United States of America

NGO assessment of the follow-up action of the U.S. Government for ICCPR Recommendation Para. 22

Submission of Brennan Center for Justice at NYU School of Law, Access and Amnesty International USA

1. This report will discuss and analyze the U.S. government's actions in response to the ICCPR Committee's recommendations on NSA surveillance.

Article 17 of the ICCPR

2. Contrary to the U.S.'s claims, there is widespread international recognition that an interference with the right to privacy under Article 17 must be "necessary and … proportionate to achieve a legitimate objective."[1] Specifically, interferences under Article 17 are "arbitrary" unless they are necessary to pursue a legitimate aim, proportionate to that aim, and minimally intrusive of protected privacy interests.[2] Non-arbitrary interferences under Article 17 may still be "unlawful" unless they are consistent with domestic and international law; regulated by laws that are specific, precise, and publicly accessible in a manner that enables the public to foresee the interference; and constrained by adequate safeguards.[3] In addition to the Committee, a growing range of human rights bodies have affirmed various of these requirements, including the Office of the High Commissioner for Human Rights, three UN Special Rapporteurs, and the European and Inter-American Courts of Human Rights.[4]

3. The Committee has categorically rejected the U.S.'s view that "obligations under the Covenant apply only with respect to individuals who are both within the territory of the State

[1] One-Year Follow-Up Response of the United States of America to Priority Recommendations of the Human Rights Committee on Its Fourth Periodic Report on Implementation of the International Covenant on Civil and Political Rights ¶ 33 (Mar. 31, 2015), *available at* http://www.ushrnetwork.org/sites/ushrnetwork.org/files/us_iccpr_follow-up_report_int_ccpr_fco_usa_19957_e_4_1_15.pdf [hereinafter *US Submission*].
[2] *See id.*
[3] *See* AMERICAN CIVIL LIBERTIES UNION, INFORMATIONAL PRIVACY IN THE DIGITAL AGE: A PROPOSAL TO UPDATE GENERAL COMMENT 16 (RIGHT TO PRIVACY) TO THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS 14-19 (2015), *available at* https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf [hereinafter *ACLU Report*].
[4] *Id.* at 20-22.

Party and within its jurisdiction."[5] In General Comment 31, for example, the Committee observed that "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party."[6] Other international bodies have reached the same conclusion, including the International Court of Justice, the Inter-American Commission of Human Rights, and the European Court of Human Rights.[7] In the privacy context, a State must take measures to "ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity *regardless of the nationality or location of individuals whose communications are under direct surveillance.*"[8]

4. The Committee's position on extraterritoriality is critical to protecting the right to privacy in the digital age. A State may interfere with the right to privacy of individuals that are not within its territory or an area under its control simply by exercising power or effective control over those individuals' communications. Such interferences are now routine: Rapid advancements in surveillance technology enable States, including the U.S., to gather and monitor massive numbers of private communications and data outside their territorial jurisdiction. This ability to intrude into the most intimate and personal aspects of an individual's life, regardless of her location, implicates the right to privacy under Article 17.

Mass Overseas Surveillance under Executive Order 12,333

5. Despite recent reform attempts, the National Security Agency ("NSA") still asserts the authority to indiscriminately acquire and collect digital communications and data around the world. The NSA has revealed that it conducts the "majority" of its surveillance operations under Executive Order 12,333 ("EO 12,333"), the primary source of authority for intelligence gathering activities overseas.[9] Leaked and declassified documents show that many of these operations sweep up massive amounts of communications and personal data, including information about every single call made to, from and within certain countries;[10]

