HUMAN RIGHTS WATCH

Human Rights Watch and the Electronic Frontier Foundation Supplemental Submission to the Human Rights Committee During its Consideration of the Fourth Periodic Report of the United States

February 14, 2014

Introduction

Human Rights Watch and the Electronic Frontier Foundation submit this addendum in advance of the Human Rights Committee's ("the Committee") upcoming review of the United States. This statement supplements Human Rights Watch's December 2012 submission in light of new information on the scope of the US's electronic surveillance and intelligence gathering practices.[1]

Documents released by former National Security Agency (NSA) contractor Edward Snowden have revealed several programs that may be potentially interfering with the privacy of millions of individuals worldwide:

- The bulk phone metadata program (Section 215 of the USA PATRIOT Act) – The NSA collects telephone records from a significant portion of US telecom companies about all phone calls to, from, and within the US carried by that carrier.[2] Section 215 may also be used for other bulk collection programs.
- Procedures used to conduct general "programmatic" surveillance under Section 702 of amendments to the Foreign Intelligence Surveillance Act (FISA) – 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

[1] Human Rights Watch, "Submission to the Human Rights Committee During its Consideration of the Fourth Periodic Report of the United States," December 2012, http://www.hrw.org/news/2013/01/04/us-human-rights-watch-submission-un-human-rights-committee.

[2] Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

US.[3] In practice, many US person's communications, both wholly domestic and international, are also swept up in the collection.

  - Under 702, the NSA engages in what it calls "Upstream" collection, where it taps fiber optic cables inside the US that carry Internet traffic, claiming that it only keeps traffic to and from the US.[4]
  - Under 702, the NSA also engages in a program called PRISM, where it collects information from US-based Internet companies, although the specifics remain unclear.[5]

- Under an Executive Order 12333, the NSA collects a massive amount of both content and non-content information abroad (and some also within the US) with limitations on its use for US persons but few, if any, for non-US persons.[6] The scope and scale of activities under Executive Order 12333 occur at the discretion of the President of the United States and are thus subject to even less oversight and control than programs occurring under US statutes.[7]

Many details about the scope of these programs remain unknown. What has so far been made public suggests that such surveillance constitutes unlawful and arbitrary interference with privacy or correspondence, in breach of Article 17 of the International Covenant on Civil and Political Rights (ICCPR). The massive scale of the programs, coupled with the secrecy of underlying legal interpretations and defects in oversight, raises serious concerns about violations of the right to privacy on an unprecedented scale. These programs also raise serious concern about the harm they cause to freedom of expression, association, and other rights.

---

[3] 50 USC 1801. This program purports to "target" persons physically outside the US (but not US citizens), though publicly released documents suggest high tolerance for unintentional collection of communications of US persons. Publicly released documents also suggest that there are almost no safeguards against arbitrary violations of the right to privacy of persons of non-US persons outside the US. See section III below.

[4] James Bamford, "They Know Much More Than You Think," *The New York Review of Books*, August 15, 2013, http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think;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).

[5] Barton Gellman and Laura Poitras, "US, British intelligence mining data from nine US Internet companies in broad secret program," *Washington Post*, June 6, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; 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 12, 2014).

[6] Executive Order 12333, United States Intelligence Activities, as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008), https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf.

[7] See Mark M. Jaycox, "Three Leaks, Three Weeks, and What We've Learned About the US Government's Other Spying Authority: Executive Order 12333," Electronic Frontier Foundation Deeplinks Blog, November 5, 2013, https://www.eff.org/deeplinks/2013/10/three-leaks-three-weeks-and-what-weve-learned-about-governments-other-spying.

In light of changes to technology that enable these new, powerful forms of surveillance, we ask the Committee to recognize and apply the following principles in its review of the US's obligations under Articles 2 and 17 of the ICCPR.

