# FISA LEGISLATIVE REFORM PROPOSALS

## MATRIX KEY
### TO ACCOMPANY THE
### *FISA LEGISLATIVE REFORM MATRIX*

The FISA Legislative Reform Tables compare changes to the Foreign Intelligence Surveillance Act of 1978 as amended (FISA) proposed by (1) 31 bills pending in the House (21) and Senate (10); (2) the report by the Privacy and Civil Liberties Oversight Board (PCLOB) issued January 23, 2014; (3) the report by the PRG on Intelligence and Communications Technologies (PRG) issued December 12, 2013; (4) PPD 28 and the Remarks by the President on Review of Signals Intelligence given January 17, 2014, and (5) the December 9, 2013 Telecommunications Consortium Open Letter. The Matrix provides a topical overview of many of the current proposals to revise FISA in nine tables, each covering a general topic of reform with its sub-topics. This Key describes these general and specific categories of proposals in greater detail, highlighting illustrative or unique provisions.

The intelligence programs at issue collect and provide access to personal information about groups of non-U.S. citizens or of U.S. citizens and long term residents (U.S. persons), through various technologies – telephone call metadata, outgoing telephone call monitoring (pen register), incoming telephone call monitoring (trap and trace), internet communications, and various agency platforms, notably NSA applications for signals intelligence programs and FBI National Security Letters seeking diverse forms of personal financial and consumer information. While the Department of Homeland Security collects and analyzes aggregations of personal information about U.S. citizens linked to their travel and border crossing, reform legislation concerning bulk data collection and analysis centers exclusively on the intelligence and law enforcement communities.

### Elements of the Matrix

The reform bills, reports, and statements described in the Matrix and discussed in this Key cover the following subjects:

Table 1. Domestic and International Bulk Metadata Collection
Table 2. Targeting Non-U.S. Persons Outside the United States
Table 3. National Security Letters
Table 4. Foreign Intelligence Surveillance Courts
Table 5. Ancillary Non-Disclosure Orders
Table 6. Transparency and Oversight
Table 7. National Security Agency
Table 8. Privacy and Civil Liberties Oversight Board
Table 9. Miscellaneous Reforms

## Discussion of Key Elements

### TABLE 1. DOMESTIC AND INTERNATIONAL BULK BUSINESS RECORDS COLLECTION

a. Purpose
b. Telephone Records
c. Internet Records
d. Retention of Metadata (currently 5 years)
e. Custody of Metadata (currently held by NSA)
f. Prior Approval of Queries (NSA makes determinations of "reasonable articulately suspicion" (RAS))
g. Post-Hoc Judicial review of Queries (NSA provides monthly reports which discuss RAS standard to FISC)
h. Scope of Queries (returns results up to three hops away from query seed)
i. Subsequent Searches of Query Results (searches of corporate store do not need to meet RAS standard
j. Law Enforcement Use
k. Study of Metadata and Privacy
l. Alternatives to Bulk Collection

These proposals address the intelligence community's (IC) authority to obtain business records, including those of U.S. citizens and lawful residents, or any "tangible thing"[1] without a warrant in order to search and access the information for foreign intelligence purposes. Telephone call and internet records are the main focus of the current public debate and legislative attention.

The proposals modify Section 215 of the USA PATRIOT Act[2], which amended FISA to authorize the FBI to obtain any tangible thing for an investigation to obtain foreign intelligence information. The Foreign Intelligence Surveillance Court (FISC), the special Article III federal court that approves FBI applications for foreign intelligence surveillance, concluded in 2006 that Sec. 215 provides an adequate legal basis for properly constructed bulk collection and mining of telephone metadata including that of U.S. persons.[3]

---

[1] 50 U.S.C. § 1861(a)(1). The relevant portion of the statute states ""the Director of the [FBI] or a designee . . . may make an application for an order requiring the production of any tangible things . . . for an investigation to obtain foreign intelligence information not concerning a United States person *or* to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." *Id*.

[2] Section 215 of the USA PATRIOT Act amended Section 501 of FISA. Statement by DNI James Clapper September 10, 2013 "DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 501 of [FISA]", *available at* http://1.usa.gov/RP6fao.

[3] Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, 23 January 2014 [hereinafter PCLOB Report] at 57-9 stating "[s]ince 2006, the government has argued before the FISA court that Section 215 of the Patriot Act provides a legal basis for the NSA's bulk telephone records program. The FISA court has agreed and has authorized the program."

PPD 28, issued by President Obama on January 17, 2014 maintains the telephone metadata program under the following conditions: that the initial "collection store" of metadata be deleted no later than five years after initially collected; that during the period of transition from current collection to new standards and procedures, the FISC approve all government assertions that selectors for queries are supported by "reasonable articulable suspicion" (RAS) prior to performing a query of the metadata, except in emergencies;[4] that queries, which begin with an original number or "seed" may extend two tiers of contacts or "hops" further, thus taking in all of the seed's contacts (hop one) and all contacts of the seed's contacts (hop two); and that further queries of the resulting information do not need to be supported by any reasonable articulable suspicion.

Most of the proposals addressing bulk collection follow the President in ratifying such programs albeit with some modifications. Only a bill introduced by Congressman Holt entirely ends bulk collection as practiced today by returning the status quo to its pre-9/11 status.

