Privacy and Civil Liberties Oversight Board
Public Hearing on Section 702 of the FISA Amendments Act
March 19, 2014

Submission of Amnesty International USA and the American Civil Liberties Union

Amnesty International USA and the American Civil Liberties Union (ACLU) thank the Privacy and Civil Liberties Oversight Board (PCLOB) for the opportunity to submit this statement for the record regarding the application of international human rights law to US surveillance practices.

In this submission, we briefly set out reasons the PCLOB should assess US surveillance practices in an international human rights law framework; summarize key characteristics of Section 702 of the FISA Amendments Act; describe international human rights law on the right to privacy; identify human rights concerns with the collection, storage and use of communications under Section 702; and explain that US human rights obligations are legally binding and applicable to US surveillance practices. We conclude by urging the PCLOB to recommend the repeal of Section 702 as well as other measures to substantially reform US surveillance practices.

I. US Commitments to Global Protection of Privacy and Internet Freedom

The PCLOB should assess US obligations under international human rights law because they are legally binding and govern US surveillance whether it is conducted within US territory or extra-territorially, as we explain in Part V. The PCLOB's review of human rights legal obligations would also be consonant with President Obama's recently affirmed commitments to the privacy of people around the world and the promotion of Internet freedom.

In January 2014, President Obama gave a major speech on National Security Agency (NSA) surveillance programs. He highlighted the US government's duty to ensure privacy and the close relationship between privacy and protection of the right to freedom of expression online. Invoking the language of human rights, he stated:

> As the nation that developed the Internet, the world expects us to ensure that the digital revolution works as a tool for individual empowerment, not government control. . . . [T]he world expects us to stand up for the principle that every person has the right to

think and write and form relationships freely, because individual freedom is the wellspring of human progress.[1]

The President's remarks followed a report by the President's Review Group on Intelligence and Communications Technologies, appointed to review US surveillance programs, that described the right to privacy as a "basic human right" and concluded that the US should provide privacy protections to non-US persons outside US territory when engaging in foreign intelligence collection.[2]

In recognition of the need for reform, the President directed the Director of National Intelligence and Attorney General to develop "safeguards" that extend "certain protections that we have for the American people to people overseas."[3] The PCLOB's review and recommendations on human rights compliance can provide needed guidance for the development of these and additional safeguards, drawing from the sources that have the greatest authority and relevance to global protection of human rights: treaties that establish the right to privacy, the international human rights bodies mandated to interpret and oversee compliance with these treaties and UN experts who have applied well-established human rights norms to fast-evolving surveillance practices.

The President also issued a directive prohibiting, inter alia, the use of signals intelligence "for the purpose of suppressing or burdening criticism or dissent."[4] As the directive reflects, privacy is integral to the protection of freedom of expression and opinion. Surveillance and mass collection undermine confidence in the security of communications. Concern over surveillance may deter individuals from engaging online when it comes to sensitive or politically controversial issues. Mass surveillance thus impedes the free flow of information and ideas—including the right to seek, receive and impart information—severely undermining the global exercise of the rights to freedom of speech, freedom of thought, freedom of association and political participation.[5]

---

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

[2] President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World 155-56 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[3] *Id*.; *see* Presidential Policy Directive, Barack Obama, Signals Intelligence Activities/PPD-28 (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities ("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").

[4] *Id.*

[5] *See* Special Rapporteur on the Right to Freedom of Opinion and Expression, *Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, 3-20, U.N. Doc. A/HRC/23/40 (April 17, 2013) (by Frank La Rue), [hereinafter Rep. by Special Rapporteur on Freedom of Expression] ("[T]he Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a

For many years, international human rights bodies and UN experts have assessed laws impacting these rights in a variety of contexts. Their findings and reports provide invaluable insight and guidance on governing standards and rules to ensure comprehensive protection of the human rights to privacy, freedom of expression and opinion, and freedom of association.

Confining the PCLOB's analysis to US law—and ignoring the protections that international human rights law affords—would send a harmful signal to the rest of the world. It would give a green light to foreign governments to disregard the privacy of communications travelling through territories under their control, including communications of US citizens. Such an approach would also run directly counter to the President's goal of ensuring that "ordinary citizens in other countries have confidence that the United States respects their privacy too."[6] As the President's Review Group wrote: "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."[7]

II. Mass Collection, Storage and Retention of Communications under Section 702

As the ACLU discussed in an earlier submission,[8] Section 702 of the FISA Amendments Act authorizes the "targeting" of non-US persons reasonably believed to be located outside the US for "foreign intelligence" purposes.[9] By making an application to the Foreign Intelligence Surveillance Court (FISC), the US government may obtain a mass acquisition order that authorizes, for an entire year, whatever surveillance the government may choose to engage in, within broadly drawn parameters.[10] The government's definition of "foreign intelligence" sweeps so broadly that it potentially encompasses the communications of almost any non-citizen at all—not just individuals who are foreign agents, engaged in criminal activity, or connected even remotely with terrorist activities. The government's targets may even be entire populations or geographic regions.[11] Finally, the US government's targeting procedures allow the NSA to

---

violation of the Internet users' right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online."); *see also* UN General Assembly Resolution 68/167, "The right to privacy in the digital age," U.N. Doc. A/RES/68/167 (Jan. 21, 2014).

[6] Obama, *supra* note 1.

[7] *See* Review Group on Intelligence and Communication Technologies, *supra* note 2, 156.

[8] For a more detailed discussion of Section 702, *see* Jameel Jaffer, Deputy Legal Director, Am. Civil Liberties Union, Submission to Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act, *available at* https://www.aclu.org/national-security/privacy-and-civil-liberties-oversight-board-public-hearing-fisa-amendments-act.

[9] 50 U.S.C. § 1881a(a).

[10] *Id*.; *id*. at (c)(2).

[11] *See* Letter from Michael B. Mukasey, U.S. Att'y Gen., and John Michael McConnell, Director of National Intelligence, to Harry Reid, U.S. Senator (Feb. 5, 2008), *available at* http://1.usa.gov/1kVLzJu (arguing that the intelligence community should not be prevented "from targeting a particular group of buildings or a geographic area abroad").

sweep up the communications of not only any non-US person who is a target, but any non-US person who may be communicating *about* the target as well.[12]

The effect of this expansive scheme is to bring virtually every international communication within the reach of the NSA's surveillance. What's more, the government retains most of the communications it collects under Section 702 for long periods, and it may disseminate and analyze collected communications with only limited restrictions. Moreover, it may do so without subjecting itself to the scrutinizing glare of the courts.

The FISC's role in reviewing the government's surveillance activities under Section 702 is "narrowly circumscribed."[13] The FISC does not review or approve the government's targeting decisions. Nor does it review or approve the list of "facilities" the government proposes to monitor—to the contrary, the law expressly provides that the government need not inform the FISC of the "facilities, places, premises, or property" at which its surveillance will be directed.[14] The FISC reviews only the general procedures that the government proposes to use in carrying out its surveillance, related to targeting and minimization. Nothing in the law requires the government even to inform the FISC who its surveillance targets are (beyond to say that the targets are reasonably believed to be outside the US) or what the surveillance is (beyond to say that a "significant purpose" of the surveillance is "foreign intelligence").

Based on this analysis, and as described more fully below, Section 702 violates basic standards of human rights law and should be repealed.

III. The International Human Right to Privacy

The International Covenant on Civil and Political Rights (ICCPR), which the US ratified in 1992, prohibits any "interference" with privacy that is "arbitrary" or "unlawful."[15] Although the ICCPR does not define these terms, there is a growing catalogue of human rights law

---

[12] *See* Procedures Used By the National Security Agency for Targeting Non–United States Persons Reasonably Believed To Be Located Outside the United States To Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended at 1–3 (2009), https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf ("2009 Targeting Procedures"); Charlie Savage, *NSA Said to Search Content of Messages to and from U.S.*, N.Y. Times, Aug. 8, 2013, at A1, *available at* http://nyti.ms/1cez5ZK.

