Comments of Human Rights Watch

Privacy and Civil Liberties Oversight Board Hearing - March 19, 2014
"The Surveillance Program Operated Pursuant to Section 702 of the
Foreign Intelligence Surveillance Act"

Human Rights Watch welcomes the opportunity to participate in the Privacy and Civil Liberties Oversight Board (PCLOB) evaluation of US surveillance practices under Section 702 of the FISA Amendments Act (FAA). Human Rights Watch is an independent global organization with a presence in more than 90 countries working to promote respect for and adherence to human rights obligations around the world. We have been asked to comment specifically on how surveillance practices under Section 702 affect the rights afforded non-US persons under the International Covenant on Civil and Political Rights (ICCPR) or any other legal authorities as well as how our analysis may translate into any policy recommendations. We therefore offer the following analysis, which focuses first on the extraterritoriality of US obligations under the ICCPR, then on the right to privacy under the Covenant, and finally on the application of international principles to Section 702.

I. Extraterritoriality of US Obligations under the International Covenant on Civil and Political Rights (ICCPR)

For years, the United States has taken the position that its obligations under the ICCPR, a treaty to which it is a party, do not apply extraterritorially. Its position is based on a very limited reading of a clause in Article (2)(1) of the treaty, which states:

> Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind …[1]

[1] International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force Mar. 23, 1976, (hereinafter ICCPR), http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (accessed March 15, 2014.)

The US interprets this language to mean that it has obligations under the treaty only if the relevant individuals are *both* within its territory *and* subject to its jurisdiction. It has claimed that this is the long-standing position of the US dating back to the days of the treaty's drafting after World War II[2] when the US proposed to modify the original language from "within its jurisdiction" to "within its territory and subject to its jurisdiction."[3]

But in recent years, several scholars have challenged the notion that this is in fact the long-standing position of the US. Instead, they argue that it only developed rather recently, after the US ratified the ICCPR in 1992 and in the context of the 1994-1995 intervention in Haiti.[4] They have also argued that it is not at all clear from the fact that the US pushed for the modification to Art. (2)(1) that it intended to do so in order to avoid all extraterritorial obligations but rather only avoid *some* obligations that would have been impossible to *ensure*.[5] Additionally, they argue that the text itself is subject to three different interpretations, all of which are grammatically correct, but the latter two of which would call for extraterritorial application of ICCPR obligations by state parties. It was recently revealed that one of these scholars was former US State Department Legal Advisor Harold Koh who, as Legal Advisor in 2010, issued a Memorandum Opinion advising that the US should reverse its position on ICCPR extraterritoriality because it was based on an inaccurate reading of the ICCPR drafting and negotiating history and not compelled by a proper reading of the text.[6]

---

[2] Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," (forthcoming, will be available at http://www.ssrn.com/en/ and on file with Human Rights Watch), p. 26, n. 68, *citing* "Cable on the US Mission to Geneva to the US Secretary of State," No. 001769, July 2006, http://www.state.gov/documents/organization/131739.pdf (accessed March 10, 2014), para. 12.

[3] Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 27.

[4] Ibid., p. 27-32; See also: Michael J. Dennis, "Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation," *American Journal of International Law*, vol. 99, no. 1, (January, 2005), p. 123-124; Beth Van Schaack, "The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change," *International Law Studies, U.S. Naval War College*, vol. 90, (2014), http://www.usnwc.edu/getattachment/a88e97e5-11ec-4dfb-a013-4cfa5f8efe5a/The-United-States--Position-on-the-Extraterritoria.aspx (accessed March 9, 2014), p. 29-31; Peter Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism," *Fordham Law Review*, (forthcoming), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2383976 (accessed March 8, 2014), p. 6-7.; Manfred Nowak, *U.N. Covenant on Civil and Political Rights CCPR Commentary*, (Kehl Am Rhein, Germany: N.P. Engel, 2d rev. ed. 2005), p. 44.

[5] Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism," *Fordham Law Review*, p. 7; Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 28.

[6] Charlie Savage, "U.S. Seems Unlikely to Accept That Rights Treaty Applies to Its Actions Abroad," *New York Times*, March 6, 2014, http://www.nytimes.com/2014/03/07/world/us-seems-unlikely-to-accept-that-rights-treaty-applies-to-its-actions-abroad.html (accessed March 10, 2014); Memorandum Opinion on the Geographic Scope of the International Covenant On Civil and Political Rights from Harold Hongju Koh, former Legal Adviser of the Department of State, to the Office of the Legal

Regarding the long-standing position, it appears that the first time the US clearly articulated its position that the ICCPR cannot be applied extraterritorially was in March 1995, at the time of the U.S. review before the Human Rights Committee.[7] In response to a question from a member of the committee,[8] the U.S. articulated a position that was based, for the most part, upon a plain reading of the text and an articulation of the belief that during the negotiating history the words "within its territory" had been added "with the clear understanding that such wording would limit the obligation to within a Party's territory."[9]