---

[5] US Submission, *supra* note 1, at ¶ 33.
[6] General Comment 31, ¶ 10, U.N. HRC, 80th Sess., U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004).
[7] ACLU Report, *supra* note 3, at 27 n.151.
[8] Concluding observations of the fourth periodic report of the United States of America, ¶ 22(a), U.N. HRC, 110th Sess., U.N. Doc. CCPR/C/USA/CO/4 (2014), http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en (emphasis added). Submission of Amnesty International USA and the American Civil Liberties Union, Privacy and Civil Liberties Oversight Board, Public hearing on Section 702 of the FISA Amendments Act (Mar. 19, 2014), *available at* http://www.amnestyusa.org/sites/default/files/recommendationsforhumanrightslawandussurveillancepractices.pdf.
[9] Legal Fact Sheet: Executive Order 12,333 (June 19, 2013), *available at* https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf.
[10] Ryan Devereaux, et al., *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, THE INTERCEPT (May 19, 2014), https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.

hundreds of millions of text messages;[11] and billions of records of e-mails, Facebook chats and Internet histories.[12]

6. Following these revelations, President Obama issued Presidential Policy Directive 28 ("PPD-28"), a set of guidelines on "whether, when and how" the intelligence community should collect, retain and disseminate communications and related data.[13] Significantly, however, PPD-28 does not place any restrictions on the NSA's *acquisition* of such information. According to the NSA's internal regulations, data acquisition is not the same as "collection," which takes place only when the Agency "intentional[ly] task[s] or select[s] … nonpublic communications for subsequent processing aimed at reporting or retention as a file record."[14] In other words, the NSA has "collected" communications only when it has processed or analyzed them for specific purposes. This strained distinction between "acquisition" and "collection" implies that the NSA may amass an unlimited number of protected communications and data without violating existing domestic regulations.

7. There is evidence to suggest that the NSA is relying on this legal loophole to conduct mass surveillance. Documents provided by Edward Snowden show that the NSA acquires comprehensive call details of all telephone calls made in five countries, and keeps for thirty days a recording of *every* mobile call placed to, from and within two of these countries.[15] *The Intercept* estimates that these surveillance operations sweep up the communications of more than 250 million people around the world.[16] However, the NSA's theory of "collection" potentially exempts such indiscriminate acquisition of communications from legal regulation, at least until it processes acquired communications for further analysis and long-term storage.[17] This position is inconsistent with international human rights law, which considers

---

[11] James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, THE GUARDIAN (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

[12] Barton Gellman & Ashkan Soltani, *NSA Collect Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html; Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[13] Presidential Policy Directive/PPD-28 on Signals Intelligence Activities (Jan. 17, 2014), *available at* http://fas.org/irp/offdocs/ppd/ppd-28.pdf [hereinafter *PPD-28*].

[14] National Security Agency, United States Signals Intelligence Directive 18: Legal Compliance and United States Person Minimization Procedures § 9.2 (Jan. 25, 2011), *available at* https://www.hsdl.org/?view&did=746666 [hereinafter *USSID 18*].

[15] Devereaux et al., *supra* note 10.

[16] *Id.*

[17] The NSA reportedly listens to only a "fraction of one percent of the[se] calls," and sends "millions [out of potentially hundreds of millions] of voice clippings . . . for processing and long-term storage" each month. The NSA may be of the position that the restrictions on "collection" apply only when they listen, process or analyze the calls

the acquisition of protected communications and data to be an interference with the right to privacy, regardless of whether they are subsequently processed, analyzed or stored.[18]

8. The rules triggered upon the NSA's "collection" of information also fail to adequately protect the right to privacy. PPD-28 recognizes that intelligence collection should be in accordance with law, nondiscriminatory, and as tailored as feasible. These "general principles," however, do not meaningfully restrict the NSA's authority to collect an extremely broad range of "foreign intelligence" under EO 12,333. The Order defines "foreign intelligence" as any information relating to the "capabilities, intentions or activities" of foreign organizations or foreign persons, regardless of whether they are associated with foreign governments or terrorist suspects or present any threat.[19] This authority to collect any information as long as it has some foreign connection would indiscriminately interfere with the privacy interests of countless individuals suspected of no wrongdoing. As a result, it is neither lawful nor proportionate to a legitimate government interest.[20]