I. The US has extraterritorial obligations to uphold the right to privacy of individuals outside its borders

In its previous submission, Human Rights Watch urged the Committee to request that the US unambiguously acknowledge the applicability of the Covenant to individuals under its power or effective control but outside the geographic boundaries of the US.[8]

Given the extraordinary capabilities and programs of the US to monitor global communications, the Committee should ask the US to acknowledge that its obligations with respect to the right of privacy apply extraterritorially to persons whose communications it scans or collects. To accept otherwise would defeat the object and purpose of the ICCPR with regard to the privacy of borderless, global digital communications.

Although the precise scope of US surveillance programs is unknown, a steady stream of press revelations suggests that these programs may be sweeping in communications and personal data of potentially millions of people worldwide. Three major shifts in technology have made it especially easy for the US to conduct broad, systematic surveillance of individuals outside its borders:

- Much of the world's digital communications flows through fiber optic cables inside the US, even where such communications do not involve a US-based Internet user. Through cooperative agreements the US appears to have access to information gathered in bulk by foreign intelligence services, including GCHQ in the UK.[9]
- Many of the world's most popular Internet companies (email providers, social media services, etc.) are US-based companies. These firms store and process global user data inside the US, making such data more readily available to the US government. The US also believes that it has jurisdiction over all of these companies' operations wherever they occur since they are incorporated in the US. This is true even where the user is not in the US and is not communicating with anyone in the US.
- Global communications has increased and shifted to a substantial degree to Internet-enabled services such as email, social media, voice services, and other online tools. Cross-border communication is now instant, commonplace, and cheap, compared to international phone

[8] Human Rights Watch, "Submission to the Human Rights Committee," p. 6.

[9] Privacy International, *Special Report: Eyes Wide Open v1.0*, November 26, 2013, https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/eyes_wide_open_v1.pdf.

calls. The Internet has also enabled the exercise of the right to freedom of expression and access to knowledge and information on an unprecedented global scale. Storage and analysis of digital data across borders is also possible on an unprecedented scale, at relatively low cost, lowering barriers to present and future mass surveillance.

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. One company can hold the data of hundreds of millions of people worldwide and its home government can assert legal control over that data. Internet networking structures often result in communications flowing through multiple, unrelated countries (especially including the US) in between communicants. Sophisticated sorting and data analysis methods can allow the communications of more people to be effectively surveilled than ever before. Electronic surveillance can also now be done at great distances: where the individual is situated and where the interference with the right to privacy "physically" occurs may be in two separate places. Put another way, 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 his or her communications.

Such surveillance has the potential to produce not only direct violations of privacy and freedom of expression, but other severe harms, whether it is remotely ordered attacks, legal penalties, exposure to attack by third parties, or other consequences harmful to human rights. As stated by the UN Special Rapporteur on the right to freedom of expression in his April 2013 report to the Human Rights Council, "[t]his 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."[10]

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, the US provides significantly weaker protections for the right to privacy for "non-US persons."[11] US persons are

---

[10] 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, U.N. 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. 64.

[11] 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).

protected no matter where they are situated, while non-US persons lose protections when outside US borders.[12]

This two-tiered approach to privacy follows from the US's long-held position that the ICCPR does not apply extraterritorially.[13] However, we urge the Committee to reject that position and reiterate the extraterritorial obligations of governments under the ICCPR.[14] Accepting the US's view that the right to privacy does not extend to its actions abroad would defeat the object and purpose of Article 17 as applied to online or digital communications. If all states adopted a similar position, it would permit governments to conduct arbitrary or unlawful surveillance on the communications of any persons physically located outside their territory or jurisdiction. This position would thwart efforts of other governments to protect the privacy rights of their own residents if every other government is free to violate that right.[15] The US's position is also contrary to the principle of the universality of rights and suggests that the right to privacy can be abrogated on the basis of citizenship and legal status.

We also urge the Committee to take 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.[16] 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. Given the US's unique position within the Internet's infrastructure, the US 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,

---

[12] FISA Amendments Act, 50 USC 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." See section II.