**A. PURPOSES OF BULK COLLECTION:** Perspectives on the proper scope of records collection vary as to whether collection should center on international terrorism, counter-espionage, and foreign intelligence generally, or for the purpose of countering the wider set of contemporary security threats. President Obama has declared that bulk collection of non-publicly available signals intelligence is for the purposes of detecting and countering espionage, terrorism, weapons of mass destruction, cybersecurity threats, force protection, and transnational criminal threats. The default position of most of the bills is that of the current standard under FISA for an application to obtain tangible things, namely that the things sought be relevant to an authorized "foreign intelligence, international terrorism, or counter-espionage investigation."

**B. TELEPHONE RECORDS:** At opposite poles, the Telecommunications Consortium in its Open Letter states that government should limit surveillance "to specific, known users," while most of the proposals would continue the government's ability to obtain telephone records in bulk. The PRG recommends that Sec. 215 be amended to authorize the FISC to issue orders compelling third party disclosure of "otherwise private information about particular individuals."[5] **S. 1631**, Senator Feinstein's bill allows bulk collection where individuals or facilities are named or otherwise identified and where a series of other requirements are met.[6] (The terms "facility" or "facilities" are not defined in FISA and remain open to broad interpretation potentially encompassing entire portals of communication and/or transatlantic cables.)

---

[4] The FISC's assumption of this duty on February 5, 2015 was not unprecedented. "Over the course of approximately six months in 2009, the FISC required RAS determinations to be made by the FISC on a case-by-case basis after instances of NSA non-compliance with the FISC's previous orders were discovered and reported to the FISC by the Department of Justice." Edward Liu, CRS Report, "Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments" at 5, R.43459, April 1, 2014.

[5] Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies [hereinafter PRG Report] at 24, *see also* 86-89; 94-108.

[6] S. 1631 § 2.

One bill, **H.R. 2818**, by Congressman Holt, would repeal both the USA PATRIOT Act and the FISA Amendments Act of 2008 "thereby restoring or reviving provisions amended or repealed by such Acts as if such Acts had not been enacted, except with respect to reports to Congress regarding court orders under the Foreign Intelligence Surveillance Act of 1978 (FISA) and the acquisition of intelligence information concerning an entity not substantially composed of U.S. persons that is engaged in the international proliferation of weapons of mass destruction." The bill "prohibits information relating to a U.S. person from being acquired pursuant to FISA without a valid warrant based on probable cause."

**C. INTERNET RECORDS:** The Telecommunications Consortium states that governments should not undertake bulk collection of Internet communications. The collection of internet content in bulk falls under Section 702 of the FISA Amendments Act of 2008 (FAA) and is discussed further below.

**D. RETENTION OF METADATA:** The PCLOB proposes reducing the current government five year retention period to three years. Some bills, such as **H.R. 4291** put forth by Congressman Mike Rogers, would require telephone companies hold the information for longer than the 18 months currently required; the longest suggested period in a bill being 5 years, the same length of time the NSA currently holds the same data.

**E. CUSTODY OF METADATA:** The PCLOB would end government collection of bulk telephone metadata. The PRG would terminate NSA storage of bulk telephone metadata and transition it to being held by private providers or a third party. President Obama tasked the Attorney General and the IC with developing options other than the government itself holding telephone metadata. Rep. Rogers' bill would require the government to obtain telephone records from private carriers.

**H.R. 3875**, the Telephone Metadata Reform Act introduced by Congressman Schiff would remove "call data records"[7] from the possible tangible things for which the Director of the FBI or his designee could apply to the FISC; thus telecommunications providers would be the custodians of the data.[8] Without changing the current legal standard[9], the bill would authorize the FBI Director or his designee to apply for a call data production order from the FISC requiring a telecommunications carrier or carriers to

[7] The bill would define "call data record" to mean "communications routing information, including an original or terminating telephone number, an International Mobile Subscriber Identity, an International Mobile Station Equipment Identity, a trunk identifier, a telephone calling card number, the time or duration of a call, or original or terminating text-message numerical information."
[8] H.R. 3875 at § 2.
[9] The current standard requires that applications to the FISC for production orders include a statement of facts showing that there are "reasonable grounds to believe that the things sought are relevant to an authorized invitation [] to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities . . . ." 50 U.S.C. § 1861(b)(2).

produce call data records within 12 hours of receiving the order.[10] The bill would also authorize the FBI, without a court order, to direct a telecommunications carrier or carriers to search call data records and produce results within 6 hours of being directed to do so where the FBI Director or his designee determines that such records are required due to exigent circumstances and that applying for a normal order would "substantially delay an investigation."[11] Where such a directive is made by the FBI without a court order, the Director or his designee must also inform a FISC judge of the order within 24 hours of the exercise of that authority and make an application for an order for the call data records to a FISC judge within 5 days of the issuance of the directive.[12] For both FISC orders and FBI directives without a court order, the bill would impose nondisclosure requirements.[13]

**F. PRIOR APPROVAL OF QUERIES:** One approach maintains President Obama's current requirement under PPD-28 that an application be made to the FISC to determine the validity of each RAS determination, as proposed by the PRG. The FISC role which it assumed on February 5, 2014 was not unprecedented. Over a roughly six month period in 2009 the FISC itself required all "RAS determinations to be made by the FISC on a case-by-case basis after instances of NSA non-compliance with the FISC's previous orders were discovered and reported to the FISC by the Department of Justice."[14]

