KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

BULK DATA COLLECTION AND ELECTRONIC SURVEILLANCE BY THE UNITED STATES NATIONAL SECURITY AGENCY

February 12, 2014

Report Update
Shadow Report to the Fourth Periodic Review of the United States
110 Session of the Human Rights Committee, Geneva

Reporting Organization

CDT is a global civil liberties and human rights organization with a mission to keep the Internet open, innovative and free. Since the Internet's infancy, CDT has played a leading role in shaping the policies, practices and norms that have supported Internet openness and empowered individuals to more effectively use the Internet as speakers and active citizens. CDT files this report to update the Shadow Report[1] it filed on October 10, 2013.

Report Update: Presidential Policy Directive/PPD-28

On January 17, 2014, the White House issued Presidential Policy Directive 28 addressing Signals Intelligence Activities conducted by the United States government. PPD-28 articulates part of the president's plan for reforming government surveillance activities, including those conducted by the National Security Agency (NSA). Two provisions of this directive have significant human rights implications and warrant greater clarification in the United States review process.

I. Use of Communications Collected In Bulk

The first provision places important limitations on use of non-publicly available signals intelligence data collected in bulk. Information is collected "in bulk" if it is acquired without the use of discriminants, such as specific identifiers like an email address or phone number, or selection terms. According to Section 2 of the Directive, the United States government "shall use that data only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;

[1] Bulk Data Collection and Electronic Surveillance by the United States National Security Agency, October 10, 2013, available at https://cdt.org/files/pdfs/ICCPR-Shadow-Report.pdf.

(4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section."[2] Though the overbroad bulk collection of information would continue without significant limitation, these are significant use restrictions that, if applied broadly, would have strong human rights benefits.

However, as noted above, they only apply to information obtained through bulk collection. In addition, footnote 5 to PPD-28 indicates that none of these use restrictions apply "to signals intelligence data that is temporarily acquired to facilitate targeted collection." This raises questions that require clarification:

- Is surveillance conducted under Section 702 of FISA (the PRISM program) considered "bulk collection" to which these use restrictions would apply? If not, would the U.S. government consider applying these use restrictions to surveillance under Section 702?
- What constitutes temporary acquisition to facilitate targeted collection to which the use restrictions would not apply? In particular, if the retention period for particular information acquired in bulk is six months, one year, or five years, and the information is queried by use of discriminants during the retention period, do the use restrictions apply?
- To what particular bulk collection activities disclosed in the media in 2013 as a result of information leaked by Edward Snowden do the use restrictions apply? Do they apply to:

  (i) bulk collection of location information generated by use of mobile devices?[3]

  (ii) collection of information passing over the main communications links that connect data centers around the world, including Yahoo and Google data centers?[4]

  (iii) collection of text messages in bulk under the Dishfire program?[5]

  (iv) collection of email address books in bulk?[6]

---

[2] Presidential Policy Directive/PPD-28, Section 2, available at: http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[3] See, e.g., Barton Gellman and Ashkan Soltani, NSA tracking cellphone locations worldwide, Snowden Documents Show, *The Washington Post*, December 4, 2013.

[4] See, e.g., Barton Gellman and Ashkan Soltani, NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, *The Washington* Post, October 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. The article describes a joint project between the British intelligence agency GCHQ, and the NSA, code-named MUSCULAR. "For the MUSCULAR project, GCHQ directs all intake to a 'buffer' that can hold three to five days of traffic before recycling storage space. From the buffer, custom-built NSA tools unpack and decode the special data formats that the two companies use inside their clouds. Then the data are sent through a series of filters to "select" information the NSA wants and 'defeat' what it does not."

[5] See, e.g., James Gall, NSA collects millions of text messages daily in 'untargeted' global sweep, *The Guardian*, January 16, 2014, available at http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

II. Personal Information of Non-U.S. Persons

The second provision addresses the safeguarding of personal information collected through signals intelligence: "All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. 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." The directive goes on to call for policies and procedures that safeguard personal information collected from signals intelligence activities, stating that, "To the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality. . ."[7]

PPD-28 also requires that rules for dissemination and retention of personal information be the same for both U.S. persons and "non-U.S. persons" (people outside the United States who are not U.S. citizens or permanent residents). This could be an important human rights protection if applied broadly. Under current minimization rules, information about a U.S. person can be retained and disseminated in identified form only when the U.S.-person information is necessary to understand "foreign intelligence" information. This is an important protection for U.S. persons: their identity is masked in foreign intelligence that is shared outside the NSA unless their identity is needed to understand foreign intelligence. However, because "foreign intelligence" under Executive Order 12333 includes any information about the activities of foreign persons,[8] and because foreign persons' identifiers would often be necessary to understand their activities, the protection this affords non-U.S. persons is doubtful. This raises questions that require clarification:

- Will the U.S. clarify the circumstances in which a non-U.S. person's identifying information will be retained and disseminated in intelligence products, consistent with PPD-28?

---

[6] See, e.g., Barton Gellman and Ashkan Soltani, NSA collects millions of e-mail address books globally, *The Washington Post,* October 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. "Rather than targeting individual users, the NSA is gathering contact lists in large numbers that amount to a sizable fraction of the world's email and instant messaging accounts. … During a single day last year, the NSA's Special Source Operations branch collected 444,743 email address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail, and 22,881 from unspecified other providers…."

[7] Presidential Policy Directive/PPD-28, Section 4, available at: http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[8] According to Executive Order 12333, as quoted in footnote 2 to PPD-28, "foreign intelligence" means "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists."

- Will the U.S. implement PPD-28's protections for non-U.S. persons by amending the minimization procedures it has adopted in USSID-18[9] and Department of Defense Regulation 5240.1-R, [10] or, will it issue and make public new minimization procedures?

- Would the U.S. consider limiting the scope of the definition of "foreign intelligence information" in EO 12333 to the scope of "foreign intelligence information" in FISA,[11] which does not permit the collection of information that merely concerns the activities of foreign persons?

Conclusion

The United States' January 17 Presidential Policy Directive, PPD-28, contains elements that could be understood as reforms to promote human rights in the national security surveillance context, but the extent to which it will actually achieve this unclear. CDT issues this report update to encourage the U.S. to clarify PPD-28.

For further information, please contact CDT Policy Analyst Emily Barabas, ebarabas@cdt.org.

[9] United States Signals Intelligence Directive 18, issued 25 January 2011, sets forth U.S. person minimization rules for signals intelligence and is available at http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

[10] Department of Defense Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, DoD Regulation 5240.1-R, was issued in December, 1982 and is available at http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf.

[11] FISA defines "foreign intelligence information" that concerns a non-U.S. person as information that relates to the ability of the U.S. to defend against an attack or hostile act, sabotage, international terrorism, clandestine intelligence activities and information with respect to a foreign power or territory that relates to U.S. national security or foreign affairs. 50 USC 1801(e) available at http://www.law.cornell.edu/uscode/text/50/1801.