[13] UN HRC, Fourth Periodic Report of the United States of America, U.N. Doc. CCPR/C/USA/4, May 22, 2012, paras. 504-505; UN HRC, Replies of the United States of America to the list of issues in relation to the fourth periodic report of the United States of America, U.N. Doc. CCPR/C/USA/Q/4/Add.1, September 13, 2013, para. 2.

[14] Cf. U.N. Human Rights Comm., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations of the Human Rights Committee: United States of America, U.N. Doc. CCPR/C/USA/CO/3/Rev.1 (Dec. 18, 2006), noting at para. 10: The United States should "in particular (a) acknowledge the applicability of the Covenant in respect of individuals under its jurisdiction and outside its territory".

[15] This would be contrary to the *erga omnest* character of human rights norms, as noted in General Comment 31 para. 2.

[16] 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).

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.[17]

Finally, the Committee should seek information on intelligence sharing arrangements the US may have with other governments, particularly under the "Five Eyes" arrangement between the US, the United Kingdom, Canada, Australia, and New Zealand.[18] The Committee should ask the US to clarify the circumstances under which information gleaned from surveillance is shared with other governments, and under what legal protections for the right to privacy. The Committee should also ask what safeguards exist in the US when, for example, the UK shares data collected on US persons from fiber optic cables running through the UK as part of British intelligence agency GCHQ's Tempora program.[19] Without protections against arbitrary or unlawful disclosure or collection, such arrangements could allow the US to evade even those constitutional or human rights safeguards that the US purports to provide only to persons within its territory.

Human Rights Watch and the Electronic Frontier Foundation urge the Committee to:

- Conclude that through its surveillance activities, the US has violated its obligation to respect the right to privacy under the ICCPR.
- Specifically request that the US acknowledge a duty to respect the right to privacy of individuals outside its borders when it acquires and monitors their digital communications.
- Seek information on intelligence sharing arrangements the US may have with other governments, as well as any related arrangements that may exist to protect privacy.

II. Collection of personal information is an interference with privacy

In responding to the Snowden revelations, US government 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.[20] This assertion is echoed in regulations that govern intelligence gathering

---

[17] UN Human Rights Committee (HRC), CCPR General Comment No. 31 [80] Nature of the General Legal Obligation Imposed on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004), http://www.unhchr.ch/tbs/doc.nsf/0/58f5d4646e861359c1256ff600533f5f (accessed February 10, 2014).

[18] Carly Nyst, "The Five Eyes Fact Sheet," Privacy International, November 27, 2013, https://www.privacyinternational.org/blog/the-five-eyes-fact-sheet (accessed February 10, 2014).

[19] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," *The Guardian*, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[20] See, 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/.

activities by specific agencies: for example, "Data acquired by electronic means is 'collected' only when it has been processed into intelligible form."[21] 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.

The Committee should recognize that the acquisition or copying of personal information can constitute an "interference" with the right to privacy under Article 17, regardless of whether the information is subsequently processed, examined, or used by the government. The right to privacy is implicated when personal data or communications are collected—in the most commonly understood use of the word—and can be violated if such collection is arbitrary, unlawful, or indiscriminate.[22]

This interpretation is consistent with prior Human Rights Committee statements, including General Comment 16, which states, "[c]orrespondence should be delivered to the addressee without *interception* and without being opened or otherwise read" and "[t]he *gathering and holding* of personal information on computers, data banks and other devices...must be regulated by law."[23] It is also consistent with interpretations by the European Court of Human Rights, which has found that storage of personal data can interfere with privacy, and that "subsequent use of stored information has no bearing on that finding."[24] These findings recognize that the mere possibility of improper access or abuse of stored personal information can cause privacy harm even if specific information is never actually misused. Fear of unjustified monitoring and gathering of personal information can also alter behavior in ways that harm other rights, such as freedom of movement, expression or association, even when an individual has done nothing wrong.[25]

---

[21] 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.

[22] For digitized data, automatic (without human intervention) interception and copying of electronic information would raise the same privacy concerns as "collection." Under US law, "intercept" is defined as "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 USC 2510(4).

