
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

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

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,

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

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

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 R-4(lna)]TJ 0 Tc 0 Tw (lna)]TJ 0R vo the C(l)-emnant6(ant6(anee (p)-4(lp14(ei)-6(e-1(v

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 permissibssc(s)-5(R.rio)2(n)212 scn /e

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

### 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

p

purpose of protecting the rights of others, for example to secure evidence to prevent the

*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-cituhe gynanhece (l)-2(u)-1l60u8ty-10(g(o)-10(r)3t)Tj 4.7 0 T26hoh-0.00

- 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 U02 TiIn(y)2-2(h) Tc 0 Tw 0 -1.TD d [(i)-2( s)-1(ur)31ct10(0(r)3

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]

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 implica

drawn a bright line distinction between responsibility over citizens and non-citizens, recognizing

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

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

calling on the US

x

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.