[13] *See* In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008, No. 08-01, 2008 WL 9487946 at *2 (FISA Ct. Aug. 27, 2008).

[14] 50 U.S.C. § 1881a(g)(4).

[15] Article 17 of the ICCPR provides that:

> 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.

International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; *see also* Universal Declaration of Human Rights, art. 12, G.A. Res. 217(III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

jurisprudence and official commentary that does, providing clear evidence of the state of the law and guidance to states regarding compliance.[16] This catalogue, which we describe below, also reflects bedrock principles of human rights law—such as legality, proportionality, non-discrimination, and the right to a remedy—that have long been regarded as fundamental to human rights protection.[17]

One of the most important sources of human rights law is the findings, recommendations and commentaries of the UN Human Rights Committee, which is mandated by the ICCPR to interpret and oversee state compliance with the treaty.[18] The Human Rights Committee plays a central role in defining rights, like privacy and freedom of expression, that the ICCPR permits governments to restrict or limit for certain purposes.[19] One of the most important functions of the Human Rights Committee in this regard is the publication of General Comments—authoritative and detailed interpretations of rights protected by the ICCPR. The reports of UN Special Rapporteurs are another important source of authority at the international level. Special Rapporteurs, who are independent experts on human rights law, are appointed by the UN Human Rights Council to review thematic issues or country situations. Finally, the decisions of regional human rights bodies from the Inter-American human rights system,[20] of which the US is a part,

---

[16] Article 38 of the Statute of the International Court of Justice (ICJ) is generally recognized as an authoritative statement of sources of international law. It lists as sources: international conventions; international custom, as evidence of a general practice *accepted as law* (emphasis added); the general principles of law recognized by civilized nations; and judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law. *See also* Third Restatement of the Law, Foreign Relations Law of the United States § 102(1) ("A rule of international law is one that has been accepted as such by the international community of states (a) in the form of customary law); (b) by international agreement; or (c) by derivation from general principles common to the major legal systems of the world").

[17] *See, e.g.*, U.N. Economic and Social Council, Commission on Human Rights, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, U.N. Doc. E/CN.4/1985/4 (Sept. 28, 1984).

[18] The Human Rights Committee reviews periodic reports from state parties, including the US, about their implementation of the ICCPR and issues observations on state practices. *See* ICCPR, *supra* note 15, art. 28. It also issues General Comments providing authoritative interpretations and guiding frameworks for compliance with treaty obligations. *See* U.N. Human Rights Comm., *General Comments Adopted by the Human Rights Committee*, U.N. Doc. CCPR/C/C/21/Rev.1 (May 19, 1989). Jurisprudence of the U.N. Human Rights Committee exists by virtue of its authority under the First Optional Protocol to the ICCPR to examine individual complaints.

[19] Special Rapporteur on Counter-Terrorism and Human Rights, *Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism*, ¶ 15, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009) (by Martin Scheinin) [hereinafter Rep. by Special Rapporteur on Counter-Terrorism] ("Article 17 is written in a manner that allows States parties the possibility to introduce restrictions or limitations....subject to the monitoring functions of the Human Rights Committee as the treaty body entrusted with the task of interpreting the provisions of the Covenant and addressing the conduct of States parties in respect of their treaty obligations.").

[20] The Inter-American Commission on Human Rights oversees state compliance with the two major human rights instruments of the Organization of American States: the American Declaration of the Rights and Duties of Man, a nonbinding statement of international legal obligations which the US has signed; and the American Convention on Human Rights, which the US has signed but not ratified. Both of these instruments protect the right to privacy. *See* Organization of American States, American Convention on Human Rights art. 11, Nov. 22, 1969, O.A.S.T.S. No. 36, 1144 U.N.T.S. 123; Inter-Am. Comm'n H.R., American Declaration of the Rights and Duties of Man art. 5, May

and the European Court of Human Rights are also persuasive authorities on human rights and provide some of the most detailed considerations of the intersection of surveillance and the protection of human rights.[21]

The ICCPR and the Human Rights Committee's General Comment on privacy, General Comment 16, were drafted prior to the advent of modern information technologies.[22] Yet they establish important human rights principles and guarantees against state intrusions on privacy. [23] Through both the General Comment and its consideration of state practice, the Human Rights Committee has affirmed that the human right to privacy encompasses the right to access and control one's personal data.[24] The Committee has also made clear that the terms "family" and "home," which are referenced in Article 17, and the concept of "privacy" itself, should be interpreted broadly to include protections beyond those explicitly listed in the ICCPR.[25] In its

---

2, 1948, OEA/Ser.L/V/II.82 doc.6 rev.1 at 17 (1992), *available at* https://www.oas.org/en/iachr/mandate/Basics/2.AMERICAN%20DECLARATION.pdf. The Inter-American Court of Human Rights is an autonomous judicial institution that applies and interprets the American Convention on Human Rights; however, the US does not accept is jurisdiction. *See* Statute Inter-Am. Ct. H.R., O.A.S. Res. 448 (IX-0/79), O.A.S. Off. Rec. OEA/Ser.P/IX.0.2/80, Vol. 1 at 98.

[21] The European Court of Human Rights is charged with evaluating state compliance with the European Convention for the Protection of Human Rights and Fundamental Freedoms ("European Convention"). Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221. Article 8 of the European Convention protects the right to privacy but includes express limitations, including that an interference may be permitted if it is "necessary in a democratic society in the interest 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." *Id*. at art. 8.

[22] *See* U.N. Human Rights Comm., *CCPR General Comment No. 16: Article 17 (The Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, ¶ 8, U.N. Doc. HRI/GEN/1/Rev.1 (Apr. 8, 1988) [hereinafter General Comment 16].

[23] General Comments provide State parties with an authoritative interpretation and guiding framework for compliance with their treaty obligations, among other functions. They are highly persuasive authority, although they are not legally binding interpretations of treaty text. Philip Alston & Ryan Goodman, International Human Rights 691 (2013).

[24] General Comment 16, *supra* note 22, ¶ 10 ("The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law"). The European Court has repeatedly found that "protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life." MK v. France, App. No. 19522/09, Eur. Ct. H.R. ¶ 32 (Apr. 18, 2013). *See also* S. and Marper v. the United Kingdom [GC], App. Nos. 30542/04 and 30566/04, Eur. Ct. H.R. ¶ 103 (Dec. 4, 2008); Gardel v. France, App. No. 16428/05, Eur. Ct. H.R. ¶ 62 (Dec. 17, 2009); M.B. v. France, App. No. 22115/06, Eur. Ct. H.R. ¶ 53, (Dec. 17, 2009); B.B. v. France, App. No. 5335/06, Eur. Ct. H.R. ¶ 61 (Dec. 17, 2009).

[25] *See, e.g.*, Coeriel et al. v. The Netherlands, U.N. Human Rights Comm., Communication No. 453/1991 ¶ 10.2,

U.N. Doc. CCPR/C/52/D/453/1991 (1994) (observing that the right to privacy protects the right to freely express one's identity); *see also* Gallicchio v. Argentina, U.N. Human Rights Comm., Communication No. 400/1990 ¶ 10.4, U.N. Doc. CCPR/C/53/D/400/1990 (1995) (finding falsification of a baby's birth certificate resulting in a different legal identity violates Article 17); Toonen v. Australia, U.N. Human Rights Comm., Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994) (confirming that the right to privacy includes the right to engage in consensual sexual activity in private); Hertzberg et al. v. Finland, U.N. Human Rights Comm., Communication No. 61/1979, Appendix, U.N. Doc. CCPR/C/15/D/61/1979 (1982) (emphasizing that Article 17 protects "the right to be different and live accordingly").