[23] UN Human Rights Committee, CCPR General Comment No. 16: Article 17, The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, (1988), http://www.refworld.org/docid/453883f922.html (accessed 10 February 2014), paras. 8-10 (emphasis added).

[24] *Amann v. Switzerland*, EHCHR, Case No. 27798/95, February 16, 2000.

[25] UN Special Rapporteur on freedom of expression, April 2013 report, paras. 19-27. For example, in Germany, a study showed that, as a result of data retention, half of Germans will not contact marriage counselors and

Further safeguards against unnecessary and disproportionate *use*, *retention*, or *dissemination* of data are also needed. On January 17, 2014, President Obama announced additional measures to restrict the use,[26] retention and dissemination of personal data gathered by intelligence services in Presidential Policy Directive 28.[27] However, these new measures still fell short of ensuring that interference with privacy was limited to only that which was necessary or proportionate and left open the possibility of bulk collection. 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.[28] While the directive is a step forward in providing at least a measure of protection for non-US persons, the rules themselves are vague, 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.[29] 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 ask the Committee to reiterate that at all stages, the invasion of personal communications data be restricted by law to just that which is necessary and proportionate to a legitimate state purpose.

Metadata vs. Content

US law distinguishes between the content of communications, and "metadata" or transactional data. Communications metadata generally consists of information other than the content of the communications, including the phone number dialled, time or date of a phone call, mobile phone location information,[30] Internet Protocol address, or website URL visited. Current US constitutional interpretation holds that while individuals have a "reasonable expectation of privacy" in the content

---

psychotherapists through telephone or email. Axel Arnbak, "What the European Commission Owes 500 Million Europeans," http://www.edri.org/files/Data_Retention_Conference_031210final.pdf.

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

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

[28] Ibid.

[29] 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.

[30] Barton Gellman and Ashkan Soltani, "NSA tracking cellphone locations worldwide, Snowden documents show," *Washington Post*, December 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (accessed February 20, 2014).

of their communications, they do not have such an expectation for their metadata because this information has been shared with the third-party company that provides communications services.[31] As a consequence, such metadata enjoys significantly weaker privacy protections and the US asserts it may collect this data from phone and Internet companies without having to obtain a warrant from a court.[32]

The US government has relied on this interpretation to justify its bulk telephone metadata program, where the government has been collecting phone call records (though not call content) of potentially millions of calls to, from, and within the US.[33] While a similar metadata program for Internet use was shut down in 2011, nothing in the law would prevent bulk collection of other kinds of metadata in future programs. In addition, mass collection of Internet metadata may also be occurring under separate authorization, either in the US or overseas.

Officials have tried to play down the intrusiveness of such collections. Yet technologists now recognize that metadata can reveal an incredibly detailed portrait of a person's individual associations, interests, movements, and communications, especially when collected and analyzed in bulk.[34] The US should recognize the privacy interest in metadata and provide greater legal protections to prevent arbitrary and unlawful collection of such sensitive personal data.

Human Rights Watch and the Electronic Frontier Foundation urge the Committee to:

- Affirm that the acquisition or copying of personal information can constitute an interference with the right to privacy under Article 17, regardless of whether the information is subsequently processed, examined, or used by the government.

---

[31] *Smith v. Maryland*, 442 U.S. 735 (1979).

[32] Obama Administration White Paper, "Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act," August 9, 2013, https://s3.amazonaws.com/s3.documentcloud.org/documents/750223/obama-administrations-legal-rationale-for.pdf.

[33] The number of call records actually collected under this program is still uncertain. A recent media report suggests that the program is less broad than first suspected, in part because of the growing popularity of mobile phones and challenges related to collecting mobile phone call records. However, even if the current program is no longer as broad, nothing in current US law would prevent telephone metadata collection on a mass scale. See Siobhan Gorman, "NSA Collects 20% or Less of US Call Data Program Doesn't Cover Records for Most Cellphones," *Wall Street Journal*, February 7, 2014, http://online.wsj.com/news/articles/SB10001424052702304680904579368831632834004 (accessed February 10, 2014); President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," December 12, 2013, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed February 10, 2014).

