitras, Marcel Rosenbach & Holger Stark, *"Royal Concierge": GCHQ Monitors Hotel Reservations to Track Diplomats*, SPIEGEL ONLINE (Nov. 17, 2013), http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html.

168. *See, e.g.*, Ewen MacAskill et al., *GCHQ Intercepted Foreign Politicians' Communications at G20 Summits*, THE GUARDIAN (June 17, 2013), http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits ("Foreign politicians and officials who took part in two G20 summit meetings in London in 2009 had their computers monitored and their phone calls intercepted on the instructions of their British government hosts, according to documents seen by the Guardian. Some

under the spatial model and her privacy would be protected by the ICCPR (again, this does not mean that the surveillance would necessarily be unlawful, but that it would have to be justified in order to be lawful). Note also that for the spatial model it is *control* over territory alone, and not *title* that matters—the result of this inquiry would be the same if Merkel were visiting Iraq while it was under U.S. occupation and the CIA did its business there.[169]

When in control of territory, states also have the positive obligation to secure or ensure human rights and protect individuals within their jurisdiction from human rights violations by third parties.[170] In the surveillance context this obligation would have two main components. First, states would need to regulate private companies operating in areas under control that collect, store, process, or have access to personal data.[171] This would include, but not necessarily be limited to, basic standards on data protection. Second, states would need to exercise due diligence and undertake all effective measures reasonably available to them to prevent interferences with privacy by third parties. If, for example, France knew that a third state was intercepting the communications of individuals living in France on a massive scale, and if such interferences were objectively unjustified under the framework of human rights law, France would need to implement such technological and other measures that are at its disposal to obstruct these interferences—for instance mandating the use of encryption when transmitting personal data.[172]

A more difficult problem arises if a state engages in surveillance of its own population and then provides the information it collected to a third party. The "Five Eyes" states share signals intelligence and the data they collect with one another, although the specifics are of course unclear.[173] The

delegates were tricked into using internet cafes which had been set up by British intelligence agencies to read their email traffic.").

169. *See generally* Loizidou v. Turkey (Judgment), App. No. 15318/89, 310 Eur. Ct. H.R. (ser. A) (1995); MILANOVIC, *supra* note 46, at 58–61.

170. *Cf.* G.A. Res. 68/167, *supra* note 16, para. 4; *supra* note 19 and accompanying text.

171. This is again a relatively straightforward application of the spatial model – what the regulation would entail in practice is of course a fact-specific question for the merits. A more difficult problem in jurisdictional terms is whether states would have such positive obligations toward individuals whose *data* is stored or processed in a facility located in a territory under the state's control, but the individual himself is not. That scenario would not seem to be covered by the spatial model, which requires individuals to be within areas under the state's jurisdiction.

172. *See* Anne Peters, *Surveillance without Borders: The Unlawfulness of the NSA Panopticon, Part II*, EJIL: TALK! (Nov. 4, 2013), http://www.ejiltalk.org/surveillance-without-borders-the-unlawfulness-of-the-nsa-panopticon-part-ii//.

173. *See, e.g.*, Scott Shane, *No Morsel Too Minuscule for All-Consuming N.S.A.,* N.Y. TIMES (Nov. 2, 2013), http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html?pagewanted=4&_r=0 ("For decades, the N.S.A. has shared eavesdropping duties with the rest of the so-called Five Eyes, the Sigint agencies of Britain, Canada, Australia and New Zealand. More limited cooperation occurs with many more countries, including formal arrangements called Nine Eyes and 14 Eyes and Nacsi, an alliance of the agencies of 26 NATO countries."); Arne Halvorsen et al., *Norway's Secret Surveillance of Russian Politics for the NSA*, DAGBLADET (Dec. 17, 2013), http://www.dagbladet.no/2013/12/17/nyheter/samfunn/politikk/utenriks/overvaking/30877258/.

individuals concerned could be within the jurisdiction of the collecting/sending state, but not necessarily under the jurisdiction of the receiving state, at least not under the spatial model. Various other complicity scenarios are possible,[174] but they introduce further legal and factual complexities that I am not able to explore in this article, other than by saying that such scenarios can implicate both the secondary rules of state responsibility under general international law[175] and specific primary rules of international human rights law which may set limits on information-sharing.[176]

### *C. Spatial Model: Interference in an Area Under the State's Control*

New technologies can today frequently lead to a disconnect between the location of the *individual* and the location of the *interference* with the individual's privacy.[177] For example, while sitting in her office in Berlin, Angela Merkel can send an email to somebody in Australia but the communication itself can be routed through a server in the United Kingdom and intercepted there by the U.K. authorities. Merkel is thus located in Germany, but the actual interference with her privacy takes place in the United Kingdom.

The question is how to determine state jurisdiction in situations in which the interference was done in an area under a state's control, but the individual is not in any such area. Should we look at such cases under the spatial model, on the basis of the location of the interference, or under the personal model, by seeing whether the interception as such qualifies as an exercise of authority and control over the individual?

At a textual and conceptual level I am skeptical that the spatial model could be applied on the basis of the location of the interference alone. If the

174. *See, e.g.*, James Ball, *US and UK Struck Secret Deal to Allow NSA to "Unmask" Britons' Personal Data*, THE GUARDIAN (Nov. 20, 2013), http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data (reporting on the UK allowing the US to "unmask" the personal data of UK residents that was collected by the NSA, but was previously subject to minimization procedures); Ewen MacAskill, James Ball & Katharine Murphy, *Revealed: Australian Spy Agency Offered to Share Data About Ordinary Citizens*, THE GUARDIAN (Dec. 2, 2013), http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens (reporting on Australia sharing un-minimized personal data of ordinary Australians with the NSA); Greg Weston, Glenn Greenwald & Ryan Gallagher, *New Snowden Docs Show U.S. Spied During G20 in Toronto*, CBC NEWS (Nov. 27, 2013), http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448 (reporting on Canada allowing the United States to conduct surveillance operations on its territory during a G20 summit in Toronto).

175. *See* Int'l Law Comm'n, 53d Sess., *Responsibility of States for Internationally Wrongful Acts*, Article 16, U.N. Doc. A/56/49; GAOR, 56th Sess. (2001).

176. For example, by saying that states have a territorially unlimited negative obligation to refrain from conduct that would assist third parties in violating the right to privacy, e.g. by analogy to the *non-refoulement* rule in cases such as *Soering v. United Kingdom* (Judgment), App. No. 14038/88, 161 Eur. Ct. H.R. (ser. A) (1989), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57619, or *Judge v. Canada*, U.N. Human Rights Comm., Comm'cn No. 829/1998, U.N. Doc. CCPR/C/78/D/829/1998 (2003).

177. *See* Carly Nast, *Interference-Based Jurisdiction Over Violations of the Right to Privacy*, EJIL: TALK! (Nov. 21, 2013), http://www.ejiltalk.org/interference-based-jurisdiction-over-violations-of-the-right-to-privacy/.

inquiry is whether the individual is within or subject to a state's jurisdiction, and if "jurisdiction" means an area under the state's effective control, it is hard to see why the location of the interference should matter.[178] But our *intuitions*, on the other hand, do seem to favour the application of human rights treaties in such circumstances. For example, I normally live and work in the United Kingdom, but I travel relatively frequently. If the U.K. police searched my flat in Nottingham or if they hacked into my office computer while I was out of the country, *surely* the ICCPR and the ECHR would apply and my privacy rights would be engaged? If they seized my U.K. bank account while I was outside the United Kingdom, *surely* my property rights under Protocol No. 1 to the ECHR would be engaged? And so forth.