March 2014 report on the US, the Committee specifically expressed concern about US surveillance practices and the "adverse impact on the right to privacy."[26] The UN Special Rapporteur on Freedom of Expression has likewise emphasized that the ICCPR's reference to protecting "correspondence" applies to "all forms of communication, including via the Internet."[27] Moreover, surveillance laws that produce a chilling effect on protected activity implicate privacy concerns for purposes of the ICCPR, as does the collection and storage of personal data. [28]

The Human Rights Committee's jurisprudence and consideration of state practice, together with statements by UN Special Rapporteurs, reflect the following key standards that must be satisfied by any surveillance program to comply with Article 17 of the ICCPR. We discuss each in depth below:

A. **Public Transparency**: The parameters of any surveillance program must be established by laws that are accessible to the public and incorporate measures that are precise, specific, and clearly defined;
B. **Proportionality and Necessity:** Surveillance measures must be necessary and proportional to a legitimate government aim, such as law enforcement or national security. The "interference" should be the least intrusive method possible to achieve the government's legitimate aim.
C. **Independent oversight and redress**: Surveillance should be subject to oversight by a competent, independent and impartial tribunal. Impacted individuals should have access to a remedy for violation of their right, regardless of their nationality or where they live.
D. **Non-discrimination:** Measures to restrict surveillance should, as a general matter, provide equal protections to everyone regardless of their nationality.

---

[26] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant: International Covenant on Civil and Political Rights*, Concluding Observations, United States, ¶ 22, Advance Unedited Version (March 2014), *available at* http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf [hereinafter U.N. Human Rights Comm., Concluding Observations on the United States].

[27] Rep. by Special Rapporteur on Freedom of Expression, *supra* note 5, ¶ 57.

[28] For example, in *Toonen v. Australia*, the Human Rights Committee found that provisions of a law that had not been enforced for several years directly interfered with the applicant's privacy where it criminalized various forms of sexual contact between men. Toonen v. Australia, *supra* note 25, ¶ 8.2. The European Court has applied this same principle in the surveillance context, emphasizing that "the 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 necessarily strikes at freedom of communication…and thereby amounts in itself to an interference…" Weber and Saravia v. Germany, App. No. 54934/00, Decision as to Admissibility, Eur. Ct. H.R. ¶ 78 (Jun. 29, 2006). International human rights law also recognizes that the collection and storage of personal data itself constitute an "interference" with privacy interests, *see e.g.*, Shimovolos v. Russia, App No. 30194/09, Judgment, Eur. Ct. H.R. ¶ 68 (Jun. 21, 2011) (finding that "systematic storage and collection of data by security services" interfered with privacy rights); there is no requirement that the data in addition be examined or otherwise processed. *Id* .

Differential treatment based solely on nationality must be reasonable, objective and based on a legitimate purpose.

A. Public Transparency

Article 17's prohibition on "unlawful" interference "means that no interference can take place except in cases envisaged by law."[29] A broad grant of surveillance powers in a statute is not sufficient to make an interference "lawful." In considering wiretapping and other state practices, the UN Human Rights Committee has emphasized that such statutes "must specify in detail the precise circumstances in which [an] interference [with privacy] may be permitted," [30] and generally be "precise" and "clearly" defined. [31]

In its March 2014 report on the US, the Human Rights Committee called on the US to ensure that any surveillance be authorized by laws that, inter alia, are "publicly accessible" and "sufficiently precise specifying in detail the precise circumstances in which any such interference may be permitted; the procedures for authorizing; the categories of persons who may be placed under surveillance; limits on the duration of surveillance; [and] procedures for the use and storage of the data collected."[32]

The requirement that laws be transparent and publicly accessible is a bedrock principle of human rights law, common to the Human Rights Committee's analysis of rights such as freedom of opinion and expression.[33] It is also a basic component of the rule of law.[34] The underlying

---

[29] General Comment 16, *supra* note 22, ¶ 3.

[30] Van Hulst v. Netherlands, U.N. Human Rights Comm., Communication No. 903/1999 ¶ 7.7, U.N. Doc. CCPR/C/82/D/903/1999 (2004). In General Comment 16, the UN Human Rights Committee likewise stated that "relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted." General Comment 16, *supra* note 22, ¶ 8.

[31] *See* U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant*, Concluding Observations, Jamaica, ¶ 20, U.N. Doc. CCPR/C/79/Add.83 (Nov. 19, 1997) [hereinafter U.N. Human Rights Comm., Concluding Observations on Jamaica].; U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant*, Concluding Observations, Russian Federation, ¶ 19, U.N. Doc. CCPR/C/79/Add.54 (July 26, 1995) [hereinafter U.N. Human Rights Comm., Concluding Observations on Russia].

[32] U.N. Human Rights Comm., Concluding Observations on the United States, *supra* note 26, ¶ 22.

[33] *See* U.N. Human Rights Comm., *General Comment No. 34, Article 19, Freedoms of opinion and expression*, ¶¶ 24-26, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011) [hereinafter General Comment 34]; *see also* U.N. Human Rights Comm., *CCPR General Comment No. 27: Article 12 (Freedom of Movement)*, ¶¶ 11-12, U.N. Doc. CCPR/C/21?Rev.1/Add.9 (Nov. 2, 1999) (in setting out permissible limitations on the right to freedom of movement, emphasizing that "restrictions should use precise criteria and may not confer unfettered discretion on those charged with their execution") [hereinafter General Comment 27].

[34] *See* Lon L Fuller, Morality of Law (Yale University Press rev. ed., 1969); Report of UN Secretary-General, "The Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies" (2004), U.N. Doc. No. S/2004/616 (describing the rule of law as requiring "legal certainty, avoidance of arbitrariness and procedural and legal transparency"); David Neuberger, President, Supreme Court of the U.K., 2013 Justice Tom Sargant Memorial

rationale is that publicly accessible laws and regulations can enable a person to ascertain the applicable legal regime in advance, providing protection against arbitrary exercise of state power.[35] This is especially crucial in the context of rapidly developing technology that permits governments to conduct surveillance in ways previously unforeseen by the public.[36]

A surveillance regime based on rules that are not accessible to the public or that allows a high degree of government discretion in its implementation may fail to be "lawful" for purposes of the ICCPR. For example, in considering the Russian government's surveillance of telephone communications, the Human Rights Committee expressed concern that surveillance was possible "without clear legislation setting out the conditions of legitimate interferences with privacy and providing for safeguards against unlawful interferences."[37] Likewise, in addressing Jamaican wiretapping practices, the Human Rights Committee emphasized the need to "adopt precise legislation" in relation to wire-tapping.[38]

The European Court of Human Rights (European Court) also emphasizes the quality of the law, rather than its mere existence.[39] According to the European Court, the law must be set out so that individuals can "foresee, to a degree that is reasonable in the circumstances, the consequence which a given action may entail."[40] In the specific context of government surveillance, the European Court stated that this requirement "cannot mean that an individual should be able to foresee when the authorities are likely to resort to secret surveillance so that he can adapt his conduct accordingly." [41] It continued: "However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on the application of secret measures of surveillance, especially as the technology available for use is continually becoming more sophisticated." [42] In

---

Lecture in London, U.K., *available at* http://supremecourt.uk/docs/speech-131015.pdf (describing the rule of law as meaning "the laws must be freely accessible: that means as available and as understandable as possible").

[35] *See* Huvig v. France, App. No. 11105/84, Judgment, Eur. Ct. H.R. ¶ 29 (Apr. 24, 1990) (quoting Malone v. United Kingdom, App No. 8691/79, Judgment, Eur. Ct. H.R. ¶ 67 (Aug. 2, 1984)).

[36] *See* Uzun v. Germany, App. No. 35623/05, Judgment, Eur. Ct. H.R. ¶ 61 (Sept. 2, 2010).

[37] U.N. Human Rights Comm., Concluding Observations on Russia, *supra* note 31, ¶ 19.

[38] U.N. Human Rights Comm., Concluding Observations on Jamaica, *supra* note 31, ¶ 20.

[39] The European Convention is worded differently, and the European Court developed its "quality of law" test to interpret various articles of the European Convention that refer to the need for limitations on rights to be "prescribed by law." *See, e.g.*, Kafkaris v. Cyprus [GC], App. No. 21906/04, Judgment, Eur. Ct. H.R. ¶ 116 (Feb. 12, 2008); Malone v. United Kingdom, *supra* note 35.