Indefinite Retention of Encrypted Communications

9. In general, the NSA may only retain U.S. persons' information for up to five years.[21] PPD-28 now extends this rule to non-U.S. persons' information.[22] However, this disproportionately long five-year retention period is further subject to significant expansions. In particular, the NSA may retain communications that are encrypted or "thought to contain secret meaning" for however long it takes to decipher them.[23] This loophole is extremely problematic. Lawyers, journalists, human rights defenders and others seeking to impart information of public interest, as well as health professionals, increasingly rely on encryption to communicate sensitive information in a manner that fulfills their duties of confidentiality in the digital age.[24] Encryption is also going mainstream: Major Internet and communications

---

they have already acquired. Barton Gellman & Askhan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST (Mar. 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.

[18] The Human Rights Committee states in General Comment 16 that the act of "gathering and holding . . . personal information on computers, databanks and other devices" must be "regulated by law." General Comment 16, ¶ 10, U.N. HRC, 23rd Sess., U.N. Doc. HRI/GEN/1/Rev.1 (1994).

[19] Exec. Order No. 12,333, 3 C.F.R. § 3.4(d) (1981), *available at* http://fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

[20] Letter from Access & Electronic Frontier Foundation, to the Privacy and Civil Liberties Oversight Board (Aug. 29, 2014), *available at* https://www.eff.org/files/2014/09/02/pclobcomment-12333.pdf.

[21] Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, 128 Stat. 3990.

[22] PPD-28, *supra* note 13, at § 4(a)(i); National Security Agency, PPD-28 Section 4 Procedures § 6.1(a) (Jan. 12, 2015), *available at* https://www.nsa.gov/public_info/_files/nsacss_policies/PPD-28.pdf [hereinafter *Section 4 Procedures*].

[23] USSID 18, *supra* note 14, at § 6.1(a)(2); Section 4 Procedures, *supra* note 20, at § 6.1(a).

[24] HUMAN RIGHTS WATCH & AMERICAN CIVIL LIBERTIES UNION, WITH LIBERTY TO MONITOR ALL: HOW LARGE-SCALE US SURVEILLANCE IS HARMING JOURNALISM, LAW AND AMERICAN DEMOCRACY 31 (2014), *available at* http://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf ("A significant number of journalists reported using various forms of encryption software for their communications with sources or colleagues."). *Id.* at

providers like Apple, Google and Yahoo! now routinely encrypt their customers' e-mails, text messages and chats.[25] As a result, the digital communications of millions of Internet users—including privileged attorney-client communications and communications between journalists and their sources—could end up in the NSA's intelligence databases for indefinite periods of time.

Large-Scale Information Sharing with Foreign Governments

10. There also appears to be no legal restriction on the NSA's ability to share communications and data collected under EO 12,333 with foreign governments. The U.S. has extensive intelligence sharing arrangements with Australia, Canada, New Zealand and the United Kingdom as part of an alliance known as the "Five Eyes."[26] Documents provided by Snowden also reveal that the NSA shares large volumes of raw private data with Israeli intelligence, including transcripts of telephone and online communications, voice clips, and facsimiles and telephone metadata concerning both U.S. and non-U.S. persons.[27] And because many of the U.S.'s partners have intelligence sharing arrangements with other countries, intelligence data collected by the NSA could end up in the hands of numerous foreign governments, including those with poor human rights records.[28]

11. Despite the scale of such information sharing, neither EO 12,333 nor PPD-28 provides any safeguards to prevent collected data from being used to commit or contribute to human rights abuses. It appears that the only available safeguards are those that the NSA and the foreign government recipient agree to include in their intelligence sharing arrangements. But these safeguards are inherently inadequate, because the U.S. has little control over how they are interpreted, how rigorously they are followed, and how frequently non-compliance is reported. If the U.S.-Israel agreement is typical of the U.S.'s intelligence sharing

---

63 ("As a result of their growing concerns about surveillance, several attorneys reported encrypting their email or other forms of electronic communications.").