[34] See Written Testimony of Edward W. Felten to the United States Senate, Committee on the Judiciary, Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act, October 2, 2013, http://www.judiciary.senate.gov/pdf/10-2-13FeltenTestimony.pdf.

- Reiterate that at all stages—whether collection, use, dissemination, or retention—the invasion of personal communications data should be restricted by law to just that which is necessary and proportionate to a legitimate state purpose.
- Urge the US to recognize the privacy interest of all persons in metadata and provide greater legal protections to prevent arbitrary and unlawful collection of such personal data.

III. Mass collection of data is fundamentally arbitrary and disproportionate

Today, technology enables mass surveillance on a scope and scale that would have been unimaginable twenty years ago. The costs of electronic data storage and processing continue to fall and many more aspects of private life are now digitized, including sensitive information about health, movements, and associations. These changes have reduced the practical constraints that once limited manual collection, combination, and analysis of such data in bulk.

The Committee should find that indiscriminate collection, search, or retention of electronic information is fundamentally arbitrary and disproportionate. Dragnet searches or collection on large groups without some threshold showing of suspicion that the information to be acquired is necessary to protect national security, or another legitimate interest of the United States, should be presumptively impermissible.

Article 17 provides for the right of every person to be protected against arbitrary or unlawful interference with his or her privacy or correspondence. The UN Special Rapporteur on counter-terrorism and the Special Rapporteur on freedom of expression have affirmed that any permissible limitation must be provided in law, must be necessary for a legitimate aim, and must conform to the principle of proportionality.[35]

In addition to bulk metadata collection discussed in section II, several other programs may be interfering with the privacy of potentially millions of individuals worldwide. Two that are currently known, noted above, occur under Section 702 of FISA. First, 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.[36] According to available information and media reports, the US may be temporarily

---

[35] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/13/37, December 2009), paras. 16-19; UN Special Rapporteur on freedom of expression, April 2013 report, paras. 28-29.

[36] "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).

copying and searching through the contents of *all* Internet and telecom traffic flowing over US borders through these cables.[37]

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.[38] 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.[39]

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 million Internet communications a year under section 702 alone.[40]

Section 702 enables intelligence agencies to obtain yearlong programmatic warrants from the FISA court to conduct surveillance to acquire "foreign intelligence information."[41] For non-US persons, "foreign intelligence information" is defined too broadly 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.[42] 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

---

[37] Charlie Savage, "N.S.A. Said to Search Content of Messages To and From US", *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).

[38] "NSA slides explain the PRISM data-collection program."

[39] 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).

[40] 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).

[41] 50 USC 1881(a).

[42] 50 USC 1801(e).

against the arbitrary or disproportionate collection and subsequent use of the personal information of non-US persons not suspected of any wrongdoing.[43] Moreover, under the NSA's targeting procedures, agencies can monitor the communications not only of specific targets, but also all communications "about" a target.[44] 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.[45]

Restrictions on the right to privacy must conform to the principle of proportionality, and should not be used where less invasive techniques are available.[46] Mass collection of personal information is by nature indiscriminate and the "targeting" practices used by the NSA also appear to be overly broad.

Regardless of whether collection 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, 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 connection to terrorism—raising serious questions as to whether such surveillance is arbitrary or unjustifiable.

Human Rights Watch and the Electronic Frontier Foundation urge the Committee to:

- Recognize that the right to privacy requires any surveillance 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 and that the mechanisms of surveillance be proportionally tailored to that suspicion.
- Ask that the US clarify the scope of surveillance and intelligence gathering done under Section 702 of FISA and Executive Order 12333.

---

[43] 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.

[44] Ibid.

[45] 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. "NSA slides explain the PRISM data-collection program."

[46] UN Special Rapporteur on freedom of expression, April 2013 report.