[40] Sunday Times v. United Kingdom, App. No. 6538/74, Judgment, Eur. Ct. H.R. ¶ 49 (Apr. 26, 1979). *See also* Kafkaris v. Cyprus [GC], *supra* note 39, ¶¶ 150-152; Hashman and Harrup v. United Kingdom [GC], App. No. 25594/94, Judgment, Eur. Ct. H.R. ¶ 31 (Nov. 25, 1999); Malone v. United Kingdom, *supra* note 35.

[41] Shimovolos v. Russia, *supra* note 28.

[42] *Id.*; "Moreover, 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 or to a judge to be expressed in terms of an unfettered power. Consequently,

particular, "[t]he law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are *empowered to resort* to any measures of secret surveillance and collection of data" (emphasis added). In light of the "risk of abuse intrinsic to any system of secret surveillance," minimum safeguards to avoid abuse must be set in statute law and include "the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided."[43]

B. Proportionality and Necessity

Article 17 of the ICCPR, like several other provisions in human rights treaties, establishes a right subject to permissible limitations rather than an absolute right. However, any limitations must be strictly construed. As a threshold matter, the limitation must be compatible with the object and purpose of the treaty and may not impair the essence of the right.[44] Article 17 also requires that the interference be both lawful and non-arbitrary, that is, "reasonable in the particular circumstances of the case."[45] In assessing reasonableness, the Human Rights Committee has applied a proportionality and necessity test. [46] To be non-arbitrary, a given measure must satisfy a traditional proportionality test: it must pursue a legitimate aim, have a

---

the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference," Weber and Saravia v. Germany, *supra* note 28, ¶ 94.

[43] Shimovolos v. Russia, *supra* note 28 (citing Uzun v. Germany). *See also* Ass'n for Eur. Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, Judgment, Eur. Ct. H.R. ¶¶ 71-77 (28 June 2007); Liberty and Others v. United Kingdom, App. No. 58243/00, Judgment, Eur. Ct. H.R. § 62 (Jul. 1, 2008).

[44] *See* ICCPR, *supra* note 15, art. 5; For a discussion of the right to remedy under human rights law, *see* U.N. Human Rights Comm., *General Comment No. 31 [80]: The Nature of the General Legal Obligation Imposed on State Parties to the Covenant*, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (May 26, 2004) [hereinafter General Comment 31]; *see also* U.N. Comm'n on Human Rights, *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, Annex, U.N. Doc. E/CN.4/1985/4 (Sept. 28, 1984).

[45] General Comment 16, *supra* note 22, ¶ 4; Canepa v. Canada, U.N. Human Rights Comm., Communication No. 558/1993 ¶ 11.4, U.N. Doc. CCPR/C/59/D/558/1993 (1997) ("arbitrariness within the meaning of Article 17 is not confined to procedural arbitrariness, but extends to the reasonableness of the interference with the person's rights under Article 17 and its compatibility with the purposes, aims and objectives of the Covenant").

[46] *See* Toonen v. Australia, *supra* note 25, ¶ 8.3 ("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* (emphasis added); Van Hulst v. Netherlands, *supra* note 30, ¶ 7.6 (the Committee recalls its jurisprudence that the requirement of reasonableness implies that any interference with privacy must be proportionate to the end sought, and must be necessary in the circumstances of any given case"; *see , e.g.*, M.G. v. Germany, U.N. Human Rights Comm., Communication No. 1482/2006, U.N. Doc. CCPR/C/93/D/1482/2006 (2008) (finding a German court's order for a medical examination on the applicant to be a disproportionate and therefore arbitrary interference with privacy); Madafferi v. Australia, U.N. Human Rights Comm., Communication No. 1011/2001 ¶ 9.8, U.N. Doc. CCPR/C/81/D/1011/2001 (2004) (finding an arbitrary interference with family, contrary to article 17).

rational connection to that aim, minimally impair the right to privacy, and strike a fair balance between pursuit of the aim and limitation of the right.[47]

In its March 2014 report on the US, the Human Rights Committee called on the US to ensure that its surveillance activities complied with the principles of proportionality and necessity. It emphasized that surveillance laws must "contain provisions that ensure that collection of, access to and use of communications data are tailored to specific legitimate aims."[48]

The Human Rights Committee's General Comment 27, which generally "codifies the position of the UN Human Rights Committee in the matter of permissible limitations to the rights provided under the Covenant,"[49] likewise emphasizes that any restriction must "conform to the principle of proportionality" and be "the least intrusive instrument amongst those which might achieve the desired result."[50] The European Court and Inter-American Court of Human Rights have similarly applied proportionality and necessity test to assess the lawfulness of any interference with privacy.[51]

In an April 2014 decision, the Court of Justice of the European Union applied a proportionality test to strike down a European Union Directive that required Member States to impose an obligation on telecommunications service providers to retain communications data of everyone in the EU, for a period of between six months and two years. [52] The Court held the Directive was disproportionate because it covered all individuals "without any differentiation, limitation or exception being made in light of the objective of fighting against serious crime;" did not lay down objective criteria to limit government authorities' access to data; and imposed a data retention period of at least six months, without providing objective criteria to ensure it was limited to what was strictly necessary, and without making any distinction between retention of different categories of data based on the persons concerned or its potential usefulness.[53]

---

[47] *See* Rep. by Special Rapporteur on Counter-Terrorism, *supra* note 19, ¶¶ 14-19; Rep. by Special Rapporteur on Freedom of Expression, *supra* note 5, ¶¶ 28-29. *See also* Manfred Nowak, U.N. Covenant on Civil and Political Rights: CCPR Commentary at 383 (2d ed., 2005); Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶ 56 (2009); Van Hulst v. Netherlands, *supra* note 30 (noting in passing that both parties argued for proportionality based on the traditional four-part test).

[48] U.N. Human Rights Comm., Concluding Observations on the United States, *supra* note 26, ¶ 22.

[49] Rep. by Special Rapporteur on Counter-Terrorism, *supra* note 19, ¶ 17; *see also* General Comment 34, *supra* note 33 (quoting General Comment 27's formulation on permissible limitations in discussing freedom of expression).

[50] General Comment 27, *supra* note 33, ¶ 14 (General Comment on freedom of movement).

[51] *See* Klass and Others v. Germany, App. No. 5029/71, Judgment, Eur. Ct. H.R. ¶¶ 42, 59, Series A no. 28 (Sept. 6, 1978); Tristán Donoso v. Panamá, *supra* note 47.

[52] Digital Rights Ireland and Seitlinger and Others, Judgment in Joined Cases C-293/12 and C-594/12, Court of Justice of the European Union (April 8, 2014), *available at* http://www.janalbrecht.eu/fileadmin/material/Dokumente/c_293_c_594.pdf.

[53] *Id.*

C. Independent Oversight and Redress

Human rights law requires impartial and independent oversight of surveillance practices as a safeguard against abuse.[54] The Human Rights Committee has emphasized the importance of review by a competent, independent and impartial oversight mechanism to ensure that only pertinent evidence is gathered,[55] and that *ex post* review should ensure that any data collected is not used for any purpose contrary to Article 17 of the ICCPR.[56]

Human rights bodies and experts have highlighted that surveillance and other measures should be taken on the basis of specific decisions by a competent, independent and impartial tribunal.[57] In *Al-Gertani v. Bosnia and Herzegovina*, the Human Rights Committee determined that the surveillance operations at issue complied with Article 17 in part because they "were considered and reviewed in a fair and thorough manner by the administrative and judicial authorities." [58] Likewise, in *Van Hulst*, the Human Rights Committee recognized that Dutch law met Article 17's requirements because the interception of communications had to be "based on a written authorization by the investigating judge."[59]

While human rights law does not necessarily mirror US constitutional requirements for warrants, it reflects similar concerns that surveillance be authorized by an independent and impartial authority and that it be particularized to specific individuals and locations.[60] As the UN Special Rapporteur on Freedom of Expression has emphasized:

> [M]easures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the

[54] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant*, Concluding Observations, Poland, ¶ 22, U.N. Doc. CCPR/C/79/Add.110 (Jul. 29, 1999) [hereinafter U.N. Human Rights Comm., Concluding Observations on Poland]; U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant*, Concluding Observations, Sweden, ¶ 18, U.N. Doc. CCPR/C/SWE/CO/6 (Mar. 25, 2009) [hereinafter U.N. Human Rights Comm., Concluding Observations on Sweden].