**S. 1631**, Senator Feinstein's bill permits the actual content of the telephone calls to be accessed only to "perform a query using a selector for which a recorded determination[15] has been made that there is a reasonable articulable suspicion that the selector is associated with international terrorism or activities in preparation therefore."[16] The PRG recommends that such orders could be issued only where the FISC finds that

---

[10] H.R. 3875 § 2. An application for a call production order would need to "specify each telecommunications carrier that the applicant requests be directed to search call data records and produce the results of such search" and include a statement of facts showing that there is a reasonable suspicion, based on specific and articulable facts, that the call data record to be used as the basis for the search is associated with a specific foreign terrorist organization, a specific clandestine intelligence activity, or specific foreign intelligence not concerning a United States person." *Id*. Where a FISC judge finds that such requirements are met, the "judge shall enter an ex parte order as requested, or as modified, approving the application." *Id*. The same section establishes categories of information that would qualify as "presumptively associated with specific foreign terrorist organization, a specific clandestine intelligence activity, or specific foreign intelligence not concerning a United States person." *Id*.

[11] *Id*. at § 2.

[12] *Id*.

[13] *Id*.

[14] Edward Liu, CRS Report, "Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments" at 5, R.43459, April 1, 2014.

[15] The bill would require a written record of any reasonable articulable suspicion ("RAS") determination "the selector, the identity of the individual who made the determination, the date and time of the determination, and the information indicating that, at the time of the determination, there was RAS that the selector was associated with international terrorism or preparation activities." For queries performed because of or based on such an RAS determination, the written record would be required to include "the identity of the individual who made the query, the date and time of the query, and the selector used to perform the query." S. 1631 § 2(j)(2).

[16] *Id*.

"the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect 'against international terrorism or clandestine intelligence activities' and "like a subpoena, the order is reasonable in focus, scope, and breadth."[17]

**H.R. 4291**, Rep. Rogers' bill would remove the FISC from direct oversight of government requests for metadata about United States Persons or facilities and thus from queries of that data as well.[18] Rather than approving an application to collect metadata regarding a specific individual or facility, the bill would require the FISC to approve selection procedures "reasonably designed to . . . minimize the impact of any acquisition authorized [] on the privacy and civil liberties of United States persons."[19] This would accomplish a similar process as that done by the FISA Amendments Act whereby the judicial oversight provided by the FISC is removed or diluted a level from approving individual applications to simply annually reviewing procedures.

**G. POST-HOC JUDICIAL REVIEW OF QUERIES:** These proposals use post-hoc review in several different ways. (1) Congressman Rogers' bill, **H.R. 4291** would allow the government to issue a directive to a service provider to collect metadata; after such collection the government would submit evidence to the FISC supporting its request, if the FISC disapproves it could but is by no means required to, order the government to purge the metadata. Requests for an emergency authorization of collection approved by the Attorney General and DNI would not need to be submitted to the FISC until seven days after the government decides to use this emergency provision.[20] Further, after the government submits a certification to the FISC regarding to these procedures, the government may amend and change that certification "at any time, including if the Court is conducting or has completed review of such certification or such procedures." Under the bill the amended certification need not be provided to the FISC until seven days after the government amends the procedures or certification.[21] After submission, while waiting for the FISC to issue a ruling, the "Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures."[22]

(2) The PCLOB proposes that the NSA provide RAS determinations to the FISC for review after they have been internally approved and used to query the database. (3) **S.1599** and **H.R. 3361**, the Sensenbrenner-Leahy reform bills, are called the *Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-*

---

[17] PRG Report at 24, *see also* 86-89; 94-108. *See* 105-107 discussing compliance issues and violations by NSA and reactions of the FISC, specifically by Judge Walton. Judge Walton concluded in one case that the NSA's minimization procedures had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively." PRG Report at 105 quoting In Re Production of Tangible Things From [Undisclosed Service Provider], Docket Number: BR 08-13 (March 2, 2009).
[18] H.R. 4291 § 11.
[19] *Id*.
[20] *Id*.
[21] *Id*. at "C. Amendments".
[22] *Id*.

*collection, and Online Monitoring Act*, or the USA FREEDOM Act. These bills rely exclusively on post-hoc determinations that are somewhat restrictive. (4) **S. 1599** eliminates bulk collection of telephony metadata except in emergency situations in which collection could only be authorized by the Attorney General[23] where he determines an emergency exists that would prevent filing for an application on time, that a factual basis under a statutory standard, and either the Attorney General or his designees informs a FISC judge at the time of the emergency authorization.[24] After an emergency authorization, an application meeting the standard outlined above must be submitted to a FISC judge "as soon as practicable, but not more than 7 days after" the Attorney General requires emergency production of call records.[25]

The standard the AG would have to meet in emergency situations is tougher than the RAS standard. Under the current statute, each application is required to include a statement of facts "showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[26] Where the applicant shows in the statement of facts that the things sought pertain to one of three categories of information[27] the "tangible things sought" are presumed to be relevant to an authorized investigation.[28] The USA FREEDOM Act would eliminate the presumption of relevance for applications under 215[29] and require additional steps be taken where the applicant seeks a nondisclosure requirement. Thus, under S.1599, the applicant's statement of facts would have to show reasonable grounds to believe that the tangible things sought *are relevant and material to* an authorized investigation to (I) obtain foreign intelligence information not concerning a United States person; *or* (II) protect against international terrorism or clandestine intelligence activities; *and* pertain to (I) a foreign power or its agent, (II) activities of a suspect agent of a foreign power who is the subject of an authorized investigation *or* (III) an individual in contact with, *or known to*, a suspected agent of a foreign power.[30] While the current FISA statute contains the "known to" language; neither that statute nor S.1599 contain a definition of the phrase as used.