There have been plenty of cases before the European Court or the Human Rights Committee with such an extraterritorial element in which everyone, including the respondent state, simply took for granted that the treaty applied.[179] Nobody ever doubted, for instance, that Article 6 of the ECHR fair trial rights applied to a person who was tried *in absentia* but who *absconded to another state's territory* while the trial went on.[180] The Court similarly found Article 6 to apply to civil proceedings brought in Italy by claimants living in Serbia for damages arising from the destruction of the same Belgrade TV station that was at issue in *Bankovic*.[181] Indeed, it would seem manifestly arbitrary for the Convention not to apply. If that is so, why should privacy rights be any different? The question, then, is *what theory* covers these kinds of situations.

The first option is to treat such situations under the spatial model, but as I have explained above, that is problematic because the focus of that model is on the location of the individual rather than on the location of the interference. The second is to examine them under the personal model. But if we accept that, for example, I am an individual under the "authority and control" of the United Kingdom when U.K. agents search my flat in Nottingham even when I am outside the country, I do not see how we could deny

178. *See* MILANOVIC, *supra* note 46, at 7–8.

179. *See, e.g.,* Gueye v. France, U.N. Human Rights Comm., Commc'n No. 196/1985, U.N. Doc. CCPR/C/35/D/196/1985 (Apr. 6, 1989) (Art. 26 ICCPR applied to former French Army servicemen of Senegalese nationality residing in Senegal, whose French pensions were reduced solely on grounds of nationality); Bosphorus v. Ireland (Judgment), App. No. 45036/98, 2005-VI Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-69564 (Convention applies to the impounding of an aircraft in Ireland that was leased by a company incorporated in Turkey); Mullai v. Albania (Judgment), App. No. 9074/07, Eur. Ct. H.R. (2012), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-107030 (property rights under the Convention regarding a building permit dispute in Albania, even though some of the applicants were not physically located in Albania); Vrbica v. Croatia (Judgment), App. No. 32540/05, Eur. Ct. H.R. (2010), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-98057 (applicant's fair trial rights were engaged regarding the recognition and enforcement of a judgment by a Montenegrin court in Croatia, even though he never lived in Croatia).

180. *See* Sejdovic v. Italy (Judgment), App. No. 56581/00, 2006-II Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-72629.

181. *See* Markovic v. Italy (Judgment), App. No. 1398/03, 2006-XIV Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-78623.

that I would also be under the authority and control of the United Kingdom if U.K. agents surreptitiously searched my flat in Belgrade, Serbia. Similarly, if the ECHR would apply to a search of my desktop computer in the United Kingdom even while I am in Serbia, because in performing this search the U.K. government is exercising authority and control over me, then I do not see why the ECHR would not apply to a similar search of my laptop by U.K. agents operating in Serbia, whether lawfully or unlawfully. In other words, the location of both the individual and the interference seems to be irrelevant under the logic of the personal model.

A third option would be to say that what we have here are territorial *acts* producing extraterritorial *effects*, a line of thinking going back to the Strasbourg *Drozd and Janousek* case.[182] But that is not, in my view, a sound way of conceptualizing the application of human rights treaties since in every case one can draw some kind of causal link between a territorial act (e.g. the decision to bomb Serbia in 1999 made by NATO governments in their own territories) and extraterritorial consequences (e.g. the bombing itself). The European Court for its parts sees *Drozd* in the context of the personal model only.[183] Moreover in cases of surveillance the possible violation of privacy is entirely consummated by the act of surveillance itself, whether it takes place in an area under the state's sovereignty, control, or beyond its control. My own preferred solution to such cases is hence the third model of jurisdiction that distinguishes between positive and negative obligations. The reason why the Convention would apply is because it should apply to *all* potential violations of negative obligations, e.g. the one to refrain from interfering with my privacy.

Whatever theory one chooses, surveillance programs in which the interference with privacy takes place within an area under the state's control, even though the individual is not located in this area, may be more open to challenge than those programs in which both the interference and the individual are outside areas controlled by the state. For example, GCHQ's massive Tempora program taps transatlantic fibre-optic cables as they pass *through the United Kingdom* or its territorial sea and obtains enormous amounts of data.[184] The interference hence takes place within the United Kingdom even though the person whose communication is intercepted is located outside it. And even if the interception of communication or the collection of personal data does *not* take place in an area under the state's

182. *See* Drozd v. France (Judgment), App. No. 12747/87, 240 Eur. Ct. H.R. (ser. A), para. 91 (1992), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57774 (holding that "[t]he term 'jurisdiction' is not limited to the national territory of the High Contracting Parties; their responsibility can be involved because of acts of their authorities producing effects outside their own territory").

183. *See* Al-Skeini v. United Kingdom (Judgment), App. No. 55721/07, 2011 Eur. Ct. H.R. paras. 133, 135.

184. *See* Ewn MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, The Guardian (June 21, 2013), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

control, its subsequent storage, processing and use—all of which would constitute separate, fresh interferences with privacy—may well take place within such an area.[185] Similarly, Australia is reported to have been using its *embassies* in a number of countries to intercept calls and data, equipping them with surveillance collection facilities, as part of the STATEROOM program of using diplomatic missions of the "Five Eyes" states.[186] The United States has also routinely used its embassies and overseas military bases for electronic surveillance.[187] Recall, in that regard, the possibility of shrinking the spatial model of jurisdiction to cover smaller areas or places, as in *Al-Saadoon*, including embassies and military bases.[188]

Notably, at least two surveillance/data collection cases before the European Court dealt with situations in which the interference was territorial while the individual was outside any area under the state's control. In the first, *Weber and Saravia v. Germany*,[189] the applicants lived in Uruguay while their communication was allegedly intercepted in Germany. Germany actually even objected that the case was outside its jurisdiction under *Bankovic*,[190] but the Court avoided the matter and dismissed the case as manifestly ill-founded on the merits.[191] In the second, *Liberty and Others v. the United Kingdom*,[192] two of the applicants were Irish organizations that communicated with a British one, and their communication was allegedly intercepted in the United Kingdom. Neither the U.K. government nor the Court *proprio motu* considered that an Article 1 jurisdiction issue arose with respect to the Irish applicants—that is, they both assumed that the ECHR applied, and the Court went on to find a violation of Article 8.

### *D. Personal Model*

The most problematic situation of surveillance is one where both the individual and the interference with their privacy take place in an area outside the state's control. Unless we opt for the third model which distinguishes between positive and negative obligations, we will have to look at such cases through the personal model of jurisdiction. We have seen how the case law

185. *See* discussion *infra* Part V for what constitutes an interference with privacy.

186. *See Australia Accused of Using Embassies to Spy on Neighbours*, THE GUARDIAN (Oct. 30, 2013), http://www.theguardian.com/world/2013/oct/31/australia-accused-embassies-spy-neighbours.

187. *See, e.g.*, *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, SPIEGEL ONLINE (Oct. 27, 2013), http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (reporting on the use by NSA Special Collection Service operatives of US embassies and consulates in Berlin, Paris, Madrid, Rome, Prague and Geneva); *Inside TAO*, *supra* note 162 (reporting on the use of a US military base in Darmstadt).

188. *See* Al-Saadoon v. United Kingdom (Judgment), App. No. 61498/08, 2010 Eur. Ct. H.R.