However, a closer look at the drafting history reveals that when Eleanor Roosevelt, the chief delegate to the United Nations during the initial drafting of the ICCPR, suggested the US add the words "within its territory," it was not necessarily to avoid entirely extraterritorial obligations under the treaty. Rather, it was intended to avoid the US having to undertake obligations to ensure rights to individuals in territories the US was occupying at the time, such as Germany and Japan after World War II. The US feared it would not have the capacity to ensure certain rights, such as protecting individuals against third parties or enacting legislation on behalf of citizens of the states they were occupying.[10] In fact, the drafting history shows that in debates over wording, the US acknowledged that "troops, although maintained abroad, remained under the jurisdiction of the State," something that scholars point to as strongly suggesting that the US conceded responsibility for the acts of its own personnel in the country of occupation.[11] Further, when the US ratified the treaty in 1992, the US Senate made several declarations and understandings, but none regarding extraterritorial application.[12] Nor did it raise the issue in its initial report to the Human

---

Adviser, October 19, 2010 (hereinafter "Koh memo"), http://www.nytimes.com/interactive/2014/03/07/world/state-department-iccpr.html?_r=0 (accessed March 10, 2014).

7 The Human Rights Committee is the body established under article 28 of the ICCPR that receives States Parties reports, issues authoritative General Comments interpreting the treaty's provisions, and adjudicates individual petitions brought under either the first or second Optional Protocols to the ICCPR. It is also mandated to adjudicate intra-State complaints under article 41 of the ICCPR.

8 Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 29; Koh memo, p. 1.

9 Ibid.

10 Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism," *Fordham Law Review*, p. 7; Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 28; Koh memo, p. 15.

11 Margulies, "The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism," *Fordham Law Review*, p. 7-8; Sarah H. Cleveland, "Embedded International Law and the Constitution Abroad," *Columbia Law Review*, vol. 110, (2010), p. 252, n.111.

12 Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 29; Van Schaack, "The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change," *International Law Studies, U.S. Naval War College*, p. 31, n. 34.

Rights Committee despite the fact that the Committee's first case finding that the Covenant applies extraterritorially predated both the report and the US ratification.[13]

The Vienna Convention on the Law of Treaties (VCLT), which the US recognizes as the guiding authority on treaty interpretation, requires that the language of a treaty "shall be interpreted 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."[14]

Regarding the "ordinary meaning," there are at least three ways Art. (2)(1) of the ICCPR can be interpreted, all of which are grammatically plausible. The first is to read the "and" in the phrase "to all individuals within its territory and subject to its jurisdiction" as conjunctive. This would result in the narrow interpretation the US has adopted. The second would be to read the "and" in the disjunctive to mean that parties to the Covenant must respect and ensure the rights recognized under the Covenant to all individuals within its territory, *as well as to* all individuals within its jurisdiction.[15] This would be a more expansive interpretation, more protective of rights.

The Human Rights Committee adopted this second disjunctive interpretation in 2004 in its General Comment 31. "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." Further, it defined "jurisdiction" within Art. 2(1) to mean "power or effective control." The same paragraph goes on to read: "[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."[16] Further, as the Human Rights Committee put it in *Lopez-Burgos*—a case dealing with the abduction by Uruguayan agents of an individual on Argentine territory: "[I]t would be unconscionable to … interpret the responsibility under article 2 of the Covenant as to

---

[13] Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 29.

[14] Vienna Convention on the Law of Treaties (VCLT), adopted May 23, 1969, UN Doc. A/Conf.39/27/1155 UNTS 331/8 ILM 679 (1969)/63 AJIL 875, Article 31(1), entered into force January 27, 1980, https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf (accessed March 10, 2014).

[15] Cleveland, "Embedded International Law and the Constitution Abroad," *Columbia Law Review*, p. 252.

[16] UN Human Rights Committee, General Comment No. 31, "Nature of the General Legal Obligation Imposed on States Parties to the Covenant," UN Doc. CCPR/C/21/Rev.1/Add. 13 (2004), May 26, 2004, para. 10, http://www.unhchr.ch/tbs/doc.nsf/0/58f5d4646e861359c1256ff600533f5f (accessed March 10, 2014).