**S. 1551**, Senator Wyden's bill would achieve many of the same reforms put forth by the Leahy-Sensenbrenner bill; it would also include amend Section 402 addressing pen registers and trap and trace authorities in its change of standards for FISA applications and otherwise

---

[23] S. 1599 § 502.
[24] *Id*.
[25] *Id*.
[26] 50 U.S.C. § 1861 (b)(2)(A).
[27] *Id*. These categories are where the "applicant shows in the statement of facts" that the information pertains to "(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation." 50 U.S.C. 1861 (b)(2)(A).
[28] *Id*.
[29] S. 1599. The bill would also change the standard from one of showing "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation" to a showing that " the records sought are "reasonable grounds to believe that the tangible things sought are relevant *and material to* an authorized investigation . . ." *Id*.
[30] S. 1599 § 502 (emphasis added).

**H. SCOPE OF QUERIES: S. 1631**, Senator Feinstein's bill may restrict the number of "tiers of contact" or "hops" from a given selector, though this is ambiguous. It provides access to such information to "return information concerning communications[:] to or from a selector in communication with the selector used to perform the query;" or "to or from any selector reasonably linked to the selector used to perform the query" in accordance with minimization procedures provided for later in the bill.[31]

**I. SUBSEQUENT SEARCHES OF QUERY RESULTS:** The PCLOB report would require a determination of reasonable articulable suspicion (RAS) prior to analysts querying "corporate store" where the collected data is held. The corporate store also contains results of contact chaining queries to the full corporate store.

**J. LAW ENFORCEMENT USE: S. 1701**, submitted by Senator Baldwin would amend FISA to apply the Classified Information Procedures Act (CIPA) to all Federal criminal proceedings wherein the court is notified that the government "intends to enter into evidence or otherwise use or disclose . . . against an aggrieved person any information obtained or derived from an electronic surveillance [under FISA] of that aggrieved person"[32] When the government seeks to disclose information obtained under those provisions of FISA for law enforcement purposes the bill would require the Attorney General or a presidentially appointed, senate confirmed designee to submit a certification "that this section is the grounds for the authorization for disclosure" within 30 days of the disclosure. Finally, the government would not be permitted to use information acquired pursuant to certain provisions of FISA "in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States or any State without the advance written authorization of the Attorney General."[33]

**K. STUDY OF METADATA AND PRIVACY:** The PRG recommends a study assessing the distinction between metadata and other types of information. President Obama requested his counselor John Podesta to lead a comprehensive review of big data and privacy. Neither the current bills nor the letter of the Telecommunications Consortium contain similar proposals.

**L. ALTERNATIVES TO BULK COLLECTION:** The PRG recommends that the government examine the feasibility of creating software that would allow intelligence

---

[31] S. 1599 § 2(j)(1, 3).

[32] 50 U.S.C. § 1806(c-d). The bill would also apply CIPA to Federal criminal proceedings where the FISA notice provision regarding physical searches is triggered. S.1701 § 2, amending 50 U.S.C. 1825.

[33] S. 1701 § 2. Such written authorization would be required to "include the reasons specific to the facts at issue for such authorization, the order of [the FISC or FISCR] . . . that permits the information to be acquired, and identifies this section as the grounds for such authorization" and "be made known to all the parties and adjudicators involved in a manner that complies with [CIPA]. *Id*.

agencies to more easily conduct targeted information acquisition. President Obama stated in his remarks that signals intelligence should be as tailored as feasible, and that alternative sources of information such as open diplomatic and public sources should be prioritized.

### TABLE 2. TARGETING NON-U.S. PERSONS OUTSIDE THE UNITED STATES

a. Minimization of U.S. person information (permits use of acquired U.S. person information in criminal proceedings)
b. Protection of non-U.S. persons
c. Applicability of Privacy Act to non-U.S. persons
d. Foreign targets entering the U.S.
e. Surveillance of foreign leaders

Currently § 702[34] of FISA provides for the Attorney General and Director of National Intelligence to jointly authorize, for up to a year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[35] Five enumerated conditions and annual review by the FISC of NSA's targeting and minimization procedures seek to prevent targeting of U.S. citizens. An exception to the FISC umbrella for exigent circumstances permits the Attorney General and DNI to authorize immediate acquisition under section 702, with a certification to the FISC within seven days. The current proposals for reform would amend section 702 to change requirements to collection and collection programs created under the authority of that statute.