189. Weber v. Germany (Decision), App. No. 54934/00, 2006-XI Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-76586.

190. *Id.*

191. *Id.*

192. Liberty v. United Kingdom (Judgment), App. No. 58243/00, Eur. Ct. H.R. (2008), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87207.

of the European Court and the Human Rights Committee defines such jurisdiction in similar terms, as "authority and control" or "power and effective control" over individuals. The question is what exactly qualifies as such authority, power, or control, and how these criteria would apply to overseas surveillance. As a thought experiment, consider the following scenarios, all of which for the sake of the argument take place in Berlin and involve a hypothetical Angela Merkel:

(1) A CIA agent grabs Angela Merkel, disables her escort (assume he is some kind of judo master), and then physically searches her for items in her possession.
(2) A CIA agent breaks into and searches Angela's apartment and plants cameras and listening devices.
(3) A CIA agent manages to get Angela's phone when she is not looking, and furtively plants a tracking device in it.
(4) A CIA agent breaks into Angela's office and hacks into her computer, uploading a virus and downloading sensitive data.
(5) A CIA agent observes and listens to Angela using a high-resolution camera/directed mike.
(6) A CIA agent observes and monitors Angela's residence from the outside using a high-resolution camera/directed mike, without necessarily observing Angela herself.
(7) A CIA agent hacks Angela's phone or computer remotely.
(8) A CIA agent intercepts Angela's calls, texts, or emails midstream.
(9) A CIA agent is able to collect information about whom Angela calls, when, for how long (telephony metadata) or whom and when she emails (internet metadata).
(10) The NSA obtains Angela's personal information from its partners in GCHQ, and proceeds to store and process that information.

Which of these scenarios qualify as an exercise of authority, power, or control over Angela? As I explained before, the personal model of jurisdiction is prone to collapse (and that may be either a bug or a feature, depending on your point of view). It is very difficult to draw lines that are not arbitrary. Indeed, some lines clearly would be arbitrary, for instance if we said that in any of these scenarios Angela would be under U.S. jurisdiction but *only* if she was a U.S. citizen.[193]

193. *See supra* Part I; *see also* Coard v. United States, Case 10.951, Inter-Am. Comm'n H.R., Report No. 109/99, OEA/Ser.L/V/II.106, para. 37 (1999) ("Given that individual rights inhere simply by virtue of a person's humanity, each American State is obliged to uphold the protected rights of any person subject to its jurisdiction. While this most commonly refers to persons within a state's territory, it may, under given circumstances, refer to conduct with an extraterritorial locus where the person concerned is present in the territory of one state, but subject to the control of another state—usually through the acts of the latter's agents abroad. In principle, *the inquiry turns not on the presumed victim's nationality or presence within a particular geographic area*, but on whether, under the specific circumstances, the State observed the rights of a person subject to its authority and control.") (emphasis added).

Of these ten scenarios, only (1) involves the exercise of physical power against Angela herself in the sense of an agent handling her bodily. (2)-(4) all involve the exercise of physical power, but against Angela's property rather than her person. (5) and (6) are physical but non-corporeal, as it were. (7)-(10) are entirely virtual or digital.[194]

I see no legitimate way of drawing lines here. Scenario (1) surely must qualify as an exercise of power, authority or control over Angela, who is held and searched against her will by a state agent. But if (1) equals jurisdiction, then why not (2)-(4), et cetera? In particular, if virtual methods can in principle accomplish the exact same result as physical ones, then there seems to be no valid reason to treat them differently and insist on some kind of direct corporeal intervention.[195] Therefore, unless one is willing to knowingly draw lines that are arbitrary and by very their nature invite evasion and abuse, for instance, by requiring such direct physical intervention or by using a nebulous and undefined criterion such as the *Bankovic/Al-Skeini* concept of "public powers," the personal model would again seem to collapse and all cases of overseas surveillance by a state would be within the state's jurisdiction. The end result would ultimately be no different than if we applied my third model from the outset and dispensed with any jurisdictional inquiry with regard to possible violations of states' negative obligations.

In sum, I submit that human rights treaties apply to most, if not all, foreign surveillance activities. This would certainly be the case under the third model of jurisdiction, and would equally be true of the personal model if it is applied consistently and coherently. But the European Court may well decide to draw an arbitrary line somewhere, especially because whatever it decides in the context of extraterritorial privacy violations will necessarily have ramifications for other controversial issues, such as targeted killings (e.g. there seems no way of saying that reading Angela's email is an exercise of power, authority, and control over her, but that killing her is not). Even though I have argued what the Court *should* do, it is impossible to predict what the Court *will* in fact do, except to say that it is more likely to find interferences with privacy that occur within a territory controlled by the state (e.g. the GCHQ Tempora program) to be covered by the Convention. The Human Rights Committee's track record, on the other hand, suggests that it will be more generous than the European Court, even if its views may prove to have less of an impact. From an advocacy standpoint, clear statements by the Committee and the U.N. special rapporteurs with relevant mandates to the effect that human rights treaties apply to extraterritorial surveillance will make it more likely for the European Court (or the U.K.

194. Note that all of these methods are physical in a wider sense—the transmission and sensation of images via photons, or of sounds via vibrations of particles in the air, or of information via electrons are physical phenomena no less than the interaction between the atoms of the CIA agent's hands and those of Merkel's body.

195. *See* Margulies, *supra* note 84, at 11–13 (arguing for a concept of virtual control).

Supreme Court or the highest court of some other party in which human rights treaties are directly applicable, or even the ICJ if a pertinent case were to come before it) to find such an approach palatable.

I will now look at what the right to privacy might mean in the extraterritorial surveillance context, assuming that the ICCPR and the ECHR apply.

## V. The Substance of an Extraterritorial Right to Privacy

### *A. Between Utopia and Apology, Universality and Effectiveness*

Until now I have only addressed the threshold question of whether individuals subject to surveillance overseas should be entitled to human rights in the first place. This part of the article will deal with the *substance* of the right to privacy in this context, if the right is found to apply. Though my main focus has been on the threshold question of extraterritorial application, and though that question is conceptually distinct from the substantive content of any given right, there is a direct connection as a matter of policy between the inquiries on jurisdiction and on the merits. The more difficult, complex, or politically controversial the merits question of whether the substantive right has been violated, the greater the temptation to say that the right simply does not apply. Courts in particular frequently resort to dismissing cases *in limine* even while furtively casting an eye on the merits, in order to avoid grappling with the merits openly. One cannot really reduce arbitrariness in resolving threshold questions without looking at what the consequences of doing so would be down the line.

I have argued in that regard that the case law on the extraterritorial application of human rights treaties, particularly that of the European Court, straddles a Koskenniemian divide between universality and effectiveness.[196] On one hand we want to follow the moral logic of universality, protect human beings no matter where they are located on the basis of their inherent dignity, and just do the *right thing*. On the other, we see the enormous practical and political difficulties of doing so, that doing the right thing often comes at a cost, and that complying with universality could require a radical departure from the status quo. An expansive approach to extraterritoriality can thus be criticized as utopian, as presenting a normative vision which has nothing to do with the real world, whereas a restrictive approach can be dismissed as pure apology for unbridled, arbitrary, and limitless exercise of state power which we would never accept domestically.