[55] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant*, Concluding Observations, The Netherlands, ¶ 14, U.N. Doc. CCPR/C/NLD/CO/4 (Aug. 25, 2009) [hereinafter U.N. Human Rights Comm., Concluding Observations on The Netherlands].

[56] U.N. Human Rights Comm., Concluding Observations on Sweden, *supra* note 54, ¶ 18.

[57] *See, e.g.*, Rep. by Special Rapporteur on Freedom of Expression, *supra* note 5, ¶ 59.

[58] Al-Gertani v. Bosnia & Herzegovina, U.N. Human Rights Comm., Communication No. 1955/2010 (2010) ¶ 5.6, U.N. Doc. CCPR/C/109/D/1955/2010 (Nov. 6, 2013).

[59] Van Hulst v. Netherlands, *supra* note 30, ¶ 7.7; *see also* U.N. Human Rights Comm., Concluding Observations on Sweden, *supra* note 54, ¶ 18 (requiring "review and supervision by an independent body" to prevent abuses in the gathering, storage and use of personal data).

[60] Compare Van Hulst v. Netherlands, *supra* note 30, with *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime…[61]

Moreover, where violations occur, human rights law requires that affected individuals have access to a remedy for violation of their right to privacy, regardless of their nationality or where they live.[62] In its March 2014 review of US surveillance practices, the Human Rights Committee called on the US to "ensure that affected persons have access to effective remedies in cases of abuse."[63]

D. Non-Discrimination

Non-discrimination and equal protection of the law are fundamental requirements of human rights.[64] The ICCPR prohibits discrimination with regard to all rights and benefits recognized by law, including between citizens and non-citizens.[65] The Human Rights Committee has identified privacy, freedom of expression and association as rights for which "[t]here shall be no discrimination between aliens and citizens."[66]

Thus, measures aimed at restricting the scope of permissible surveillance should, as general matter, be extended equally to everyone regardless of their nationality. Any distinctions made in treatment based solely on nationality are justifiable only if they are reasonable, objective, and based on a legitimate purpose.[67] Indeed, in its March 2014 report on the US, the Human Rights Committee expressed concern about US law's "limited protection against excessive surveillance" for non-citizens. [68] It called on the US "to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity

[61] Rep. by Special Rapporteur on Freedom of Expression, *supra* note 5, ¶ 59.

[62] For a discussion of the right to remedy under human rights law, *see* General Comment 31, *supra* note 44; in the privacy context, *see* Bulgakov v. Ukraine, U.N. Human Rights Comm., Communication No. 1803/2008 ¶ 9, U.N. Doc. CCPR/C/106/D/1803/2008 (Sept. 11, 2012).

[63] U.N. Human Rights Comm., Concluding Observations on the United States, *supra* note 26, ¶ 22.

[64] UN Human Rights Comm., *CCPR General Comment No. 18: Non-Discrimination*, ¶ 1, U.N. Doc. HRI/GEN/1/Rev. 1 (Nov. 10, 1989) [hereinafter General Comment 18].

[65] ICCPR, *supra* note 15, art. 26; U.N. Human Rights Comm., *General Comment No. 15: The position of aliens under the Covenant*, ¶ 2, U.N. Doc. HRI/GEN/1/Rev.1 (April 11, 1986) ("The general rule is that each one of the rights of the Covenant must be guaranteed without discrimination between citizens and aliens").

[66] *Id.* at ¶ 7 ("[Aliens] may not be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. They have the right to freedom of thought, conscience and religion, and the right to hold opinions and to express them. Aliens receive the benefit of the right of peaceful assembly and of freedom of association. 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.").

[67] General Comment 18, *supra* note 65, ¶ 13.

[68] U.N. Human Rights Comm., Concluding Observations on the United States, *supra* note 26, ¶ 22.

regardless of the nationality or location of individuals whose communications are under direct surveillance" (emphasis added).[69]

The US government and some ally governments provide greater protections against surveillance to citizens than non-citizens.[70] However, there can be no justifiable basis for the blanket distinction between citizens and non-citizens established by Section 702 with regard to the substantive and core protection of privacy.[71] Although some procedural requirements may, for example, vary based on an individual's location, such difference in treatment must be based on reasonable grounds and must be compatible with the Convention.[72] The difference in treatment established by Section 702 is unreasonable because non-citizens are not as a class inherently more dangerous to state security than citizens, nor are their private communications of inherently greater value or interest to a government conducting surveillance. The difference in treatment in Section 702 operates to deny altogether protection of the privacy rights of non-citizens located outside the US.[73]

The Human Rights Committee has also noted that "the enjoyment of Covenant rights is not limited to citizens of State parties but must also be available to all individuals . . . who may find themselves in the territory or *subject to the jurisdiction* of the State party" (emphasis added).[74] There is no territorial limit on the equal protection provision of the ICCPR; the issue of the jurisdictional scope of the ICCPR is a separate one.[75]

IV. Mass Collection, Storage and Retention of Communications under Section 702 as an Arbitrary and Unlawful Interference with the Right to Privacy

[69] *Id.*

[70] These countries include Australia, New Zealand and the United Kingdom. *See* Marko Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age, Harvard International Law Journal (forthcoming) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485; Center for Democracy & Technology, Systematic Government Access to Personal Data: A Comparative Analysis (2013), *available at https://www.cdt.org/files/pdfs/govaccess2013/government-access-to-data-comparative-analysis.pdf.*

[71] *See* General Comment 16, *supra* note 22, ¶ 6 ("In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right").

[72] *See* Simunek et al. v. Czech Republic, U.N. Human Rights Comm., Communication No. 516/1992 ¶ 11.5, U.N. Doc. No. CCPR/C/54/D/516/1992 (1995) ("A differentiation which is compatible with the provisions of the Covenant and is based on reasonable grounds does not amount to prohibited discrimination within the meaning of article 26").

[73] *See* Milanovic, *supra* note 70, 23-25; *see also* A and Ors. v. United Kingdom, App. No. 3455/05, Judgment, Eur. Ct. H.R. ¶¶ 186, 189-90 (Feb. 19, 2009) (finding that law distinguishing between nationals and non-nationals for preventive security detention was disproportionate, discriminatory and irrational, and noting that the issue was not "immigration measures, where a distinction between nationals and non-nationals would be legitimate, but instead concerned with national security").

[74] General Comment 31, *supra* note 44, ¶ 10.

[75] *See infra* Part V.

The US government's surveillance authorized under Section 702 violates US obligations under Article 17 of the ICCPR for the following reasons:

- Section 702 violates Article 17's requirement of lawfulness because it provides US officials an extremely broad grant of authority and effectively unfettered discretion to secretly collect, store, and use protected communications. The statute fails to establish clear and precise limitations on the scope of the surveillance it authorizes.[76] Key terms such "foreign intelligence" are defined so broadly that the statute's authority potentially encompasses the communications of almost any foreign person at all—not just individuals who are foreign agents, engaged in criminal activity, or connected even remotely with terrorist activities. Neither the FISA Amendments Act itself nor FISC opinions, most of which have been withheld from the public, provide the public with sufficient access to information about the potential scope or duration of surveillance or the grounds required for ordering it.
- Mass acquisition orders under Section 702 are "arbitrary" and violate Article 17 because they are a disproportionate measure and are not narrowly tailored to achieve a stated national security objective; to the contrary, they provide a blank check for surveillance subject only to "targeting and minimization" procedures that themselves are not aimed at providing any protection of the privacy interests of non-US persons outside US territory. In *Van Hulst v. Netherlands*, the Human Rights Committee emphasized—in the context of phone-tapping—that "the decision to allow such interference can only be taken by the authority designated by law, on a case-by-case basis."[77] Mass acquisition is completely contrary to this particularized approach.
- Mass collection of about-the-target communications constitutes an arbitrary interference with the right to privacy for the same reasons and because it does not represent the least intrusive means of achieving a legitimate end.
- Targeting and minimization procedures fail to address concerns about the privacy of non-US persons. They are intended principally to protect against intentional surveillance of particular, known US persons and permanent residents.