[25] Nicole Perlroth & David E. Sanger, *Internet Giants Erect Barriers to Spy Agencies*, N.Y. TIMES (June 6, 2014), *available at* http://www.nytimes.com/2014/06/07/technology/internet-giants-erect-barriers-to-spy-agencies.html ("Google . . . is encrypting more data as it moves among its servers and helping customers encode their own emails. Facebook, Microsoft and Yahoo are taking similar steps.").

[26] Paul Farrell, *History of 5-Eyes – Explainer*, THE GUARDIAN (Dec. 21, 2013), http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer. To be sure, there have been reports that the U.S. also has intelligence sharing arrangements with Western countries beyond the 'Five Eyes,' including Germany and France. *See .e.g.* Melissa Eddy, *For Western Allies, a Long History of Swapping Intelligence*, N.Y. TIMES (July 9, 2014), http://www.nytimes.com/2013/07/10/world/europe/for-western-allies-a-long-history-of-swapping-intelligence.html.

[27] Glenn Greenwald et al., *NSA Shares Raw Intelligence Including Americans' Data with Israel*, THE GUARDIAN (Sept. 11, 2013), http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[28] For example, New Zealand, a "Five Eyes" partner, routinely shares "intelligence leads" with several Bangladeshi intelligence agencies that have been accused of extrajudicial killings, torture and other human rights violations. *See e.g.*, Ryan Gallagher & Nicky Hager, *New Zealand Spy Data Shared with Bangladeshi Human Rights Abusers*, THE INTERCEPT (Apr. 15, 2015), https://firstlook.org/theintercept/2015/04/15/new-zealand-bangladesh-gcsb-surveillance-human-rights/.

arrangements, it indicates that safeguards are usually scant: While there are certain limits on how information concerning U.S. persons may be used, there are no protections for non-U.S. persons.[29]

Continued Lack of Effective Oversight of NSA's Surveillance Activities

12. Although the NSA exercises expansive authority to acquire, collect, store and share information under EO 12,333, these surveillance activities are subject to minimal external oversight. Such activities do not fall within the jurisdiction of the Foreign Intelligence Surveillance Court ("FISC"), the main judicial body that oversees foreign intelligence surveillance operations. Congressional oversight is also weak. Intelligence agencies are supposed to keep Congress "fully and currently informed" of any "significant anticipated intelligence activities,"[30] but Senator Dianne Feinstein, the former Chair of the legislative body that oversees intelligence activities, has indicated that this did not happen.[31] As a result, the intelligence community effectively oversees compliance with the very rules it created to regulate the operations it conducts under EO 12,333. As Senator Feinstein pithily observed, EO 12,333 operations "are under the executive branch *entirely*."[32] Although the U.S. insists that it has "strong" *internal* oversight mechanisms, self-regulation is inadequate under the ICCPR because it is no substitute for independent, external oversight conducted by other branches of government.

13. Since the 2014 Review, efforts to reform judicial oversight of surveillance activities conducted inside the United States have been unsuccessful. Congress is currently considering a bill that would facilitate the declassification of the FISC's "significant" opinions, and purports to enhance the court's adversarial process.[33] In particular, the bill establishes a panel of legal and technical experts to serve as *amici curiae*, or friends of the court, to provide input and argue in favor of privacy and civil liberties. However, the court has ultimate control over whether they would be allowed to appear or argue in cases that arise, raising significant doubts about the experts' ability to meaningfully and independently participate in

[29] *NSA and Israeli Intelligence: Memorandum of Understanding – Full Document*, THE GUARDIAN (Sept. 11, 2013), http://www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document.
[30] Exec. Order No. 12,333, 3 C.F.R. § 3.1 (1981), *available at* http://fas.org/irp/offdocs/eo/eo-12333-2008.pdf; 50 U.S.C. § 3091(a)(1) (general congressional oversight provisions).
[31] Ali Watkins, *Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued*, MCCLATCHY DC (Nov. 21, 2013), http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html; Eli Lake, *Congress Scouring Every US Spy Program*, THE DAILY BEAST (Oct. 10, 2014), http://www.thedailybeast.com/articles/2014/10/10/congress-scouring-every-u-s-spy-program.html.
[32] Watkins, *supra* note 31.
[33] H.R. 2048, 114th Cong. (2015), *available at* https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048ih.pdf.