A persuasive argument regarding the threshold of extraterritorial application hence must also look at the substance and attempt to strike a better balance between universality and effectiveness. It must provide states and courts with sufficient *flexibility* in the extraterritorial context and not impose

196. *See* Milanovic, *supra* note 46, at 106–17 (relying on Martti Koskenniemi, From Apology to Utopia: The Structure of International Legal Argument (2005)).

unrealistic burdens and restrictions with which they could never comply. Resistance to extraterritorial application flows in large part from the fact that most human rights case law was built in times of normalcy, and the fear that applying this case law to external situations would be rigid and inflexible. It is this fear that leads to categorical rejections of the possibility that human rights treaties can apply extraterritorially, or to the drawing of arbitrary lines on threshold jurisdictional issues. However, while real, this fear is overstated. Most human rights, including privacy, analytically employ balancing tests that can be used less strictly if this is objectively justified by the circumstances—but such a justification must be made out and evaluated on its merits.[197]

Compare, in that regard, the inherent malleability of balancing tests with the U.S. Fourth Amendment's categorical warrant requirement for searches and seizures. While the European Court has interpreted the notions of "private life" and "correspondence" that are protected by the Convention very generously, thereby increasing the scope of acts that can constitute an interference with privacy,[198] the U.S. Supreme Court has at times interpreted the concept of a search or seizure quite narrowly, because this was the only way of avoiding what appeared as an inflexible, overly rigid requirement for a specific search warrant on probable cause.[199] In other words, the scope of the right to privacy under the ECHR (and arguably the ICCPR) is wider than the current state of the U.S. Supreme Court doctrine on "reasonable expectations of privacy."[200] For instance, while the Supreme Court held in *Smith v. Maryland* that individuals had no reasonable expectation of privacy in telephony metadata,[201] such metadata would be within the scope of the human right to privacy, even if collecting this metadata would not necessarily require a warrant.[202]

197. *See* MILANOVIC, *supra* note 46, at 110–13.

198. *See, e.g.*, Shimovolos v. Russai (Judgment), App. No. 30194/09, Eur. Ct. H.R. para. 64 (2011), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105217 ("The Court reiterates that private life is a broad term not susceptible to exhaustive definition. Article 8 is not limited to the protection of an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world. Private life may even include activities of a professional or business nature. . . . There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life.'") (citing relevant case law).

199. *See* Elisabet Fura & Mark Klamberg, *The Chilling Effect of Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA, in* FREEDOM OF EXPRESSION – ESSAYS IN HONOUR OF NICOLAS BRATZA 463 (Josep Casadevall et al., eds., 2012).

200. The test for what constitutes a search in a constitutionally protected context, originating in Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). *See generally* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007) (discussing the inability of the Supreme Court to provide a single, consistent answer on the nature of a search under the Fourth Amendment).

201. Smith v. Maryland, 442 U.S. 735 (1979).

202. *See* Malone v. United Kingdom (Judgment), App. No. 8691/79, 82 Eur. Ct. H.R. (ser. A), para. 84 (1984), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-5753 ("As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone

The human rights framework is hence inherently flexible when it comes to justifying interferences with privacy, while simultaneously being very inclusive on what constitutes such interference.[203] But even though the human rights framework can and could be applied even *more* flexibly in the external context, it must not be applied *so* flexibly that it ceases to have any *impact* or compromises the *integrity* of the whole regime.[204] By impact I mean that there would be no point in applying human rights extraterritorially if they brought nothing new to the table, if they made no difference whatsoever and did not in any way challenge the status quo. On the contrary, watering down the substantive requirements of human rights too much in the external as opposed to the internal context would only serve to *legitimize* the status quo, and thereby enhance the apology critique. In that sense, while governments run the risk that their current arrangements in conducting foreign surveillance would be deemed to be unjustified within the human rights framework, privacy activists also run the risk that these arrangements—perhaps with some minor changes here or there—would actually be found to be acceptable within that very same framework, especially if the relevant courts or treaty bodies conducted their review very deferentially.[205]

Finally, we must produce rules that are reasonably *clear and predictable*, both with regard to the threshold question of applicability and with regard to the merits. This is precisely what I have tried to do with my third model of jurisdiction when it comes to applicability, while the merits inquiry is necessarily more fact-specific and can be outlined in the abstract only in very broad strokes, which I will now (quite briefly) do.

---

service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8).”). The Court went on to hold that the interference constituted a violation of Article 8 because it was not “in accordance with the law” in the sense of Article 8(2). *Id.*, paras. 86–88.

203. Note that two U.S. Courts of Appeals have tried to avoid the rigidity of the Fourth Amendment’s warrant requirement by holding that in an extraterritorial context even a citizen would only be entitled to a reduced, core reasonableness protection under the Fourth Amendment, which would (like human rights law) not necessarily require a warrant. *See* United States v. Stokes, 726 F.3d 880 (7th Cir. 2013); *In re* Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157, 171 (2d Cir. 2008).

204. *See* MILANOVIC, *supra* note 46, at 113–15.

205. *See also* Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 434 (2008) (arguing that in the U.S. context there are systemic problems in applying balancing tests so that the importance of security interests is inflated while the value of liberty interests is diminished, and that the lack of transparency about data mining programs compromises any balancing exercise regarding their justifiability).

### B. Privacy and Surveillance within the Human Rights Framework

At this point we should recall some of the textual differences between the ICCPR and the ECHR with respect to the right to privacy. Article 17 of the ICCPR prohibits "arbitrary or unlawful" interferences with privacy or correspondence, while under Article 8 of the ECHR interferences with privacy or correspondence can only be justified if they are "in accordance with the law" and "necessary in a democratic society" for the achievement of the legitimate goals specified therein, such as national security. Both provisions are vague, broad in scope, and require interpretation. The words "unlawful" and "in accordance with the law" refer to the legality of the interference, e.g. surveillance measures, under the relevant state's own domestic law. The "arbitrary" standard in the ICCPR, on the other hand, at least *prima facie* appears more lenient than the "necessary in a democratic society" ECHR standard.

But the Human Rights Committee has never read "arbitrary" in Article 17 or other provisions of the Covenant that use it by its purely discretionary meaning,[206] as referring to unrestrained decisions made purely by discretion or on whim, without any rational reason—a standard so low that it could be satisfied by having almost any rule allowing for the interference.[207] Nor has the European Court read "necessary in a democratic society" to require *absolute* necessity in the sense of always requiring the exhaustion of all possible, less intrusive means capable of achieving the same end, since that would put an unreasonable burden on states which are in most situations faced with many alternatives and trade-offs and the choice between them is subject to the political process.[208] Rather, both bodies have adopted a virtually identical analytical approach in assessing whether there has been a violation of the right to privacy, in a four-part test:

(1) Has there been an interference with privacy or correspondence?
(2) If so, was the interference lawful/in accordance with the law?
(3) If so, did the interference pursue a legitimate aim?
(4) If so, was it proportionate to that aim?

206. *See* ICCPR, art. 6.1, 9.1, 12.4.

207. *See* U.N. Human Rights Comm., General Comment No. 16: Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, UN Doc. HRI/GEN/1/Rev.1 at 21 (1994) [hereinafter *General Comment No. 16*]; *see also* Donoso v. Panamá (Judgment), Inter-Am. Ct. H.R., para. 56 (Jan. 27, 2009), available at http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_ing.pdf (holding that "right to privacy is not an absolute one, and, so, it may be restricted by the States provided that their interference is not abusive or arbitrary; accordingly, such restriction must be statutorily enacted, serve a legitimate purpose, and meet the requirements of suitability, necessity, and proportionality which render it necessary in a democratic society").