The meaning of the authority granted here is difficult to understand precisely. The section appears to have been intended to authorize and also limit active intelligence programs exploiting the content of telephone and internet communications. It clearly anticipates the incidental collection of U.S. person information since U.S. citizens may be located where certain foreign intelligence is to be acquired, among other reasons. Sec. 702 counts on FISC review of targeting and minimization procedures to limit access to U.S. person information before collection and after presumably incidental collection, restrain its use, retention, and dissemination. But how its provisions relate to other parts of the statute, the degree of search or privacy protection citizens may claim under this provision, and how courts will interpret a geographically driven provision when it is applied to counter significant mobile threats are all questions that are hard to assess.[36]

---

[34] 50 U.S.C. § 1881a. This provision is entitled "Procedures for targeting certain persons outside the United States other than United States persons." *Id*.
[35] 50 U.S.C. § 1881a(a).
[36] Indeed, the titles of the statutory provisions demonstrate that the application of certain provisions turn on geographic location and (in part) citizenship of the target and others turn on the geographic location of the acquisition. *See* 50 U.S.C. 1881a entitled; 50 U.S.C. § 1881b entitled "Certain acquisitions inside the United States targeting United States persons outside the United States"; and 50 U.S.C. § 1881c entitled "Other acquisitions targeting United States persons outside the United States."

**A. MINIMIZATION OF U.S. PERSON INFORMATION:** These proposals define the types of minimization required for information about U.S. persons acquired in the context of Sec. 702 collection. The PRG recommended the purging of any U.S. person information unless it has foreign intelligence value or is necessary to prevent serious harm to others. The PRG also stated that the government should not search for U.S. persons in the data except to prevent a threat of death or serious bodily harm, or with a warrant based on probable cause to believe the person is planning or is engaged in acts of international terrorism. The Telecommunications Consortium would permit use of acquired U.S. person information in criminal proceedings. President Obama spoke of asking the Attorney General and DNI to institute reforms that place additional restrictions on the government's ability to retain, search, and use in criminal cases communications between foreigners and Americans collected under Sec. 702.

The bills emerging from the intelligence committees would do little to amend this section. **H.R. 4291**, by Rep. Rogers, would not amend or change any existing provision in section 702. **S. 1631**, Senator Feinstein's bill[37] would permit a query of the contents of communications acquired under section 702 with a selector "known to be used by a" USP where the query's purpose it "to obtain foreign intelligence information or information necessary to understand foreign intelligence information or to assess its importance."[38] The bill would also require a record be created for any query performed with a selector known to be used by a USP; such record would include the name of the personnel who performed the query, the query's date and time, and the information indicating that it was performed for the purposes outlined above.[39]

Other bills stake out positions closer to that of the PRG. **S. 1599**, the Leahy-Sensenbrenner USA FREEDOM Act repeals FISA procedures regarding targeting of non-U.S. persons located outside the United States to acquire foreign intelligence information as of June 1, 2015. It limits collection of wholly domestic communications of a U.S. person to those communications (1) to which any party is a target of the acquisition; or (2) that contain an identifier of a target of an acquisition, only if the communications are acquired to protect against international terrorism or the proliferation of weapons of mass destruction. It also prohibits searching of collections of communications of U.S. persons, except: (1) under an order or authorization for electronic surveillance or physical search, (2) with the consent of such person, or (3) under a reasonable belief that the life or safety of the person in threatened and the information is sought to assist that person.

**S. 1551**, Senator Wyden's bill prohibits (with exceptions) a government search of a collection of communications in order to find the communications of a particular U.S. person, and prohibits the use against any U.S. person of unlawfully obtained information, except with consent of such person or, if information indicates a threat of death or serious

[37] S. 1631 § 6.
[38] *Id*.
[39] *Id*. Each record made under this provision would be required to be made available to the DOJ, ODNI, the "appropriate Inspectors General", the FISC, and the HPSCI and SSCI. *Id*.

bodily harm to any person. It also requires the Attorney General to adopt procedures limiting the focus of content acquisition to international terrorism and requires acquisition authorization when a significant purpose is to acquire the communications of a particular, known person reasonably believed to be in the United States.

**B. PROTECTION OF NON-U.S. PERSONS:** The PRG and President Obama speak to the purpose of intelligence activities – protection of national security of the United States and our allies – and to prohibited ends of intelligence collection – competitive advantage to the private sector, suppression of criticism or dissent, disadvantaging of people based on their race, ethnicity, sexual orientation or religious beliefs. The PCLOB Report and the Report and Recommendations of the PRG on Intelligence and Communications Technologies discuss this issue in considerable detail.

**C. APPLICABILITY OF PRIVACY ACT TO NON-U.S. PERSONS:** The PRG proposes that the government apply the Privacy Act of 1974 in the same way to both U.S. persons and non-U.S. persons, as is the case at DHS with respect to travel information.

**D. FOREIGN TARGETS ENTERING THE U.S.:** The PRG proposes that the NSA have a limited statutory authority to continue to track known targets of counterterrorism surveillance when they first enter the United States, until the FISC has time to issue an order authorizing continuing surveillance here.

**E. SURVEILLANCE OF FOREIGN LEADERS:** President Obama declares that monitoring the communications of heads of state and government of close friends and allies may only be for a compelling national security purpose. The PRG proposes a five part test to determine whether such monitoring is appropriate, taking into account significant national security threats, the closeness of the relationship, duplicitousness by the foreign leader, alternative means of collection, and the impact of the monitoring becoming public.

