

Reproduced with permission from Privacy & Security Law Report, 13 PVLR 2101, 12/15/2014. Copyright © 2014 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

Changes to NSA's Bulk Collection Stall in Congress While Intelligence Community Continues Works to Implement Presidential Policy Directive 28



BY CHARLES A. BLANCHARD, RONALD D. LEE AND
NICHOLAS L. TOWNSEND

The Senate in November fell two votes short of advancing legislation to limit bulk metadata collection by the National Security Agency (NSA). The bill (S. 2685), which was introduced by Sen. Patrick Leahy (D-Vt.) and was mainly supported by Democrats, will likely face dimmer prospects when Republicans take control of the Senate in January 2015.¹ Although the House passed legislation (H.R. 3361) this year to

¹ S. 2685, 113th Cong. (2014), available at <https://www.congress.gov/113/bills/s2685/BILLS-113s2685pcs.pdf> (13 PVLR 2013, 11/24/14).

Charles A. Blanchard is a partner in Arnold & Porter LLP's Washington office and is a member of the firm's Government Contracts and National Security practices. Blanchard previously served as general counsel and chief ethics officer for the U.S. Air Force and as general counsel for the U.S. Army.

Ronald D. Lee is a national security and government contracts partner in Arnold & Porter's Washington office. Lee previously served as general counsel at the National Security Agency.

Nicholas L. Townsend is an associate in Arnold & Porter LLP's National Security and Public Policy practices in Washington.

curb bulk surveillance,² a number of U.S. technology companies supported the Senate bill over the House legislation, which they said contains “an unacceptable loophole.”³ The issue is expected to be hotly debated in the next Congress because Section 215 of the USA PATRIOT Act, which authorizes the NSA program, must be renewed by June of 2015.

For the time being, Congress's inaction leaves the issue of reforming the NSA's bulk collection in the wake of leaks by Edward Snowden to the executive branch, which has been working to implement the policy changes that President Barack Obama outlined in his January 2014 speech⁴ and Presidential Policy Directive 28 (PPD-28) regarding signals intelligence (SIGINT) activities.⁵ On Oct. 17, the Office of the Director of National Intelligence (ODNI) released a report on the

² H.R. 3361, 113th Cong. (2014), available at <https://www.congress.gov/113/bills/hr3361/BILLS-113hr3361rfs.pdf> (13 PVLR 918, 5/26/14).

³ Dustin Volz, *Google, Facebook Warn NSA Bill Wouldn't Stop Mass Surveillance*, Nat'l J., May 21, 2014, available at <http://www.nationaljournal.com/tech/google-facebook-warn-nsa-bill-wouldn-t-stop-mass-surveillance-20140521> (13 PVLR 918, 5/26/14).

⁴ President 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> (13 PVLR 165, 1/27/14).

⁵ Presidential Policy Directive—Signals Intelligence Activities (PPD-28) (Jan. 17, 2014), available at <http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (13 PVLR 165, 1/27/14).

implementation of PPD-28.⁶ ODNI's report, which was required under Section 4 of PPD-28, found that all elements of the intelligence community (IC) are on track to have policies and procedures in place to implement PPD-28 by Jan. 17, 2015.

The report states that “[m]ost agencies already have adequate existing procedures for some aspects of PPD-28.”⁷ However, updates to IC agencies' existing policies and procedures regarding handling information collected through SIGINT and the establishment of new policies and procedures will be required. In particular, the National Security Agency/Central Security Service (NSA/CSS) is developing a set of supplemental procedures to build the requirements of PPD-28 into the policy framework that governs the U.S. SIGINT System. ODNI's report anticipates that IC agencies other than the NSA will update their policies and procedures as well, but notes that the changes other IC agencies “will be required to make will be narrower than NSA's” because other IC agencies are generally consumers of SIGINT, rather than collectors.⁸

The ODNI report outlines key principles that all IC agencies must incorporate in their policies and procedures implementing PPD-28 in order to ensure protection for personal information collected through SIGINT. Such policies and procedures will:

- include limitations on the use of SIGINT collected in bulk, such as a restriction to use for the six purposes specified in PPD-28⁹ and prohibiting the use of SIGINT for suppressing or burdening criticism or dissent; disadvantaging individuals based on their ethnicity, race, gender, sexual orientation or religion; or affording a competitive advantage to U.S. companies and U.S. business sectors commercially;
- incorporate the principles for the collection of SIGINT outlined in PPD-28, including ensuring that new and unique SIGINT collection programs or significant changes to existing programs are au-

thorized by law and are not conducted for a prohibited purpose; ensuring that civil liberties and privacy protections are integral considerations in the planning and execution of SIGINT collection activities; and ensuring that such SIGINT activities are as tailored as feasible and that IC agencies focus collection on specific foreign intelligence targets or topics;

- set appropriate standards for querying SIGINT data, including seeking to structure queries or search techniques to identify intelligence information relevant to a valid intelligence or law enforcement task and minimizing the review of personal information not pertinent to intelligence or law enforcement requirements;
- establish that the mere fact that SIGINT is about a non-U.S. person is not sufficient to permanently retain or disseminate such information;
- consider as a default position subjecting non-U.S. person information to the same retention periods afforded to U.S.-person information under the U.S. attorney general approved guidelines;
- require that IC agencies make a written request to the ODNI for an extension of the five-year retention period that includes a specific justification for the extension and the views of the relevant privacy and civil liberties officer;
- establish procedures that permit dissemination of personal information of non-U.S. individuals collected through SIGINT only if the dissemination of comparable information concerning U.S. individuals would be permitted under Section 2.3 of Executive Order 12333;
- require adequate training as a condition of access or handling of unevaluated and unminimized personal information in SIGINT;
- make available information on how IC personnel report privacy and civil liberties complaints and other violations of law;
- require that, when a significant compliance issue involving personal information collected through SIGINT occurs, it must be reported promptly to the head of the IC agency who will notify the ODNI so that ODNI can determine if corrective action is necessary; and
- develop robust oversight and compliance programs to ensure adherence to PPD-28, including mechanisms for periodic auditing and review of each agency's practices for protecting personal information contained in SIGINT by privacy and civil liberty officers.

IC agencies' implementing policies and procedures will be publicly released to the maximum extent possible, consistent with classification requirements. Such policies and procedures will be carefully analyzed by privacy advocates and telecommunications, social media and other technology companies.

⁶ ODNI, *Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28* (July 2014), available at http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf; see also Robert Litt & Alexander W. Joel, *Interim Progress Report on Implementing PPD-28* (Oct. 17, 2014), available at <http://www.dni.gov/index.php/newsroom/reports-and-publications/204-reports-publications-2014/1126-interim-progress-report-on-implementing-ppd-28>.

⁷ ODNI, *supra* note 6, at 8.

⁸ *Id.* at 9.

⁹ Authorized purposes include: “(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; (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 above.” *Id.* at 4.