208. Such absolute necessity is used only in the context of Article 2 of the ECHR and deprivation of life. This has similarly been the approach of the Human Rights Committee, even though Article 6(1) of the ICCPR also prohibits only *arbitrary* deprivations of the right to life—the intensity of the proportionality analysis will inevitably be higher in the right to life than in the right to privacy contexts.

With regard to (1), as explained above human rights bodies have taken an expansive view as to what constitutes an interference with privacy. This would not be limited merely to the interception of the content of a communication, but also to the collection of metadata about the communication,[209] audio-visual observation,[210] GPS tracking,[211] as well as to the storing and use of personal information.[212] Telephone, facsimile, and email communications would be covered by notions of privacy and correspondence, as would other similar forms of telecommunication, e.g. voice or video calls or chats over the Internet.[213] Moreover, "the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference."[214] A violation is conceivable even in the absence of any detriment to the affected individual.[215] Finally,

> [T]he mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.[216]

Question (2) has been of particular importance in the surveillance context. This is so because human rights bodies do not merely require surveillance measures to have a basis in and be lawful under the domestic law of the state concerned, but also for that law to possess certain interrelated *qualities* and satisfy the autonomous meaning of lawfulness under human rights treaties:

---

209. Malone v. United Kingdom (Judgment), App. No. 8691/79, 82 Eur. Ct. H.R. (ser. A), para. 84 (1984).

210. El Haski c. Belgique [El-Haski v. Belgium] (Judgment), App. No. 649/08, Eur. Ct. H.R. para. 102 (2012) (in French), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-113336.

211. Uzun v. Germany (Judgment), App. No. 35623/05, 2010 Eur. Ct. H.R. para. 12–13, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-100293; *see also supra* note 160.

212. *See* S. v. United Kingdom (Judgment), App. Nos. 30562/04 & 30566/04, 2008 Eur. Ct. H.R. paras. 20, 33, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051; Amann v. Switzerland (Judgment), App. No. 27798/95, 2000-II Eur. Ct. H.R. para. 69, *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58497; Leander v. Sweden (Judgment), App. No. 9248/81, 116 Eur. Ct. H.R. (ser. A), para. 48 (1987), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57519.

213. *See* Kennedy v. United Kingdom (Judgment), App. No. 26839/05, Eur. Ct. H.R. (2010), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-98473; Liberty v. United Kingdom (Judgment), App. No. 58243/00, Eur. Ct. H.R. (2008).

214. Weber v. Germany (Decision), App. No. 54934/00, 2006-XI Eur. Ct. H.R.

215. *See* Huvig v. France (Judgment), App. No. 11105/84, 176-B Eur. Ct. H.R. (ser. A), para. 35 (1990), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57627.

216. *Weber*, App. No. 54934/00, Eur. Ct. H.R. para. 78; *see also supra* note 10, at 4 and accompanying text.

accessibility, foreseeability, and compatibility with the rule of law.[217] A breach of domestic legal requirements, or the absence of sufficient legal regulation of surveillance, would automatically lead to a violation at the international level.[218]

Accessibility is satisfied mainly through the publication of the primary and secondary legislation regulating surveillance, which achieves transparency and allows the public to familiarize themselves with the relevant rules. Accessibility does not require the full disclosure of all internal regulations regarding the methods of signals intelligence, if their publication would enable surveillance to be evaded. But a certain level of accessibility must be maintained.[219]

The foreseeability criterion obviously does not require individuals to have advance notice to that they will be subjected to surveillance, as that would defeat the whole purpose of the exercise. Rather, the public must be able to ascertain in what circumstances the authorities have the power to subject individuals to measures of surveillance.[220] In particular, the European 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 individual communications, on the one hand, and more general programmes of surveillance, on the other."[221] The Human Rights Committee also cautioned a number of states that their present legal arrangements on surveillance were insufficiently clear and precise and lacked appropriate safeguards.[222]

With regard to compatibility with the rule of law, the key requirement is that authorities are not granted unfettered discretion in applying surveil-

217. *See Liberty*, App. No. 58243/00, Eur. Ct. H.R.; Malone v. United Kingdom (Judgment), App. No. 8691/79, 82 Eur. Ct. H.R. (ser. A), para 84 (1984); *General Comment No. 16*, para. 3 ("Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.").

218. *See, e.g.*, *Malone*, App. No. 8691/79, Eur. Ct. H.R. para. 87 (regarding the collection of telephony metadata which simply collected in the absence of any legal prohibition, rather than pursuant to an affirmative legal authority); *Weber*, App. No. 54934/00, Eur. Ct. H.R. para. 90.

219. *See* Shimovolos v. Russia (Judgment), App. No. 30194/09, Eur. Ct. H.R. paras. 67–71 (2011); *Liberty*, App. No. 58243/00, Eur. Ct. H.R. paras. 60–61.

220. *Malone*, App. No. 8691/79, Eur. Ct. H.R. para. 67 ("In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."); *see also General Comment No. 16*, para. 8; Van Hulst v. Netherlands, U.N. Human Rights Comm., 82d Sess., Commc'n No. 903/1999, at para. 7.7, UN Doc. CCPR/C/82/D/903/1999 (Nov. 15, 2004). ("[T]he relevant legislation authorizing interference with one's communications must specify in detail the precise circumstances in which such interference may be permitted and that the decision to allow such interference can only be taken by the authority designated by law, on a case-by-case basis.").

221. *Liberty*, App. No. 58243/00, Eur. Ct. H.R. para. 63.

222. *See, e.g.*, U.N. Human Rights Comm., *Concluding Observationson Jamaica*, para. 20, UN Doc. CCPR/C/79/Add.83 (Nov. 19, 1997); U.N. Human Rights Comm., *Concluding Observations on the Russian Federation*, para. 19, UN Doc. CCPR/C/79/Add.54, (July 26, 1995).

lance measures.[223] With regard to telephone tapping in particular, the European Court requires minimum safeguards to be set out in statutory law with respect to "the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."[224] Thus, for instance, in *Liberty* the Court was quite concerned that the "legal discretion granted to the executive for the physical capture of external communications was . . . virtually unfettered."[225] Similarly, both the Human Rights Committee and the European Court have considered independent, especially judicial, supervision of specific surveillance measures to be a crucial safeguard for preventing abuse.[226]

When it comes to arbitrariness/necessity in a democratic society, states will almost invariably be able to satisfy criterion (3), namely that their surveillance regime pursues a legitimate aim, such as national security, public safety, or the prevention of crime.[227] While Article 8(2) of the ECHR provides that safeguarding the "economic well-being of the country" is also a legitimate aim, it remains an open question whether purely economic or industrial espionage would be considered as legitimate if it involved intrusions into the privacy of individuals.

If the formal legality requirements are satisfied, justifiability will turn on criterion (4), proportionality.[228] The proportionality analysis will take into

223. *Malone*, App. No. 8691/79, Eur. Ct. H.R. para. 68 ("Since 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 to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.").

224. Weber v. Germany (Decision), App. No. 54934/00, 2006-XI Eur. Ct. H.R., para. 95; *see also* Iordachi v. Moldova (Judgment), App. No. 25198/02, Eur. Ct. H.R. (2009), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-91245.

225. *Liberty*, App. No. 58243/00, Eur. Ct. H.R. para. 64.