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."[17]

The International Court of Justice (ICJ) agreed that there could be two interpretations but ultimately also adopted the second, more expansive, interpretation using the disjunctive language:

> 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. ... while the jurisdiction of States is primarily territorial, it may sometimes be exercised outside the national territory. Considering the object and purpose of the International Covenant on Civil and Political Rights, it would seem natural that, even when such is the case, States parties to the Covenant should be bound to comply with its provisions. ...the 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.[18]

Finally, there is yet a third interpretation that has garnered more attention in recent years that is somewhat different from the reading that both the HRC and the ICJ have adopted. This would interpret Art. (2)(1) in a way that would make a clearer distinction between the obligation to "respect" —a negative obligation to refrain from acting or infringing on certain rights, and the obligation to "ensure" —a more positive obligation that entails specific, proactive measures. Under this interpretation, the limiting clause "within its territory and subject to its jurisdiction" modifies only the obligation "to ensure" to which it is appended, not the obligation to "respect." It would mean a "State Party would undertake 'to respect' Covenant obligations by refraining from infringing protected rights, but undertake 'to ensure' Covenant rights only to persons who are both 'within its territory and subject to its jurisdiction.'"[19]

---

[17] UN Human Rights Committee: *Lopez-Burgos v. Uruguay*, Communication, UN Doc. CCPR/C/13/D/52/1979, July 19, 1981, para. 12.3, http://www.unhchr.ch/tbs/doc.nsf/0/e3c603a54b129ca0c1256ab2004d70b2?Opendocument (accessed March 10, 2014).

[18] Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, ICJ Reports 136, July 9, 2004, para. 108, 109, 111, http://www.icj-cij.org/docket/files/131/1671.pdf (accessed March 6, 2014).

[19] Koh memo, p. 8; Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 32; Cleveland, "Embedded International Law and the Constitution Abroad," *Columbia Law Review*, p. 252, *citing* Nowak, *U.N. Covenant on*

Harold Koh and other scholars argue that this third interpretation is the best reading of the treaty.[20] In his recently leaked 2010 memorandum, Koh made the argument most extensively laying out five different reasons for why this third interpretation is the best and most accurate from the point of view of grammatical coherence, the assumption against redundancy, and most important, the need to read each part of a treaty in line with its object and purpose:[21]

To read the key passage conjunctively, Koh argues, would produce "absurd" results and would "flout[] the animating purpose of post-World War II human rights regime, which was to develop legal tools to respond effectively to Nazi and other atrocities."[22] Marko Milanovic, lecturer in law at the University of Nottingham School of Law who writes extensively on these issues, calls this the "Auschwitz rule." Surely the drafters of the Covenant, "could not possibly have intended to create a human rights treaty which would not be violated by the deliberate extermination of a million Jews in Auschwitz. Make no mistake: this would indeed be the consequence of the absolutist position that the ICCPR can *never* apply extraterritorially, and thus not even to Nazi-occupied Poland in which the death camp was located."[23] It also would "yield the bizarre result that a state that was obligated to protect citizens within its borders could act against those same citizens with impunity under the Covenant, the moment they stepped outside the state's borders."[24]

The United Nations Human Rights Committee, in its General Comment 31, underscores that the Covenant's rights are *erga omnes* in character, that is, all States Parties to the Covenant have an interest in the performance and respect of Covenant rights by all other States Parties. This understanding of the wide scope of the duty to respect is in accord with both the Human Rights Committee's understanding of State obligations under the ICCPR, and the UN Charter, both of which affirm the universal obligation to promote and encourage "respect" for human rights. To that end, when a state acts not to promote respect for rights, but rather to violate them or undermine the ability of another state to protect its inhabitant's rights, it violates this fundamental purpose.

Civil and Political Rights CCPR Commentary, p. 43-44 ("The obligation of a State party to ensure the rights of the Covenant relates to all individuals 'within its territory and subject to its jurisdiction' ....").

[20] Koh memo, p. 8.

[21] Ibid., p. 9-15.

[22] Ibid., p. 12.

[23] Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 35.

[24] Koh memo, p. 13.

Nevertheless, the US has consistently since 1995 taken the position that its obligations under the ICCPR do not apply extraterritorially in any context or under any circumstances, while failing to articulate any compelling response to the arguments. In written responses, in July 2013, to questions from the HRC about the US position on the question of extraterritoriality, the United States referred the HRC to an earlier submission on the issue in its Fourth Periodic Report to the Committee. "With respect to the scope of applicability of the ICCPR, the United States refers the Committee to ¶¶ 504 – 510 of its Fourth Periodic Report."[25] The relevant portion of those parts of paragraphs of the report simply states the US's prior position even though it notes the US is aware that the HRC in General Comment 31 and the ICJ had both interpreted Art.(2)(1) to require States Parties to respect and ensure Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction.[26] The position was reiterated by the US before the Human Rights Committee on March 13, 2014 as well.[27]

Indeed, the US is nearly alone, internationally, on this issue. In addition to the HRC, the ICJ, a number of other States Parties, including some of the US's closest allies including Australia, Belgium, Germany, the Netherlands and the United Kingdom, have formally acknowledged to the Committee that they accept some extraterritorial reach for the Covenant, including with respect to military activities in Iraq and Afghanistan.[28] Apparently Israel is the only other country that has offered a strictly territorial reading of the Covenant's scope before the HRC.[29] According to Koh, this position has "been a source of ongoing international tension" with "significant deleterious effects on [the US'] international human rights reputation and [] ability to promote international human rights internationally.[30]

---

[25] US State Department, "United States Written Responses to Questions From the United Nations Human Rights Committee Concerning the Fourth Periodic Report," July 3, 2013, para. 2, http://www.state.gov/j/drl/rls/212393.htm (accessed March 10, 2014).