## TABLE 3. NATIONAL SECURITY LETTERS

a. Issuance (issued without prior judicial approval)
b. Minimization Procedures
c. Records

These proposals would amend statutes governing the authorization, use, and non-disclosure of National Security Letters. Five federal statutes allow certain intelligence officials to request specific business record information in connection with a national

security investigation.[40] Authority to issue NSLs is comparable to the authority to issue administrative subpoenas. The USA PATRIOT Act, section 505 expanded the scope of four existing NSLs and added a fifth type of NSL.[41] Three NSLs are available exclusively to the FBI pursuant to the Electronic Communications Privacy Act (ECPA), the Right to Financial Privacy Act (RFPA), and (3) the Fair Credit Reporting Act (FCRA) (§505 of the USA PATRIOT Act).[42]

For the three original types of NSLs, the PATRIOT Act extended issuance authority from officials at FBI headquarters to heads of the FBI field offices (i.e., Special Agents in Charge [SACs]); it eliminated the prior requirement that the record information sought pertain to a foreign power or the agent of a foreign power, instead requiring that the NSL request be relevant to an investigation to protect against international terrorism or foreign spying.[43] Finally, the act required that no investigation using these NSLs "be predicated exclusively on First Amendment-protected activities."[44]

**A. ISSUANCE:** These proposals would change existing law governing the issuance of NSLs, the provisions of some bills that amend law regarding NSL nondisclosure orders are further discussed in Table 5 entitled "Ancillary Nondisclosure Orders."

Senator Leahy's bill **S. 1215**, the FISA Accountability and Privacy Protection Act of 2013, would revise procedures for obtaining judicial review of national security letter nondisclosure orders.[45] It would also permit a recipient of a nondisclosure order to request judicial review of the order and require the government to respond in a manner that sets forth specific facts in a certification to justify the need for nondisclosure based upon national security and other concerns.[46] The bill would also require the appropriate courts, in determining whether to grant a nondisclosure order, to give substantial weight to the facts as alleged by the government in its certification.[47] Finally, S.1215 would also dispense with the current conclusive presumption that disclosure of a nondisclosure order for tangible things would (i) endanger national security or a person's life or safety or (ii) interfere with a criminal or terrorist investigation or with diplomatic relations.

Additionally, Congresswoman Lofgren's bill, **H.R. 983** would amend ECPA to require the government to obtain a warrant under a uniform warrant standard to access to

[40] Charles Doyle, CRS Report "National Security Letters in Foreign Intelligence Investigations" at 1-5, RS22406, January 3, 2014.
[41] *Id*. The fifth category, Subsection 358(g) of the USA PATRIOT Act, amended the Fair Credit Reporting Act and notably, unlike the others, was available for use by any "government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism . . ." *Id*.
[42] *Id*. at 2.
[43] *Id*.
[44] *Id*. (emphasis supplied).
[45] S. 1215.
[46] *Id*.
[47] *Id*.

compel service providers to disclose stored communications.[48] **H.R. 3557** by Congressman Gosar would amend ECPA in similar ways.[49]

Finally, the PRG would have NSLs issued only upon a judicial finding that: (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities" and (2) like a subpoena, the order is reasonable in focus, scope, and breadth.[50]

**B. MINIMIZATION PROCEDURES:** The PRG recommends that "all statutes authorizing the use of National Security Letters should be amended to require the use of the same oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders."[51]

**C. RECORDS:** Senator Leahy's bill, **S. 1215** would require the FBI to retain an internal statement of facts that would demonstrate the relevance of information sought to its investigation prior to issuing a National Security Letter. This proposal is the only one of its kind.

**TABLE 4. FOREIGN INTELLIGENCE SURVEILLANCE COURTS**

a. Nature of proceedings (currently ex parte, but FISC has discretion to appoint amici)
b. Transparency in judicial proceedings
c. Technical assistance
d. Appeals
e. Selection of judges
f. Transparency of judicial opinions
g. Report and recommendations

These bills suggest changes to the Foreign Intelligence Surveillance Court (FISC) or the Foreign Intelligence Surveillance Court of Review (FISCR). Many bills would apply their proposed changes to both the FISC and the FISCR; some only address the FISC.

**A. NATURE OF PROCEEDINGS:** Current proceedings before these courts are typically *ex parte* and many aspects of the litigation are *in camera,* although the FISC has discretion to appoint *amici*. Some bills propose the establishment of an office of a permanent advocate, others would require the FISA courts to appoint an advocate to argue in the FISC and/or FISCR to provide the court(s) with a voice or viewpoint other

[48] H.R. 983.
[49] H.R. 3557.
[50] PRG at 24, 89.
[51] *Id*. at 25, 89-90.

than the applicant's in some or all cases, and still other bills would attempt to[52] grant the FISA courts discretion as to when to appoint an advocate. Currently four Senate bills and four House bills would change the nature of FISC and FISCR proceedings as would the PRG, the PCLOB, and the President himself.[53] These proposals differ in specifics including in the name of the advocate, the branch and office of government providing that person or in which the advocate's office would be created, whether the advocate could participate in court proceedings at his/her discretion, be required to participate in all proceedings, or only participate in proceedings when asked to do so by the FISC or FISCR.[54]