226. *See, e.g.*, Telegraaf Media Nederland Landelijke Media B.V. v. Netherlands (Judgment), App. No. 39315/06, Eur. Ct. H.R. paras. 89–102 (2012), *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-114439; Rotaru v. Romania (Judgment), App. No. 28341/95, 2000-V Eur. Ct. H.R. para. 59 , *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58586; U.N. Human Rights Comm., *Concluding Observations on The Netherlands*, para. 14, UN Doc. CCPR/C/NLD/CO/4 (Aug. 25, 2009); U.N. Human Rights Comm., *Concluding Observations on Sweden*, para. 18, UN Doc. CCPR/C/SWE/CO/6 (April 2, 2009); U.N. Human Rights Comm., *Concluding Observations on Zimbabwe*, para. 25, UN Doc. CCPR/C/79/Add.89, (April 6, 1998).

227. *See, e.g.*, *Weber*, App. No. 54934/00, Eur. Ct. H.R. paras. 103–04.

228. *See* Van Hulst v. Netherlands, U.N. Human Rights Comm., 82d Sess., 70-71, Commc'n No. 903/1999, UN Doc. CCPR/C/82/D/903/1999 (Nov. 15, 2004); Toonen v. Australia, U.N. Human Rights Comm., 50th Sess., para. 8.3, Commc'n No. 488/1992, UN Doc CCPR/C/50/D/488/1992 (Apr. 4, 1994) ("The Committee interprets the requirement of reasonableness to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."); *General Comment No. 16*, para. 4 (holding that non-arbitrariness requires reasonableness).

account a number of factors, and incorporates a level of deference to the state:

> The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.[229]

In *Weber and Saravia* the European Court conducted such an analysis and found that the German G 10 Act on surveillance, as amended after a judgment of the Federal Constitutional Court, satisfied both the legality and proportionality criteria and contained sufficient safeguards to prevent abuse.[230] In *Liberty*, on the other hand, the Court found that the 1985 version of the RIPA did not satisfy the accessibility and foreseeability criteria since it did not "provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing, and destroying intercepted material."[231] But in *Kennedy* the Court found the revised RIPA 2000 to be compliant with Article 8 with regard to the collection of *internal* communications, i.e. within the United Kingdom, pursuant to a specific warrant and with appropriate safeguards.[232]

### *C. Outlook*

The preceding discussion was admittedly general. It is not my purpose here to argue that any given surveillance program, as for example is run by the NSA or GCHQ, is substantively unlawful. Rather, my point is that there already exists an analytical framework in which their lawfulness can be

229. *Weber*, App. No. 54934/00, Eur. Ct. H.R. para. 106.
230. *Id.* paras. 108–38.
231. Liberty v. United Kingdom (Judgment), App. No. 58243/00, Eur. Ct. H.R. para. 69 (2008).
232. Kennedy v. United Kingdom (Judgment), App. No. 26839/05, Eur. Ct. H.R. (2010).

assessed. Hence, while those sceptical about an extraterritorial right to privacy are correct in saying that the advocates for such a right need to explain what it would look like and how it would affect foreign espionage activities that most countries in the world have historically engaged in,[233] this does not mean that we are starting from a blank slate. Nor does this mean that privacy advocates have to come up with a complete extraterritorial privacy blueprint, replete with ready-made, fully-fledged solutions for every conceivable problem, especially when new technologies allow for the application of surveillance measures to vast numbers of ordinary individuals.

Rather, just as in the domestic context, the fleshing out of an extraterritorial right to privacy will happen in an iterative process. Cases will be decided; reports will be filed and debated. Even domestically this process is not restricted to litigation, but also includes dialogue between the executive and the legislative branches, and within each branch, under public scrutiny. Internationally this process involves an even greater multiplicity of actors, from governments and international organizations to human rights bodies, NGOs, academics and activists. Indeed, privacy activists already *have* drawn up a set of principles to govern extraterritorial surveillance, drawing on the case law I have just outlined above.[234] In developing an extraterritorial right to privacy we can always draw upon domestic experiences, including those on data protection,[235] and the already rich case law of national and international courts and human rights bodies on surveillance and related matters, be it the judgments of the German Constitutional Court on dragnets[236] or the European Court's on DNA databases.[237]

In other words, developing a right to privacy externally is fundamentally no different from developing it internally, except that the latter project has had a significant head-start. In doing so, the normative starting point should be the same. The factors that we consider relevant internally would also be relevant externally, be it the type of data being collected, the purpose for which the data will be used, the type and quality of oversight mechanisms, and the clarity and predictability of the legal framework. But while the starting point would be the same, the end result need not be if the differences between the internal and external settings so warrant.

Perhaps most importantly, restricting the use of surveillance internally more than externally can be justified by the state having alternative tools at

233. *See* Benjamin Wittes, *A Global Human Right to Privacy?*, LAWFARE BLOG (Nov. 11, 2013, 5:05 PM), http://www.lawfareblog.com/2013/11/a-global-human-right-to-privacy/.

234. *See International Principles on the Application of Human Rights to Communications Surveillance*, *supra* note 8, at 2 (discussing legality, legitimate aim, necessity, adequacy, proportionality, a competent judicial authority, due process, user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, and safeguards against illegitimate access).

235. *See generally* CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW (2013).

236. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Apr. 4, 2006, 1 BvR 518/02, (Ger.).

237. S. v. United Kingdom (Judgment), App. Nos. 30562/04 & 30566/04, 2008 Eur. Ct. H.R.

its disposal in the domestic context that enable it to achieve the same ends, and this is what a proportionality analysis would be able to take into account. An extraterritorial right to privacy would emphatically *not* mean the end of all traditional (and novel) methods of foreign espionage and surveillance, nor a complete elision of all distinctions between internal and external surveillance. The human rights framework is sufficiently flexible so as to accommodate legitimate governmental interests, and human rights bodies have been prepared to extend to states a significant measure of deference in matters of national security.[238]

Or, to turn back to our Angela Merkel example, although she would like anyone be entitled to respect for her human right to privacy, this does not mean that she could never be lawfully spied upon. This is so not because she would in the eyes of the interfering state be a foreign citizen, or because her privacy would intrinsically be less valued, but because she is the head of a foreign government and the countervailing state interest in knowing what she is up to would be that much stronger when compared to an ordinary person.[239] Yet, she would still be entitled to *some* protection—arguably one could not violate the most intimate areas of her individual autonomy, e.g. by collecting data about her sex life with the purpose of blackmailing her.[240]

In sum, while the human rights framework is flexible, it will still have an impact on the existing surveillance practices, some of which would be regarded as unlawful. While governments should not fear reckless human rights scrutiny, they should also not think that this scrutiny will have no bite.[241] We have seen how the European Court has already dealt with signals

238. In addition to the cases examined above, one of the most comprehensive examples of the deference given by the European Court to a state is *Finogenov v. Russia* (Judgment), App. Nos. 18299/03 & 27311/03, 2011 Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-108231 (dealing with Russia's use of an anaesthetic gas during the terrorist siege of the Dubrovka theatre in Moscow, with the Court refusing, for example, to draw inferences from Russia's failure to supply it with the formula of the gas used, or to question Russia's judgment that the use of the gas was appropriate under the circumstances, despite the many casualties it caused among the hostages).

239. Obviously, governments themselves do not possess human rights. If all a spy did was to steal official documents or computer files, without collecting the personal data or communications of any individual, no human rights issue would arise. Thus, if Edward Snowden was working for Russia or some other states, and all he did was to obtain secret U.S. government documents, he violated applicable U.S. laws but did not necessarily violate anyone's right to privacy. This kind of espionage would not be regulated by international human rights law.