[76] The European Court's approach in *Liberty v. United Kingdom* is instructive. In considering a British law authorizing surveillance of telephone communications, the European Court noted that relevant legislation provided an "extremely broad discretion," with "no limit to the type of external communications" caught by surveillance or caught by what the State could listen to or read. Consequently, the court held that the law did not provide "adequate protection against abuse of power." Liberty v. United Kingdom, App. No. 58243/00, Judgment, Eur. Ct. H.R. ¶¶ 64–65 (Jul. 1, 2008).

[77] Van Hulst v. Netherlands, *supra* note 30, ¶ 7.7; *see also* Rep. by Special Rapporteur on Freedom of Expression, *supra* note 5, ¶ 38 ("Mass interception technology eradicates any considerations of proportionality….It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for reach individual case of interception").

- Section 702 violates non-discrimination and equal protection provisions of the ICCPR by denying any protection whatsoever to non-US persons outside the US. This differential treatment appears premised on a flawed belief that the US government does not owe any privacy protections to non-US persons; a position that the President recently rejected.
- The FISC's oversight and review authorized under Section 702 does not constitute independent oversight sufficient to comport with Article 17 or related provisions of the ICCPR, either as an *ex ante* or *ex post* matter, since it reviews only general procedures, not targeting decisions, as described above.

V. The Applicability of US Obligations Under Human Rights Law

The US is obligated to comply with human rights law in conducting surveillance of people around the world. This obligation extends to all US surveillance irrespective of the nationality of its intended targets. Article 2(1) of the ICCPR provides that the government must "respect and ensure to all individuals within its territory and subject to its jurisdiction the rights recognized" in the treaty.[78] Thus, the US is responsible for violations of the right to privacy regardless of where the interference with privacy occurs and regardless of the nationality of the victim.

In the first part of this section, we explain that human rights obligations to protect privacy apply to surveillance conducted under Section 702 because all such surveillance takes place within US territory, even if it impacts the privacy rights of persons living outside US territory. The US is responsible for any privacy violations that may occur while conducting Section 702 surveillance because it exercises jurisdiction over the territory where the surveillance happens. In other words, the surveillance takes place on US soil.[79]

In the second part of this section, we explain that even if the US regards its surveillance under Section 702 as extraterritorial, ICCPR obligations still apply. According to the Human Rights Committee, Article 2(1) the ICCPR requires that "a State party must respect and ensure the rights laid down in the ICCPR to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party." [80] The International Court of Justice has adopted this same interpretation. [81] In relation to privacy rights, it is control over communications, not custody of the person, that is the touchstone of state responsibility under the ICCPR. Thus, obligations under the ICCPR apply to surveillance conducted under Section

[78] ICCPR, *supra* note 15, art. 2(1).

[79] 50 U.S.C. § 1881a(h)

[80] *See* General Comment 31, *supra* note 44.

[81] Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 111 (July 9).

702 where the US exercises "effective control" over the person's communications, that is, their right to privacy.

A. Territorial Surveillance

All surveillance conducted pursuant to Section 702, by definition, requires the assistance of telecommunications providers within US jurisdiction.[82] As such, Section 702 surveillance entails either the collection of information routed through the US or information stored on US territory. This is the case even if that information belongs to persons who are neither within the US or US persons. Privacy obligations apply because the interference (collection of private information) and potential rights violation physically occur within US territory.[83] These surveillance practices are the modern-day equivalent of searching, collecting, and opening international mail transiting through or stored on US territory. The fact that modern technology enables the clandestine searching, collection, and storage of millions of messages electronically, as opposed to the physical opening of specific items of mail, makes no difference to the ICCPR's application; both forms of surveillance constitute "interferences" within US territory and both are governed by Article 17.[84]

This territorial surveillance is possible because much of the world's telephone and Internet traffic is either routed through the US or stored on servers here.[85] According to one estimate, the US is the vehicle for or the home of 90 percent of this information.[86] Even seemingly local exchanges of information outside of the US actually take place on US soil. For example, the email conversations of two Yahoo mail users located in Egypt will most likely travel through and be stored in Yahoo mail servers in the US. Thus, any interference and potential violation of rights occurs within US territory because intelligence agencies' control of

[82] *See* 50 U.S.C. § 1881a(h).

[83] "Jurisdiction" under international law refers to the ability of a state to lawfully exercise its domestic authority over persons or property. *See* Sarah Cleveland, *Embedded International Law and the Constitution Abroad*, 110 Colum. L. Rev. 225, 231 (2010) (citing Antonio Cassese, International Law 49 (2d Ed. 2005)). The European Court has considered two surveillance/data cases where the interference was territorial while the impacted individual was outside of the territory. The first, *Weber and Saravia v. Germany*, was dismissed as manifestly ill-founded on the merits and so the Court did not address the jurisdictional question. Weber and Saravia v. Germany, App. No. 54934/00, Decision as to Admissibility, Eur. Ct. H.R. (Jun. 29, 2006). The second, *Liberty and Others v. the United Kingdom*, both the UK government and the Court assumed that the European Convention applied. Liberty and Others v. United Kingdom, App. No. 58243/00, Judgment, Eur. Ct. H.R. § 62 (Jul. 1, 2008). *See also* Milanovic, *supra* note 70.

[84] The ACLU and other civil liberties organizations have made the same argument regarding UK surveillance practices. *See* ACLU and Ors. v. Government Communications Headquarters, in the matter of a claim in the Investigatory Powers Tribunal under section 7 of the Human Rights Act of 1998 (on file with the ACLU).

[85] *See Global Internet Map 2012*, Telegeography, http://global-internet-map-2012.telegeography.com/ (last visited March 31, 2014).

[86] James Ball, *NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show*, The Guardian, Sept. 30, 2013, *available at* http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

personal data, through its collection, search, and storage takes place within the territorial jurisdiction of the US.

Surveillance that occurs within US territory but that has extraterritorial effects is not "extraterritorial" for the purposes of assessing US responsibility under the ICCPR.[87] Rights implicated in a physical search provide a helpful analogy: if a foreigner abroad held property in the US, and US agents illegally searched or seized that property, the search or seizure would give rise to rights and obligations under the ICCPR, despite the owner's location. [88]

B. Extraterritorial surveillance

Even surveillance that the US regards as extraterritorial—either because the persons subject to surveillance are located outside US territory or because the communication collected is neither routed through the US or stored on US territory—triggers US human rights obligations under the ICCPR where the US exercises power or effective control over a targeted person's communications. Any government that exercises power or effective control over personal information is bound by the ICCPR; there can be no question that the US, particularly in view of its predominating control of the global information infrastructure and its powerful surveillance capacities, exercises the degree of control necessary to satisfy this long-recognized standard.

1) The "Effective Control" Test

The Human Rights Committee and all other major international bodies that have considered the extraterritorial scope of human rights obligations have concluded that a state's extraterritorial exercise of effective control over a person or a territory places that conduct within a state's "jurisdiction."[89] In applying obligations extraterritorially, none of these institutions have

[87] Thus, in *Andreou v Turkey*, the European Court held that, "even though the applicant had sustained her injuries in territory over which Turkey exercised no control, the opening of fire on the crowd from close range, which was the direct and immediate cause of those injuries, had been such that the applicant should be regarded as 'within [the] jurisdiction' of Turkey within the meaning of Article 1 of the Convention." Andreou v. Turkey, App. No. 45653/99, Judgment, Eur. Ct. H.R. (Oct. 27, 2009).