[26] US State Department, Fourth Periodic Report of the United States of America to the United Nations Committee on Human Rights Concerning the International Covenant on Civil and Political Rights, December 30, 2011, http://www.state.gov/j/drl/rls/179781.htm (accessed March 10, 2014).

[27] Charles Savage," U.S., Rebuffing U.N., Maintains Stance That Rights Treaty Does Not Apply Abroad," New York Times, March 13, 2014, U.S., http://www.nytimes.com/2014/03/14/world/us-affirms-stance-that-rights-treaty-doesnt-apply-abroad.html?_r=0 (accessed March 15, 2014).

[28] Cleveland, "Embedded International Law and the Constitution Abroad," *Columbia Law Review*, p. 255-56, n. 124. See also Koh memo, p. 32-49.

[29] Koh memo, p. 32.

[30] Ibid., p. 4.

From a technological standpoint, there are very good policy reasons why the US should reject this narrow interpretation of extraterritoriality, including with regard to privacy rights. Data flows over the internet are not based on geography but on the technical parameters that are most efficient and the route data will take can be unpredictable.[31] The structure of the internet and the advent of cloud computing means that even a transfer to a party in the same country may result in the message or file transiting via other countries without the sender ever being aware.[32] Thus, a failure to recognize the obligation to respect the right to privacy extraterritorially exposes US data to vulnerability when it is situated in the territory of other states—a situation the average US citizen faces daily. Additionally, the technological complexity and the effort required to track data sent over the Internet means that it may no longer even be feasible to differentiate between trans-border data flows and those that do not cross national borders.[33]

Concepts of jurisdiction based on control over territory and persons—and the human rights obligations necessarily entailed—can and should adapt to the reality of mass digital surveillance, which can produce the reality of control even through remote means. A government can now easily violate the privacy of an individual without having physical control over that person, and without that person being located inside an area under its control because a government may have power or effective control over the individual's communications (or over the company that stores or transmits them). Unjustified surveillance of individual communications, moreover, may open the way to violation of other rights, among them freedoms of expression, association, and many other potentially severe abuses.

For this reason, the UN Special Rapporteur on the right to freedom of expression, in his April 2013 report to the Human Rights Council, expressed alarm that a number of States, including the US, which had renewed the FISA Amendment Act in 2012, had adopted laws authorizing the conduct of extraterritorial surveillance to intercept communications in foreign jurisdictions. "This raises serious concern with regard to the extra-territorial commission of human rights violations and the inability of individuals to know that they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance, or seek remedies."[34] The US has a unique position within the Internet's

---

[31] Christopher Kuner, *Transborder Data Flows and Data Privacy Law*, (Oxford: Oxford University Press, 2013), p. 6.

[32] Ibid., p. 3.

[33] Ibid., p. 6.

[34] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/23/40, April 17, 2013.

infrastructure and therefore arguably has "effective control" over the communications and intimate details of millions of US and non-US persons as they flow through US-based networks or data centers. That capability to control such integral aspects of individual personality (in the sense of human agency, self-determination, and dignity) confers extraterritorial obligations with respect to the rights enumerated in the ICCPR, among them privacy, freedom of association, and freedom of information and expression. We also note that the US's position under Articles 2 and 17 is in tension with the US's own interpretation of its jurisdiction under the USA PATRIOT Act and other surveillance laws. Under the USA PATRIOT Act, the US asserts jurisdiction over any data held by companies based in the US, regardless of where that data may be physically stored.[35] In effect, the US asserts its jurisdictional control over data located outside the US, even as it argues that it is not responsible for any interference with privacy that results.

The potentially massive scale of surveillance of individuals outside US territory would have been inconceivable in the pre-Internet era. At the same time, in both law and practice, specifically under section 702, the US provides significantly weaker protections for the right to privacy for "non-US persons."[36] US persons are protected no matter where they are situated, while non-US persons lose protections when outside US borders.[37]

II. The Right to Privacy

---

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed February 10, 2014), para. 64. Special Rapporteurs are generally highly regarded legal experts that hold an independent mandate from the UN Human Rights Council to examine, monitor and report on specific global rights issues or conditions in particular countries. Their findings and recommendations often form the basis of action by the Human Rights Council and other bodies of the United Nations.