240. *Cf.* Glenn Greenwald, Ryan Gallagher & Ryan Grim, *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit "Radicalizers"*, The Huffington Post (Nov. 26, 2013, 11:20 PM), http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html; Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 3, 2004, 1 BvR 2378/98, (Ger.) (holding that the human dignity guarantee in Article 1(1) of the German Basic Law requires that a central core of a person's private life is inviolable and absolutely protected, and that invasion thereof cannot be justified in the public interest).

241. *See, e.g.*, Ira Rubinstein, Greg Nojeim, & Ronald Lee, *Systematic Government Access to Personal Data: A Comparative Analysis*, Center for Democracy and Technology (Nov. 13, 2013), https://cdt.org/files/pdfs/govaccess2013/government-access-to-data-comparative-analysis.pdf (arguing that due to the pace of technological developments the legislative frameworks of most states do not adequately regulate extraterritorial surveillance and are not satisfactory from a human rights standpoint).

intelligence cases, upholding the surveillance programs in some and requiring improvements in others. The intelligence world did not come crashing down. There is room enough within the human rights framework for both meaningful privacy protections and effective intelligence work—as well as for plenty of practices that may well be stupid but are not unlawful.[242]

## Conclusion

The central thesis of this article is that human rights treaties do apply to all or the vast majority of foreign surveillance activities, including the bulk collection of the communications and personal data of millions of ordinary people by the NSA and GCHQ. The appeal of human rights as a regulatory framework lies precisely in the fact that surveillance measures are now deployed against masses of ordinary people both at home and abroad, rather than simply against the agents of foreign governments who could otherwise be left to their own devices.[243] While it is natural for governments and their intelligence agencies to resist this development, and while some courts and human rights bodies may be prepared to set arbitrary limits on the extraterritorial application of the right to privacy, this resistance is unwise. Any proposed limits on extraterritorial application will ultimately prove unstable and unpersuasive, since they are not supported by any coherent normative theory as to why a certain group of humans is deserving of protection of their privacy, while a different one is not. A categorical rejection of extraterritorial application will only serve to undermine states' arguments on the substantive lawfulness of their surveillance programs.[244] We have already seen, for instance, how the U.K. government's strategy of opposing the application of the ECHR to its forces in occupied Iraq in the end backfired and left it exposed on the merits.[245]

---

242. *See, e.g.*, James Ball, *Xbox Live among Game Services Targeted by US and UK Spy Agencies*, The Guardian (Dec. 9, 2013, 6:26 PM), http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life (reporting on NSA agents deployed to World of Warcraft and other mass online games to monitor whether in-game communications were being used by terrorists).

243. *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches "Into the Past" to Retrieve, Replay Phone Calls*, Wash. Post (Mar. 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (reporting on an NSA program capable of recording and sifting through all of the phone calls made in an unidentified country over the course of a month).

244. *See also* Van Schaack, *supra* note 84, at 62 (calling on the US to relinquish its "untenable and ultimately pointless" categorical opposition to the extraterritorial application of the ICCPR).

245. *See, e.g.*, Al-Jedda v. United Kingdom (Judgment), App. No. 27021/08, 2011 Eur. Ct. H.R., *available at* http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-105612 (holding that UN Security Council resolutions were not clear enough to displace the Article 5 ECHR prohibition on preventive security detention); Smith v. Ministry of Defence, [2013] UKSC 41 (holding that UK soldiers deployed abroad are protected by the ECHR vis-à-vis the UK itself); Al-Skeini v. Sec'y of State for Def., [2005] EWCA (Civ) 1609, [2007] QB 140 (Eng.), *available at* http://www.bailii.org/ew/cases/EWCA/Civ/2005/1609.html; *see also* Marko Milanovic, Hassan v. United Kingdom*, IHL and IHRL, and Other News in (Extra-)Territoriality and Shared Responsibility*, EJIL: Talk! (Dec. 18, 2013), http://

Where the real discussion is to be had, therefore, is not on the threshold question of applicability but on the substance of an extraterritorial right to privacy. And here opinions will obviously differ, likely less so on the general principles and more so on the specifics. Some will naturally incline towards more protection for privacy both internally and externally, while others will favour the pursuit of national security interests.[246] Privacy advocates will, for example, argue that the content/metadata distinction is meaningless in light of modern technological developments and should be abandoned, that distinctions between individuals on the basis of citizenship and immigration status should equally be abandoned, that bulk collection and mass surveillance are categorically incompatible with the right to privacy as inherently disproportionate, that judicial supervision is a central safeguard against abuse, that individuals subjected to surveillance have a right to notified after the fact, and that states have strong positive obligations to be prevent spying by third parties and to regulate private actors.[247] States with extensive surveillance programs will push back against all or some of these arguments, while other states may be more inclined to accept them. But this is a good, healthy process, since many of these issues are complex and non-obvious. Human rights law will thus provide a space for contestation at the international legal level where these issues can be rationally discussed.

And indeed there will be plenty of space for this debate in the near-to-medium term. First, there is the follow-up process to the General Assembly's privacy in the digital age resolution, which will consist inter alia of the report to be prepared by Navi Pillay, the UN High Commissioner for Human Rights, for the next session of the Assembly. That report will be influenced by meetings with stakeholders and experts, and depending on the political situation the Assembly and the Human Rights Council will take further action. Second, the human rights implications of foreign surveillance will be on the agenda of national parliaments[248] and other deliberative bodies.[249]

---

www.ejiltalk.org/hassan-v-united-kingdom-ihl-and-ihrl-and-other-news-in-extra-territoriality-and-shared-responsibility/ (discussing the pending Hassan case, which raises the issue of whether human rights treaties can be derogated from in extraterritorial situations, something that the UK did not do with regard to Iraq and Afghanistan in order to be able to deny that the ECHR applied altogether).

246. *See, e.g.*, Margulies, *supra* note 84, at 29 (arguing that U.S. surveillance programs are broadly consistent with Article 17 ICCPR).

247. *See, e.g.*, *Eyes Wide Open, Special Report*, Privacy Int'l (Nov. 26, 2013), https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf.

248. *See, e.g.*, Jemima Stratford QC & Tim Johnston, Advice in the Matter of State Surveillance, Brick Court Chambers (2014), *available at* http://www.brickcourt.co.uk/news-attachments/APPG_Final_%282%29.pdf (concluding that bulk surveillance by GCHQ is contrary to Article 8 ECHR).

249. *See, e.g.*, Rapporteur of the Comm. on Civil Liberties, Justice & Home Affairs, Draft Report on the US NSA Surveillance Programme, Parl. Eur. Doc. 2013/2188(INI) (2014), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE526.085.

Third, the issue will also be on the agenda during the periodic review of state reports by the Human Rights Committee and perhaps by other treaty bodies. The consideration of the U.S. fourth periodic report already took place in March 2014, with the Committee expressing serious concerns about the NSA's surveillance programs, noting in particular that the United States should

> take all necessary measures to ensure that its surveillance activities, *both within and outside the United States*, conform to its obligations under the Covenant, including article 17; in particular, measures 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 individuals whose communications are under direct surveillance.[250]

The Committee here undoubtedly endorsed the extraterritorial application of the Covenant to foreign surveillance, albeit without explaining under exactly what theory the Covenant would do so. The Committee here also pointed out the normative irrelevance of nationality to the protection of privacy, as I have argued above.