[88] For example, in *Bosphorous Hava Yollari Turizm Ve Ticaret Anonim Sirketi v Ireland*, the European Court of Human Rights held that the seizure in Ireland of an airplane belonging to the applicant, who did not reside within Ireland, meant that the state had jurisdiction over the applicant and was therefore accountable for potential violations. *See* Bosphorous Hava Yollari Turizm Ve Ticaret Anonim Sirketi v Ireland, App. No. 45036/98, Judgment, Eur. Ct. H.R. (Jun. 30, 2005).

[89] For the Human Rights Committee, *see* General Comment 31, *supra* note 44, ¶ 10. In at least thirteen other instances the Committee has upheld the extraterritorial application of the ICCPR, *see* Letter from Amnesty International to Office of the High Commissioner for Human Rights, AI Index: ACT 30/003/2014 (Apr. 1, 2014), *available* at http://www.amnesty.org/en/library/info/ACT30/003/2014/en. For the ICJ, *see* Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 111 (July 9); *see also*, Armed Activities on Territory of Congo (Dem. Rep. Congo. v. Uganda), 2005 I.C.J. 168, 234 (Dec. 19). For regional human rights bodies *see* Al-Skeini and Others v. United Kingdom, App. No. 55721/07, Judgment, Eur. Ct. H.R. (Jul. 7, 2011); Issa and Others v. Turkey, App. No. 31821/96, Judgment, Eur. Ct. H.R. (Mar. 30, 2005); Őcalan v. Turkey, App. No. 46221/99, Judgment, Eur. Ct. H.R. ¶¶ 91, 190 (May 12, 2005); Ilascu and Others v. Moldova and Russia, App. No. 48787/99, Judgment, Eur. Ct. H.R. ¶ 311 (Jul. 8, 2004);Victor Saldaño v. Argentina, Inter-

drawn a bright line distinction between responsibility over citizens and non-citizens, recognizing that in a modern world of instant global communications, categorical restrictions based on territory or alienage are unworkable.[90]

Since 1995, the US government has taken a contrary view.[91] As then-State Department Legal Adviser Harold Koh noted in a 2010 memo, it is not a long-standing position.[92] It is also counter to the "consistent interpretation" of the ICCPR, as the US government expressly recognized in 2011.[93] In his 2010 memo, Koh concluded that the 1995 interpretation was "no longer tenable." Noting that the US position had been "a source of ongoing international tension, with significant deleterious effects on our international human rights reputation and our ability to promote international human rights internationally,"[94] Koh set forth a jurisdictional test broadly consistent with international law and practice: "[A] state is obligated to respect *rights under its control* in circumstances in which the State exercises authority or *effective control over a particular person or context*" (emphasis added).[95]

Koh's position also conforms with the animating principle for extraterritorial application of human rights obligations: that it "would be unconscionable to so interpret the responsibility under article 2 of the ICCPR as to permit a State party to perpetrate violations of the ICCPR on

---

Am. Ct. H.R., Petition, Report No. 38/99 ¶ 18 (Mar. 11, 1999).; s*ee also* Coard v. United States, Case 10.951, Inter-Am. Comm'n H.R., Report No. 109/99, OEA/Ser.L/V/II.106, doc. 3 rev. ¶ 37 (1999) (suggesting that the important issue is not the victim's nationality or presence within "a particular geographic area" but whether under the circumstances the state observed rights of those subject to its "authority and control"); Armando Alejandre Jr. and Others v. Cuba ('Brothers to the Rescue'), Case 11589, Inter-Am. Comm'n H.R., Report No. 86/99 at (1999).

[89] Cleveland, *supra* note 83, 248.

[90] *Id.*

[91] In 1995, in a brief oral response to a question regarding the geographic scope of the Covenant during the United States' Initial Report to the Human Rights Committee, then-Legal Adviser Conrad Harper stated, "[t]he Covenant was not regarded as having extraterritorial application." *See* U.N. Human Rights Comm., 53rd Sess., 1405th mtg., U.N. Doc. CCPR/C/SR 1405 (April 24, 1995). The US government subsequently took the position that it was obligated to recognize Covenant rights only for "individuals who are both within the territory of a State Party and subject to that State Party's sovereign authority," i.e. "exclusively within the territory" of the United States. U.N. Human Rights Comm., *Consideration of Reports Submitted by State Parties Under Article 40 of the Covenant, Third Periodic Reports of States Parties Due in 2003: United States of America*, Annex I, U.N. Doc. CCPR/C/USA/3 (Nov. 28, 2005); U.S. Dep't of State, *List of Issues to be Taken Up in Connection with the Consideration of the Second and Third Periodic Reports of the United States of America*, Question 4 (July 17, 2006).

[92] Prior to 1995 both Executive branch and Senate officials operated with the understanding that the ICCPR applied extraterritorially, at least with regard to the obligation to "respect" rights. *See* Memorandum Opinion from the Office of the Legal Adviser of the U.S. Dep't of State on the Geographic Scope of the International Covenant on Civil and Political Rights (October 19, 2010), *available at* http://justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf.

[94] *Id.*

[95] *Id.*

the territory of another State, which violations it could not perpetrate on its own territory."[96] Even more fundamental is the concept that human rights do not 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."[97]

2) Applying the "Effective Control" Test to Privacy

The effective control test is not limited to cases of physical custody or control. Rather, the determining factor is the nature of the right protected.[98] Thus the right to liberty depends to a large extent on custody or power over the individual.[99] However, for obligations to apply in relation to other rights, such as the right to life,[100] the right to property[101] and non-discrimination[102] there is no custodial requirement. A state can interfere and potentially violate these rights without physical custody—for example, a State may exercise power over right to life (the ability to arbitrarily kill a person) or the power to expropriate property.[103]

---

[96] Sergio Euben Lopez Burgos v. Uruguay, Communication No. R.12/52, ¶ 12.3, U.N. Doc. Supp. No. 40 (A/36/40) at 176 (1981).

[97] Milanovic, *supra* note 70.

[98] *See* Manfred Nowak, *What does extraterritorial application of human rights treaties mean in practice?*, JustSecurity (Mar. 11, 2014, 8:06 AM), http://justsecurity.org/2014/03/11/letter-editor-manfred-nowak-extraterritorial-application-human-rights-treaties-practice/ (stating that "[a] correct interpretation of "effective control" over a person must […] take the specific right at issue into account").

[99] *Id.*

[100] *See* European Court of Human Rights in *Issa v. Turkey*, App. No. 31821/96, Judgment, Eur. Ct. H.R. (Mar. 30, 2005) (concerning the killing of Iraqi shepherds by Turkish military forces in Iraq); *Pad and others v Turkey*, Eur. Ct. H.R., App. No. 60167/00, ¶¶ 53-55 (June 28, 2007). In *Pad*, some Iranian nationals had been killed by fire from Turkish helicopters, and Turkey was found to have jurisdiction. Whether the events had occurred on the Iranian or Turkish side of the border remained in dispute, but the Court decided that it was not necessary to determine the exact location, as Turkey had already admitted that its forces had caused the killings by firing upon the victims from helicopters. This decision contradicts the Court's decision in *Bankovic*, where it found that jurisdiction did not apply in similar circumstances. *See* Bankovic et al. v. Belgium et al., App. No. 52207/99, Grand Chamber Decision, Eur. Ct. H.R. (Dec. 12, 2001).

[101] For example in *Bosphorous Hava Yollari Turizm Ve Ticaret Anonim Sirketi v. Ireland*, the European Court of Human Rights held that the seizure in Ireland of an airplane belonging to the applicant, who did not reside within Ireland, meant that the state had jurisdiction over the applicant and was therefore accountable for potential violations. Sirketi v. Ireland, *supra* note 88.

[102] See for example *Gueye et al. v. France*, in which the Human Rights Committee found a violation of ICCPR article 26 (nondiscrimination) when France had enacted legislation that provided for the same service in the French military a lower pension to retired Senegalese soldiers living in Senegal than it provided to Frenchmen living in France (or even living in Senegal). The act of legislating occurred in France but its discriminatory effect was felt by beneficiaries of French pensions living in Senegal. Gueye et al. v. France, U.N. Human Rights Comm., Communication No. 196/1985, U.N. Doc. CCPR/C/35/D/196/1985 (1989).