[35] See Alex C. Lakatos, "The USA Patriot Act and the Privacy of Data Stored in the Cloud," January 18, 2012, http://www.mayerbrown.com/publications/The-USA-Patriot-Act-and-the-Privacy-of-Data-Stored-in-the-Cloud-01-18-2012 (accessed February 10, 2014).

[36] FISA Amendments Act, 50 U.S.C. § 1881a. Under US law, "US Person" refers to citizens of the United States, aliens lawfully admitted for permanent residence, an unincorporated association with a substantial number of members who are citizens of the US or are aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the US. Foreign Intelligence Surveillance Act, 50 USC 1801(i).

[37] FISA Amendments Act, 50 U.S.C. § 1881a(b)-(d), EO12333. On January 17, 2014, US President Obama released Presidential Policy Directive 28 on signals intelligence activities, which provides for some greater protection on the retention and dissemination of information of data collected on non-US persons abroad. However, the directive does little to limit the scope of collection in the first place and excludes so-called "targeted collection." In view of the ICCPR obligation to respect rights of those individuals within a State Party's effective control without distinction, including as to nationality, the unequal treatment of non-citizens outside the territory of the U.S. but within the scope of U.S. mass communications acquisition is suspect under international law. See ICCPR, arts. 2.1 and 26.

Surveillance by the government can be conducted in a way that comports with human rights law. Restrictions on rights are permissible but "[w]here such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right."[38]

The right to privacy is articulated in Article 17 of the ICCPR, which states:

> (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.[39]

The Human Rights Committee expanded on the terms "unlawful" and "arbitrary" in its General Comment 16. In that comment, the HRC made clear that States may interfere with privacy, but any such interference with the right to privacy must be both lawful and non-arbitrary. For it to be lawful, it must not only be envisaged by law, but the law in question must comply with the provisions, aims and objectives of the Covenant. Additionally, it must "specify in detail the precise circumstances in which such interferences may be permitted" to allow people to foresee when their conduct might be regulated. For this reason, laws that are secret or convey excessive discretion in their application would not meet the standard. The requirement that a law not be arbitrary means it "should be in accordance with the provisions, aims and objectives of the Covenant and …. reasonable in the particular circumstances."[40] The Committee added: "Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de

---

[38] UN Human Rights Committee, General Comment No. 31, "Nature of the General Legal Obligation Imposed on States Parties to the Covenant," UN Doc. CCPR/C/21/Rev.1/Add. 13 (2004), May 26, 2004, para. 6, http://www.unhchr.ch/tbs/doc.nsf/0/58f5d4646e861359c1256ff600533f5f (accessed March 10, 2014).

[39] ICCPR, adopted December 16, 1966, G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force Mar. 23, 1976, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (accessed March 15, 2014.).The Universal Declaration of Human Rights contains virtually identical language. Universal Declaration of Human Rights (UDHR), adopted December 10. 1948, G.A. Res. 217A(III), U.N. Doc A/810 at art. 12(x) (1948).

[40] UN Human Rights Committee, General Comment No. 16, "Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation," UN Doc. HRI/GEN/1/Rev.1, http://www.unhchr.ch/tbs/doc.nsf/0/ca12c3a4ea8d6c53c1256d500056e56f/$FILE/G0441302.pdf (accessed March 10, 2014), para. 3, 4 and 8.

jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read."[41]

Although the restrictions on privacy do not contain an explicit requirement that they be necessary to a legitimate state purpose and proportionate to that end, these requirements are usually read as applicable to restrictions on privacy as they are common to most derogable rights in the Covenant, including freedom of expression, freedom of belief, and freedom of association which are closely associated with privacy. Special Rapporteur on Freedom of Expression Frank La Rue explained the common requirements for restrictions on rights under the Covenant in his 2013 report: "For a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims. It must be necessary for reaching the legitimate aim ….Restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected."[42]

General Comment 16 was adopted in 1988, long before the advent of technology that has made electronic surveillance practices as systematic and pervasive as they are today. Nor has the Human Rights Committee yet adjudicated many cases dealing with the legality of electronic surveillance. Though the obligation remains firmly rooted in the treaty, a more modern and well developed body of law has emerged out of the European Court of Human Rights (ECtHR) and other international adjudicative bodies that interpret rights guarantees very similar to those of the ICCPR. The Human Rights Committee often looks to regional human rights jurisprudence in interpreting the ICCPR, just as U.S. law is often informed by the jurisprudence of other democracies and international bodies.

Members of civil society groups and experts in communications surveillance law, policy and technology, have drawn upon this case law to assemble a set of principles on application of human rights law to communications surveillance. The document, called "Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance," are drawn from the Universal Declaration of Human Rights, the ICCPR, the European Convention on Human Rights (ECHR), the Inter-American

---

[41] Ibid., para. 8.