Fourth, foreign surveillance will invariably also be on the radar of universal periodic review before the Human Rights Council, as well as the Council's special procedures. Establishing a special rapporteur on privacy would probably be helpful, but would also run against many states' concerns, budgetary and otherwise, about the proliferation of special procedures. Finally, and perhaps of greatest interest to lawyers, there is the pending and future litigation brought by individuals and NGOs challenging surveillance measures before both domestic and international courts. And while contentious inter-state cases are possible but politically unlikely, it is not unthinkable that the follow-up process to the General Assembly's resolution could produce a request for an advisory opinion from the ICJ on the threshold questions of applicability or on the substantive principles of the human right to privacy in the digital age.

## Postscript

This postscript addresses some important developments, from the finalization of the substantive text of this article in March 2014, up to the end of October 2014. Most importantly, as requested by the General Assembly,[251] and after having conducted an extensive consultation with various stake-

250. U.N. Human Rights Comm., *supra* note 109, at 9 (emphasis added).

251. Resolution on the Right to Privacy in the Digital Age, G.A. Res. 68/167, para. 5, UN Doc. A/RES/68/167, (Jan. 21, 2014).

holders,[252] the Office of the High Commissioner for Human Rights produced a report on privacy in the digital age in July 2014. The OHCHR Report was submitted to the General Assembly and the Human Rights Council,[253] and it is an important and thoughtful contribution to the debates on extraterritorial surveillance. While it is very much pro-privacy oriented, the Report acknowledges the legitimate national security interests of states and does not put privacy on a pedestal of human rights fundamentalism.

The Report correctly finds that interferences with the privacy of electronic communication cannot be justified by reference to some supposedly voluntary surrender of privacy on the Internet by individual users;[254] that the collection of communications metadata can be just as intrusive as the collection of the content of the communication;[255] and that because of the chilling effect of surveillance: "[t]he very existence of a mass surveillance programme thus creates an interference with privacy."[256] The Report hence adopts a broad understanding of what would constitute an interference with privacy that is in line with existing international case law and the arguments developed in this article.

That privacy is interfered with does not mean that that it has been violated. The Report interprets the text of Article 17 of the ICCPR, under which interferences with privacy can only be justified if they are not arbitrary and unlawful, and in doing so it adopts the general analytical framework of legality, necessity, and proportionality. Indeed, it approvingly cites the principles on surveillance and human rights adopted by a number of important NGOs.[257]

While accepting that national security is a legitimate interest for justifying interferences with privacy, the Report notes that the "degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose,"[258] and concludes that mass surveillance programs are especially problematic on proportionality grounds:

> 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 program-

252. Contributions available on the OHCHR website at http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

253. Office of the High Comm'r for Human Rights, *The Right to Privacy in the Digital Age: Report of the OHCHR*, U.N. Doc. A/HRC/27/37, (June 30, 2014) (hereinafter *OHCHR Report*).

254. *Id.* para. 18.

255. *Id.* para. 19.

256. *Id.* para. 20.

257. *Id.* paras. 21–23, fn. 14.

258. *Id.* para. 24.

> mes 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.[259]

This assessment, although hedged somewhat ("may be deemed to be arbitrary," not "*are* arbitrary"(emphasis added)), is still perhaps overly emphatic. It is non-obvious that any kind of bulk collection is inherently disproportionate. If, for example, the U.S. government had reliable intelligence that a terrorist attack was being prepared in New York City in some specific period, and decided to collect communications metadata in bulk in order to thwart this attack while that specific threat persisted, I at least would not find such a measure to be ipso facto disproportionate. It is not necessarily bulk collection as such, but the vast scale, magnitude, and relative permanence of certain mass surveillance programs that warrant serious proportionality concerns.

The Report is similarly skeptical of mandatory third-party data retention policies,[260] and finds that intelligence and data-sharing arrangements may violate the right to privacy without appropriate safeguards, while wisely refraining from exploring in detail the complex and unclear framework of state responsibility regarding compound wrongful acts involving multiple actors.[261] The Report puts much emphasis on the accessibility of the *domestic* legal framework: "secret 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 scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity."[262]

With regard to extraterritoriality problem, which was the main focus of my article, the Report takes a very expansive approach:

> It follows that digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physically controls the data, that State also would have obliga-

259. *Id.* para. 25.
260. *Id.* para. 26.
261. *Id.* para. 27.
262. *Id.* para. 29.

> tions under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation of those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond. This holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty.[263]

While it is good that the Report takes an expansive approach to extraterritoriality, with an emphasis on the *fact* of jurisdiction (rather than the lawfulness of its exercise), the concept of power and control over communications *infrastructure* does not fit well with the existing case law (which, as we have seen, looks at either control over territory or control over individuals). Nor does it seem adequate for those types of surveillance that require no control over the infrastructure at all (for example, directly hacking Angela Merkel's phone, or subjecting her to audio-visual monitoring). But while I submit that my proposed model which relies on the distinction between positive and negative obligations is best suited to deal with the extraterritoriality problem, the Report's approach is still a step in the right direction.

The Report similarly strongly criticizes nationality-based distinctions in domestic legislation regulating surveillance,[264] and addresses the importance of the involvement of private actors (especially businesses) in governmental surveillance.[265] The Report concludes with a number of recommendations,[266] the most important of which is that:

> As an immediate measure, States should review their own national laws, policies and practices to ensure full conformity with international human rights law. Where there are shortcomings, States should take steps to address them, including through the adoption of a clear, precise, accessible, comprehensive and non-discriminatory legislative framework. Steps should be taken to ensure that effective and independent oversight regimes and practices are in place, with attention to the right of victims to an effective remedy.[267]

The OHCHR Report will be an important reference point in the discussions to follow. Indeed, at its 27th regular session in September 2014, the Human Rights Council held a panel discussion on the right to privacy in the digital age, which I had the privilege of moderating. The discussion consisted of an interactive exchange of views between four eminent ex-

263. *Id.* para. 34.
264. *Id.* paras. 35–36.
265. *Id.* para. 45.
266. *Id.* paras. 47–51.
267. *Id.* para. 50.

perts[268] and the representatives of states and other stakeholders.[269] There was broad endorsement, from states as well as from the panelists, of the OHCHR Report, with some disagreement on specific issues. The comments from the floor were substantively quite varied, but two big themes were the application of the ICCPR to extraterritorial surveillance, and the quantity and quality of oversight and accountability mechanisms. The panelists and NGOs also called for the establishment of a new special rapporteur on the right to privacy.

As I am writing this postscript, the right to privacy in the digital age is back on the agenda of the General Assembly at its 69th regular session. A new draft resolution is being negotiated in the Assembly's Third Committee, and it may well call on the Human Rights Council to establish a special mandate on privacy.

268. Catalina Botero, the special rapporteur on the freedom of expression in the Inter-American system; Sarah Cleveland, professor at Columbia Law School; Yves Nissim, deputy chief of corporate social responsibility at Orange Telecom; and Carly Nyst, legal director of Privacy International.

269. The video of the panel discussion is available at http://webtv.un.org/meetings-events/watch/panel-discussion-on-the-right-to-privacy-10th-meeting-27th-regular-session-of-human-rights-council/3781559740001, while a press release summarizing some of the statements is available at http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=15017&LangID=E. OHCHR will be producing a more detailed report on the discussion in due course.