Rep. Rogers' bill, **H.R. 4291**, would allow the FISC in limited cases to appoint an *amicus curiae* from a list of individuals "who have been determined by the appropriate executive branch officials to be eligible for access to classified information"[55] and would be required to notify the Attorney General each exercise of their authority to make such an appointment.[56] The bill could permit executive branch attorneys, including attorneys working for the intelligence agencies, to be detailed to the FISC or FISCR or be appointed as the *amicus curiae*. [57]

By contrast, **S. 1551**, Senator Wyden's bill, would create an Office of the Constitutional Advocate within the judicial branch of the government. The Privacy and Civil Liberties Oversight Board (PCLOB) would submit a list of no less than five people and the Chief Justice of the Supreme Court would appoint the Constitutional Advocate from that list for a term of three years.[58] The Constitutional Advocate would review "each application to the FISA Court by the Attorney General; Each decision of the [FISC], the petition review pool, or the [FISCR] . . . and all documents and other material relevant to such decision in a complete, unredacted form . . . ." among other duties and abilities to participate in proceedings.[59]

---

[52] Some reports have suggested that current proposals regarding the FISC or FISCR's authority to appoint *amici curiae* could be redundant. Andrew Nola and Richard Thompson, CRS Report, " Reform of the Foreign Intelligence Surveillance Courts" at Summary, R.43362, January 16, 2014. "While formally codifying the FISA courts' authority in statute could arguably clarify the scope of the court's authority with respect to *amici* . . . it is unclear what legal difference a codification . . . ultimately makes, as the statutory authority is largely duplicative of the authority the FISA courts already possess as a matter of their inherent power." *Id*.

[53] In his January 17, 2014 Remarks by the President on Review of Signals Intelligence, the President said "To ensure that the court hears a broader range of privacy perspectives, I am also calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court." *Id*. *available at* http://1.usa.gov/1awEWY8.

[54] It should be noted that there exist some constitutional concerns regarding proposals for a public advocate or amicus in FISC or FISCR proceedings; such concerns emanate from the Appointments Clauses of the Constitution and Artilcle III. *See* Andrew Nolan et al., CRS Report "Introducing a Public Advocate into the Foreign Intelligence Surveillance Act's Courts: Select Legal Issues" at 8-27, 7-5700, October 25 2013.

[55] H.R. 4291 § 5(2-4).

[56] *Id*. at § 5 (5, 9(b)).

[57] *Id*. at § 5(6).

[58] S. 1551 § 402(1).

[59] *Id*.

Senator Feinstein's bill, **S. 1631** would also allow the FISC and FISCR "to appoint amicus curiae to assist the court in the consideration of . . . an order or review made to" either provided the application in the opinion of such a court, presents a novel or significant interpretation of the law."[60] This final caveat could narrow greatly the scope of the advocate's involvement as much of the work of the FISA courts involves renewal of applications previously approved or issues of law that have been decided at least once in the FISC and FISCR's histories since their establishment in 1978.

**B. TRANSPARENCY IN JUDICIAL PROCEEDINGS:** Senator Baldwin's bill, **S. 1701** would require notice be provided to an "aggrieved person" as defined under the notice provisions of FISA, of all information collected and used in an investigation relevant to a FISA criminal proceeding including the information in the government's possession but not intended to be intended into evidence.

**C. TECHNICAL ASSISTANCE:** The PRG recommends that greater technological expertise be available to the FISC judges. The PCLOB stated that the FISC and the FISC judges "should take advantage of their ability to appoint Special Masters or other technical experts to assist them in reviewing voluminous or technical materials, either in connection with initial applications or in compliance reviews." The PCLOB also recommended that the "FISC and the FISCR should develop procedures to facilitate amicus participation by third parties in cases involving questions that are of broad public interest, where it is feasible to do so consistent with national security."[61]

**D. APPEALS.** These proposals permit review from the FISCR to the Supreme Court or allow other changes to the current appeals process from a decision of the FISC. These sections usually accompany provisions that would create a special advocate position to allow such a person to appeal decisions of the FISC or the FISCR and/or to participate in proceedings at each level. The PCLOB stated that "Congress should enact legislation to expand the opportunities for appellate review of FISC decisions by the FISCR and for review of FISCR decisions by the Supreme Court."[62] Providing for such appellate review from rulings of the FISC and FISCR would "strengthen the integrity of judicial review under FISA. Providing a role for the Special Advocate in seeking that appellate review will further increase public confidence in the integrity of the process."[63]

**E. SELECTION OF JUDGES.** These proposals alter aspects of the current judicial selection process and/or the terms of service. Currently the Chief Justice of the Supreme Court publicly designates all 11 FISC judges from at least seven of the United States judicial circuits with no fewer than three residing within 20 miles of the District of Columbia.[64] The Chief Justice also publicly designates the three judges from the United States district courts or courts of appeal to serve on the FISCR.[65] Judges on both the

[60] S. 1631 § 4.
[61] PCLOB Report *supra* note 3 at 18.
[62] *Id*.
[63] *Id*.
[64] 50 U.S.C. § 1803(a)(1).
[65] 50 U.S.C. § 1803(b).