[42] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/23/40, April 17, 2013, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed February 10, 2014), para. 29(e)-(f).

Convention on Human Rights (I-ACHR) and the African Charter of Human and Peoples' Rights (African Charter), but also adjudicative bodies like the HRC and ECtHR, UN Resolutions and reports of Special Rapporteurs.[43] The principles have been signed by hundreds of human rights and civil society groups, including Human Rights Watch.

This body of international and regional legal sources also points to a number of other commonly-supported requirements for surveillance regimes to be compatible with human rights:

- *There must be an ability to challenge secret monitoring laws*: 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 could 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.[44]
- *Accessibility - there must be a statutory basis for the law*: "[R]elevant legislation must specify in detail the precise circumstances in which such interferences may be permitted."[45]
- *Foreseeability*: Foreseeability does not 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. "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."[46]
- *Compatibility with the rule of law*: The law must not provide too much discretion on the public authorities empowered enforce the law.[47] Independent, especially

---

[43] The International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles), https://en.necessaryandproportionate.org/text (accessed March 10. 2014).

[44] European Court of Human Rights, *Weber and Seravia v. Germany*, no. 54934/00, Judgment of June 29, 2006, available at www.echr.coe.int, para. 78.

[45] UN Human Rights Committee, General Comment No. 16, "Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation," UN Doc. HRI/GEN/1/Rev.1, http://www.unhchr.ch/tbs/doc.nsf/0/ca12c3a4ea8d6c53c1256d500056e56f/$FILE/G0441302.pdf (accessed March 10, 2014), para. 8.

[46] European Court of Human Rights, *Shimovolos v. Russia*, no. 30194/09, Judgment of June 21, 2011 , available at www.echr.coe.int, para. 68.

[47] European Court of Human Rights, *Malone v. United Kingdom*, no. 8691/79, Judgment of August 2, 1984, available at www.echr.coe.int, para. 68. See also European Court of Human Rights, *Case of Liberty and Others v. The United Kingdom*, no.

judicial, supervision of specific surveillance measures are crucial to preventing abuse.[48]

III. Application of these Principles to 702

Under Section 702, the US is authorized to collect and analyze communications, including content, of non-US persons reasonably believed to be outside the US when those communications are available within the US.[49] Under its "upstream" collection, the NSA taps an unknown number of fiber optic cables or other infrastructure that carry global Internet traffic to and from the US.[50] According to available information and media reports, the US may be copying and searching through the contents of *all* Internet and telecom traffic flowing over US borders through these cables.[51] Second, under the PRISM program, the US collects the contents of communications of persons reasonably believed to be outside the US when those communications are available within the US—that is, available from US-based Internet companies.[52] The breadth of orders to produce such communications served on US-based Internet companies remains unclear, nor do we know how many users have been affected by these collections.[53]

Although the full scale of the US's national security and intelligence surveillance programs is unknown, according to a 2011 opinion of the FISA court, the NSA collects more than 250

58243/00, Judgment of July 1, 2008, para. 64, ("The legal discretion granted to the executive for the physical capture of external communications was, therefore, virtually unfettered.").

[48] Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age," p. 67, n. 204, *citing* Concluding Observations of the Human Rights Committee: Zimbabwe, UN Doc. CCPR/C/79/Add.89, 6 April 1998, para. 25; Concluding Observations of the Human Rights Committee: The Netherlands, UN Doc. CCPR/C/NLD/CO/4, 25 August 2009, para. 14; Concluding Observations of the Human Rights Committee: Sweden, UN Doc. CCPR/C/SWE/CO/6, 2 April 2009, para. 18; European Court of Human Rights, *Rotaru v. Romania* {GC}, no. 28341/95, ECHR 2000-V, available at www.echr.coe.int, para.59; European Court of Human Rights, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, Judgment of November 22, 2012, available at www.echr.coe.int, para. 89-102.

[49] 50 U.S.C. § 1881(a).

[50] "NSA slides explain the PRISM data-collection program," *Washington Post*, June 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents (accessed February 10, 2014).

[51] Charlie Savage, "N.S.A. Said to Search Content of Messages To and From U.S.," *New York Times*, August 8, 2013, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?_r=0&pagewanted=all (accessed February 10, 2014).

[52] "NSA slides explain the PRISM data-collection program," *Washington Post*.