the court's proceedings.[34] Accordingly, the criticisms that we submitted previously to the Committee and other human rights bodies concerning the FISC's inability to oversee large-scale surveillance programs and secret interpretations of relevant intelligence laws remain largely intact.[35]

Continued Lack of Access to Effective Remedies for Privacy Violations

14. Persons affected by the NSA's surveillance operations have little or no opportunity to challenge surveillance that affects them, which is usually conducted in secret. Until late 2013, U.S. prosecutors failed to notify criminal defendants when evidence against them stemmed from certain large-scale, warrantless surveillance programs conducted inside the U.S.[36] Although the government has recently begun to issue such notices, no defendant has ever been permitted to view the government's surveillance applications, making it extremely difficult to challenge the scope and nature of their surveillance. Furthermore, prosecutors reportedly continue to assert that they need not give notice to defendants when they use evidence derived from information collected under EO 12,333.[37] This lack of notice is particularly concerning given the ability of law enforcement authorities to access a wide range of NSA-collected information for purposes unrelated to national security.[38] The lack of notice effectively forecloses the ability of criminal defendants to challenge the practice of obtaining evidence of ordinary crimes from surveillance operations that are supposed to be conducted only for foreign intelligence and national security purposes.

15. As for non-U.S. persons located abroad, there is essentially no possibility of relief from improper U.S. surveillance. In the event of a privacy violation involving a non-U.S. person, PPD-28 permits the Director of National Intelligence to notify the relevant foreign

[34] Note, however, that an annual report must specify to Congress the number of findings where the appointment was found unnecessary as well as publicly state the number of times when an appointment occurred.
[35] BRENNAN CENTER FOR JUSTICE, U.S. SURVEILLANCE: UNCHECKED AND UNSUPERVISED (2013), *available at* http://www.brennancenter.org/sites/default/files/publications/182138137-U-S-Surveillance-Unchecked-and-Unsupervised.pdf; AMERICAN CIVIL LIBERTIES UNION, UNITED STATES' COMPLIANCE WITH THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (2013), *available at* https://www.aclu.org/files/assets/american_civil_liberties_union_shadow_report_to_the_u.s._fourth_periodic_report_final.pdf.
[36] Charlie Savage, *Door May Open For Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 16, 2013), *available at* http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challengeto-secret-wiretaps.html?pagewanted=2&_r=0.
[37] Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights Says Departing Aide*, N.Y. TIMES (Aug. 14, 2014), *available at* http://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html; *see also* Patrick C. Toomey, *Executive Order 12,333, Notice, and the Due Process Rights of Criminal Defendants*, JUST SECURITY (Aug. 14, 2014), http://justsecurity.org/14040/executive-order-12333-notice-due-process-rights-criminal-defendants/.
[38] Memorandum from the Department of Justice on Reporting of Information Concerning Federal Crimes (1995), *available at* http://fas.org/irp/agency/doj/mou-crimes.pdf.

government, though only in some cases.[39] However, there appears to be no substantive remedy for the affected non-U.S. person apart from notice to her government.

Recommendations

16. Given our observations and analysis above, we urge the Committee to make these follow-up recommendations to the U.S.:

    a. The U.S. should recognize a legal obligation to respect and ensure the right to privacy and other human rights of persons outside its territory or jurisdiction when it acquires, processes, uses, stores or shares their communications and information.

    b. The U.S. should recognize that any interference with the right to privacy under Article 17 of the ICCPR must be a necessary and proportionate means of pursuing a legitimate aim, and minimally intrusive of protected interests.

    c. The U.S. should recognize that any interference with the right to privacy (including the sharing of information with foreign governments) must be consistent with the prohibition against discrimination on protected grounds (such as those listed in Article 2(1) of the ICCPR).

[39] PPD-28, *supra* note 13, at § 4(a)(iv).