[103] *See also* Montero v Uruguay, U.N. Human Rights Comm., Communication No. 106/1981, U.N. Doc CCPR/C/OP/2 (1983); Mbenge v Zaire, U.N. Human Rights Comm., Communication No. 16/1977, U.N. Doc CCPR/C/OP/2 (1983).

Another example is fair trial guarantees and trials *in absentia*. Even though the defendant is absent during trial—even outside the country—a state is still obligated to provide the defendant with a fair trial. The right to a fair trial applies not because the person is in the government's physical control, but because the government has exerted control over the person in subjecting them to criminal trial.[104]

The Human Rights Committee,[105] the Inter-American Commission on Human Rights,[106] African Commission on Human Rights,[107] UN Committee on the Elimination of Racial Discrimination,[108] and the UN Committee on the Elimination of Discrimination against Women,[109] have all applied their respective human rights instruments to situations in which a State did not have control over territory or physical custody over persons, but rather over the rights at issue.[110]

Here, the question is not whether US surveillance establishes effective control over a person, but whether US authorities exercise effective control over a person in relation to their right to privacy.[111] Indeed, the UN Human Rights Committee considered US surveillance practices in its March 2014 review of US compliance with the ICCPR and applied this same test,

[104] As one scholar has explained in relation to privacy rights: "If virtual methods can in principle exact the same exact result as physical ones, then there seems to be no valid reason to treat them differently and insist on some kind of direct corporeal interventions." Milanovic, *supra* note 70, 58.

[105] *See* Gueye et al. v. France, *supra* note 102.

[106] *See* Armando Alejandre Jr. and Others v. Cuba *('Brothers to the Rescue')*, *supra* note 89; Saldaño v Argentina, *supra* note 89 (holding that, 'a state party to the American Convention may be responsible *under certain circumstances* for the acts and omissions of its agents which produce effects or are undertaken outside that state's own territory.').

[107] African Comm'n. H.R., *Association Pour la Sauvegarde de la Paix au Burundi v Tanzania, Kenya, Uganda, Rwanda, Zaire and Zambia (2003-2004)*, ¶ 75, Communication No. 157/96 (2003). In that case, the Commission examined whether States imposing the sanctions on Burundi were compliant with the African Charter, even though they had no territorial control or presence in Burundi.

[108] UN Committee on the Elimination of Racial Discrimination, Concluding Observations: United States of America (2008) U.N. Doc. CERD/C/USA/CO/6, ¶ 30.

[109] UN Committee on the Elimination of Discrimination Against Women, *General Recommendation 28 on the Core Obligations of States Parties under Article 2*, U.N. Doc CEDAW/C/GC/28 (2010) ("States parties are responsible for all their actions affecting human rights, regardless of whether the affected persons are in their territory.")

[110] Similar findings by the Committee on Economic, Social and Cultural Rights and the Committee on the Rights of the Child are not listed here as those extraterritorial obligations are partially founded on obligations of international cooperation and assistance contained in the relevant treaties.

[111] As Manfred Nowak, a former UN expert and leading authority on the Covenant, explains: "The real test of "effective control" in the case of surveillance and data protection is not whether the person is under the direct control (custody) of foreign agents, but whether the correspondence and communications under direct control, which is the case with any surveillance measure." *See* Nowak, *supra* note 98.

calling on the US " to ensure that its surveillance activities, *both within and outside the United States*, conform to its obligations under the ICCPR, including article 17" (emphasis added).[112]

Control of the global communications infrastructure is certainly not a prerequisite to a state's exercise of "effective control." We note, however, there can be no doubt that US surveillance practices satisfy the "effective control" test in light of how expansive they are in type, scale and duration. The extent of US control over communications means that it can obtain as much personal data from an individual target using electronic surveillance as it can if it had physical control over that target. Indeed US digital surveillance capabilities are now so powerful that a US agent who kidnapped an individual abroad and searched all of their possessions, including their mobile phone and laptop, would likely obtain less information that than the US government could access and obtain through remote digital surveillance.

As one scholar explains: "The extended duration and seamlessness of U.S. control in the virtual sphere constitute an ongoing state presence that is in some ways more pervasive than states' dominance within their physical territory."[113] This point was recently underscored by reports that the NSA has allegedly built a surveillance system capable of recording "100 percent" of a foreign country phone calls, enabling the agency to rewind and review conversations a month after they take place.[114]

VI. Recommendations

The ACLU and Amnesty International USA urge the Privacy and Civil Liberties Oversight Board to recommend the repeal of Section 702 of the FISA Amendments Act. As the ACLU explained in its March 19, 2014 submission to PCLOB, Section 702 is unconstitutional.[115] Moreover, as Amnesty International USA and the ACLU have explained in this submission, Section 702 permits arbitrary and unlawful interferences with the right to privacy in violation of international human rights law. In sum, Section 702 violates international obligations to protect privacy guaranteed by Article 17 of the ICCPR for the following reasons:

[112] U.N. Human Rights Comm., Concluding Observations on the United States, *supra* note 26, ¶ 22.

[113] Peter Margulies, The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism (Jan. 23, 2014) (unpublished research paper, Roger Williams University), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2383976.

[114] Barton Gellman and Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, Wash. Post, March 18, 2014, *available at* 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.

[115] Jaffer, *supra* note 8.

- **Public Transparency**: Section 702 fails to establish clear and precise limitations on the scope of surveillance authority granted; to the contrary, it provides broad and effectively unfettered discretion to US authorities to conduct surveillance;
- **Proportionality and Necessity:** Section 702 permits the collection and storage of personal data, including of "about-the-target" communications. This involves the copying and scanning of virtually any message entering or leaving the US), without any consideration of the danger to national security posed by the intended target.
- **Independent oversight and redress**: The FISC reviews only general procedures, not specific targeting decisions, making its review wholly inadequate under the ICCPR.
- **Non-discrimination:** Section 702 denies any protection whatsoever to non-US persons outside the US, apparently based solely on the flawed premise that the US government does not owe any privacy protections to non-US persons—a premise that the President has recently rejected.

At the very least, Section 702 should be amended to prohibit surveillance without individualized suspicion and prior review by a competent, independent and impartial tribunal. Section 702 should also provide strict limitations on the scope and duration of surveillance, and use, retention and dissemination of personal communications. The definition of "foreign intelligence information" should be amended and strictly limited to, for example, information pertaining to espionage or national security.

The ACLU and Amnesty International USA also recommend that the Executive Branch disclose the legal authority and scope of all signals intelligence practices of non-US persons outside of US territory. All signals intelligence collection—regardless of nationality or the location of individuals—should be authorized in a publicly accessible law setting out the potential scope and duration of surveillance, rather than by secret executive orders or other non-accessible rules. At the very least, the President should direct the disclosure of a meaningful unclassified description of the targeting procedures used in collecting communications under Section 702. The President should also direct the release of executive memoranda and FISC opinions interpreting Section 702, with only those redactions necessary to protect legitimately secret information.

The ACLU and Amnesty International USA urge that all branches of the US government recognize and adhere to US human rights obligations with regard to surveillance operations that impact people across the world. Any surveillance measure must comport with international law, and human rights protections should not be denied solely on the basis of nationality. Section 702 fails to provide any protection to non-US persons outside US territory and US law should be changed to reflect, at minimum, the necessary protections required by international law. Notwithstanding the US official position on extraterritorial application of international human rights law generally and obligations to respect privacy specifically, the Executive Branch should, as a matter of policy, commit to meeting human rights

standards protecting the rights to privacy and freedom of expression and opinion as it conducts surveillance inside and outside of US territory.

We appreciate the opportunity to present our views to PCLOB as it formulates its findings and recommendations to protect privacy and human rights. We look forward to further collaboration with you. For more information, please contact Naureen Shah (nshah@aclu.org) at the ACLU and Zeke Johnson (zjohnson@aiusa.org) at Amnesty International USA.