[53] The US Internet companies named in slides released by media reports deny that the NSA has "direct access" to their servers. Craig Timberg, "The NSA slide you haven't seen," *Washington Post*, July 10, 2013, http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (accessed February 10, 2014).

million Internet communications a year under section 702 alone.[54] Section 702 enables intelligence agencies to obtain yearlong programmatic warrants from the FISA court to conduct surveillance to acquire "foreign intelligence information."[55] For non-US persons, "foreign intelligence information" is in sweeping terms to include information that merely "relates to" international terrorism, weapons of mass destruction, counterintelligence, national security, and the conduct of foreign affairs of the US.[56] These programs are referred to as "programmatic" surveillance because the FISA court does not approve specific targets of such surveillance. Instead, the FISA court approves "targeting" and "minimization" procedures drafted by intelligence agencies, which purport to guide how, once information is collected, the material will be retained, searched, or shared.

However, the purpose of the "targeting" guidelines is to ensure agencies are only targeting non-US persons abroad, and not US citizens or residents. These procedures are not designed to prevent bulk collection of data on non-US persons outside the US. They also do not provide sufficient safeguards against the arbitrary or disproportionate collection and subsequent use of the personal information of non-US persons not suspected of any wrongdoing or connected to terrorism.[57] Moreover, under the NSA's targeting procedures, agencies can monitor the communications not only of specific targets, but also all communications "about" a target.[58] This formulation allows the NSA to potentially sweep in broad swaths of information even in the "targeted" phase, depending on how broadly or narrowly a "target" is defined.[59]

Though the US has declassified some prior minimization procedures, it is not clear that these will be made public going forward. Further, these minimization procedures protect

---

[54] Ellen Nakashima, "NSA gathered thousands of Americans' e-mails before court ordered it to revise its tactics," *Washington Post*, August 21, 2013, http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html (accessed February 10, 2014); "FISA court ruling on illegal NSA e-mail collection program," *Washington Post*, August 21, 2013, http://apps.washingtonpost.com/g/page/national/fisa-court-documents-on-illegal-nsa-e-mail-collection-program/409/ (accessed February 10, 2014).

[55] 50 U.S.C. § 1881(a).

[56] 50 U.S.C. § 1801(e).

[57] US Foreign Intelligence Surveillance Court, "Exhibit A, 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," July 29, 2009.

[58] Ibid.

[59] According to slides published by the Washington Post, on April 5, 2013, the NSA had 117,675 active surveillance "targets" in the program. Through PRISM, the NSA was also able to access real-time data on live voice, text, email, or Internet chat services, in addition to analyzing stored data. See "NSA slides explain the PRISM data-collection program," *Washington Post*.

mostly US person information, not non-US person information. Regarding the targeting procedures, the only ones that have been made public are those that were released through the disclosures made by NSA whistleblower Edward Snowden.[60] Therefore, there is not enough information in the public domain for individuals to have a precise understanding of the circumstances in which such interferences with communications may be permitted.

Further, in responding to the Snowden revelations, US officials have implied that the US does not consider electronic information to have been "collected" until that information is searched or processed in some way.[61] This assertion is echoed in regulations that govern intelligence gathering activities by specific agencies: for example, data acquired by electronic means is "collected" only when it has been processed "into intelligible form."[62] Significantly, this interpretation implies that the US may acquire vast stores of digital information without running afoul of the already limited safeguards against arbitrary "collection" of such information in US law, especially for Internet and mobile phone users outside the US.

Restrictions on the right to privacy must conform to the principle of proportionality, and should not be used where less invasive techniques are available.[63] Mass acquisition of personal information is by nature indiscriminate and the "targeting" practices used by the NSA also appear to be overly broad.

Regardless of whether acquisition of personal information occurring under section 702 is mass or more "targeted," the burden is on the US government to demonstrate that such surveillance is still necessary to a legitimate aim. The statute authorizes collection of information about non-US persons that merely "relates to" the foreign affairs of the US–

---

[60] Glenn Greenwald and James Ball, "The top secret rules that allow NSA to use US data without a warrant," *The Guardian*, June 20, 2013, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant (accessed February 10, 2014).

[61] Bruce Schneier, "Why the NSA's Defense of Mass Data Collection Makes No Sense," *The Atlantic*, October 21, 2013, http://www.theatlantic.com/politics/archive/2013/10/why-the-nsas-defense-of-mass-data-collection-makes-no-sense/280715 (accessed February 10, 2014).

[62] USSID 18, October 20, 1980, http://cryptome.org/nsa-ussid18-80.htm (accessed February 12, 2014), Section 3.4. See also, "Collection means intentional tasking and/or selection of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record." Department of Defense, Procedures Governing the Activities of DoD Intelligence Components that Affect United States persons, DoD 5240 1-R, December 1982.

[63] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/23/40, April 17, 2013,

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed February 10, 2014).

questionable as a sufficiently defined purpose for restriction of rights. Even if this is interpreted as relating to national security or public safety, it is highly doubtful that the vast majority of non-US person users whose privacy is being harmed under this program are in any way suspected of wrongdoing or connected to terrorism—raising serious questions as to whether such surveillance is arbitrary or unjustifiable.

On January 17, 2014, President Obama announced additional measures to restrict the use,[64] retention and dissemination of personal data gathered by intelligence services in Presidential Policy Directive 28.[65] However, these new measures fell short of ensuring that interference with privacy was limited to only that which was necessary or proportionate, and they left open the possibility of bulk collection. It is also not clear from the directive whether or how it applies to data obtained under section 702. Further safeguards are necessary. These new measures purport to bring rules on retention and dissemination of data collected on non-US persons closer to those governing data collected on US persons.[66] While the directive is a step forward in providing at least a measure of protection for non-US persons, the rules themselves are opaque, do not go far enough to prevent abuse, and create no justiciable rights. They are also temporary given that they are not part of US law and can be changed by any subsequent US administration.

The directive, moreover, specifically exempts data "temporarily acquired to facilitate targeted collection" from the use restrictions placed on continued bulk data collection.[67] As what constitutes a "targeted collection" remains undefined, this places few real limits on either the initial sweep or later searching of data, much less its retention or even use for an impermissible purpose. We would ask that the PCLOB make clear that at all stages, acquisition, invasion, use and retention, of personal communications data should be restricted by law to just that which is necessary and proportionate to a legitimate state purpose.

<u>Recommendations</u>:

---

[64] The use restrictions announced pertained only to continued "bulk" collection.

[65] Presidential Policy Directive/PPD-28, "Presidential Policy Directive -- Signals Intelligence Activities," January 17, 2014, http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (accessed February 10, 2014).

[66] Ibid.

[67] Ibid., Section 2, note 5. It should be noted that these "use restrictions" are themselves quite general, namely, that use should be for a permissible general purpose such as countering various types of security threats, rather than for an obviously impermissible purpose, such as discrimination. Thus it is all the more worrying that bulk acquisition to support targeted collection is exempt from these broad-stroke restrictions.

- The PCLOB should recommend to the US government that it acknowledge it has obligations under the ICCPR that apply extraterritorially and that it accept it has an obligation to respect the right to privacy of individuals outside its borders. Specifically, the US has an obligation to ensure rights, in the sense of active protection and legislation, to individuals who are both within its territory and subject to its jurisdiction. In addition, it has an obligation to respect the rights recognized in the Covenant in the sense of refraining from violating rights, in those circumstances where it can exercise effective control over an individual or the individual's rights.

- Recommend that surveillance under Section 702 take place only upon some threshold showing of individualized suspicion that the information to be acquired is necessary for the protection of US national security or public safety interests. Currently the only requirement is that the purpose of the acquisition be to collect "foreign intelligence information," which is too broadly defined, and that the NSA be reasonably certain the target is a non-US person located abroad. Though apparently the collection is further limited by certifications, even a FISC judge approving these certifications does not know the identity of the individuals or targets at whom such acquisitions would be directed.

- Recommend that the definition of "foreign intelligence information" so that what can be acquired is limited to, for example, information about espionage, sabotage, and national security. It should not allow for the collection of foreign intelligence information merely because it aids in the conduct of foreign affairs.

- Recommend that the US make the rules governing 702 practices public in sufficient detail so that the precise circumstances in which such interferences may be permitted are made clear. The administration has only made public minimization procedures in response to FOIA requests and the only targeting procedures publicly available are those disclosed by Snowden.

- Recommend that Congress reform the law to determine who has authority to select targets, who may initiate data collection, how that authority may be exercised, and the scope of discretion conferred on competent authorities , so that individuals will have the capacity to guard against and challenge arbitrary interference.

- In its fact finding capacity, the Board should try to clarify the nature of "selectors" (including "soft selectors") and "targets" used to determine scope of data collection.

- According to Washington Post Prism slides, the NSA had 117,675 active FISA "targets" as of April 5, 2013.[68] If 702 permits, in addition to the collection of information to and from a target, also information "about" a target, that potentially allows for vastly overbroad collection of the communications of individuals who are remote from any suspicion of wrongdoing or connection to terrorism. While it is difficult to formulate a specific recommendation regarding this practice without more information regarding how and when it is being undertaken, consider recommending ending the practice of acquiring "about" communications.

- Make a finding that the acquisition or copying of personal information can constitute interference with privacy, regardless of whether the information is subsequently processed, examined, or used by the government. The right to privacy and privacy interests are implicated when personal data or communications are acquired, and can be violated if such acquisition is arbitrary, unlawful, discriminatory, unnecessary or disproportionate.

Respectfully Submitted,

Laura Pitter
Senior National Security Researcher
Human Rights Watch
350 5th Ave. 34th Fl.
New York, NY
10118
Date: March 17, 2014

[68] "NSA slides explain the PRISM data-collection program," *Washington Post*, June 6, 2013, Updated July 10, 2013, slide 4, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents (accessed March 15, 2014).