FISC and FISCR serve terms of a maximum of seven years.[66] The proposals vary from changing the length of judicial terms to changing the manner in which they are appointed.[67]

Senator Blumenthal's bill, **S. 1460** the FISA Judge Selection Reform Act of 2013 would expand the number of judges from 11 to 13 assigning the two new seats to a judge from DC Circuit and the Federal Circuit. It would also require that, upon a vacancy on the court, the Chief Judge of the circuit assigned to the vacant seas would nominate an Article III judge for the vacancy.[68] If the Chief Justice rejects the nominee and does not designate him or her to the FISA Court, he would request from the Chief Judge of the applicable circuit two more nominees from the that circuit and must choose one of those two to fill the vacancy.[69]

Another example is **H.R. 2586**, the FISA Court Accountability Act, introduced by Congressman Steve Cohen. This bill would divide appointments for the 11 FISC judges between the Chief Justice, who would select three, and would allow two judges each to be appointed by (i) the Speaker of the House, (ii) the House Minority Leader, (iii) the Majority Leader of the Senate, and (iv) the Minority Leader of the Senate.[70]

**F. TRANSPARENCY OF JUDICIAL OPINIONS.** These proposals amend current provisions in FISA to require disclosure of opinions or orders of the FISC and/or FISCR by the Attorney General. Proposals differ as to which opinions they would require to be declassified (all opinions, orders, etc. or opinions on a "novel or significant construction of law") and to whom the disclosures would be made (to each member of Congress, to the public, etc.) with some exceptions for withholding certain opinions. Bills or documents containing this suggestion usually require the Attorney General or another executive branch to produce a periodic report to Congress or publicly on the number of documents withheld under an exception or the general number of FISC or FISCR documents being disclosed. **S. 1130**, Senator Merkley's bill would amend section 702 to requires the Attorney General to disclose opinions of the FISC or FISCR that "include[] a significant construction or interpretation" of 702.[71] In total, 3 Senate bills and 10 House bills would require the disclosure of FISC and/or FISCR opinions.

**G. REPORT AND RECOMMENDATIONS:** S. 1460 by Senator Blumenthal proposes that the Committee on Intercircuit Assignments of the Judicial Conference of the United States would be required to report to Congress "on how to ensure that judges appointed to the FISA Court and the FISA Court of Review are diverse and representative" within one year of the bill's enactment.[72]

---

[66] 50 U.S.C. § 1803(d).
[67] *See* Menno Goedman, Reforming FISC: Legislative Proposals for Creating a More Balanced FISA Court, Harvard Law National Security Journal, Sept. 8, 2013, *available at* http://bit.ly/1qkWWuG.
[68] S. 1460.
[69] *Id*.
[70] H.R. 2586.
[71] S. 1130 § 4.
[72] S. 1460.

## TABLE 5. ANCILLARY NON-DISCLOSURE ORDERS

a. Issuance
b. Judicial Review
c. Duration

**A. ISSUANCE:** These proposals, including Senator Leahy's bill **S.1215** and the Leahy-Sensenbrenner bill, **S.1599/H.R. 3361** would impose additional requirements requiring more information for FISA applications seeking an accompanying or ancillary nondisclosure orders. Senator Wyden's bill, **S. 1551** would impose similar restrictions on the issuance of nondisclosure orders.

**B. JUDICIAL REVIEW**: These proposals would allow recipients of nondisclosure orders to challenge them in a new way. As one example, as discussed above, Senator Leahy's bill **S. 1215**, the FISA Accountability and Privacy Protection Act of 2013, for example, would revise procedures for obtaining judicial review of national security letter nondisclosure orders.[73] It would also permit a recipient of a nondisclosure order to request judicial review of said order and require the government to respond in a manner that sets forth specific facts in a certification to justify the need for nondisclosure based upon national security and other concerns.[74] The bill would also require the appropriate courts, in determining whether to grant a nondisclosure order, to give substantial weight to the facts as alleged by the government in its certification.[75] Finally, S.1215 would also dispense with the current conclusive presumption that disclosure of a nondisclosure order for tangible things would (i) endanger national security or a person's life or safety or (ii)interfere with a criminal or terrorist investigation or with diplomatic relations.

**C. DURATION:** These bills would alter or amend the current duration of a nondisclosure order. Again, **S. 1215** would amend FISA to eliminate the current requirement prohibiting recipients of a nondisclosure order from challenging the order within one year of receipt.

## TABLE 6. TRANSPARENCY AND OVERSIGHT

a. Aggregate reporting by providers/Immunity*
b. Aggregate reporting by government
c. Secrecy of government surveillance activities
d. Congressional reporting
e. Review of IC methods and priorities
f. IC oversight

[73] S. 1215.
[74] *Id*.
[75] *Id*.

g. Attorney General review
h. IG review
i. Privacy and Civil Liberties Policy Official
j. Privacy and Civil Liberties Impact Assessments
k. Future technological developments
l. Legislative sunset provisions

Transparency and oversight are dominant themes across the spectrum of proposals.

**A. AGGREGATE REPORTING BY PROVIDERS/IMMUNITY*:** These proposals encourage the recipients of FISA orders to disclose information about the government orders received and some of the bills, including Senator Franken's bill S. 1621, would accord immunity from lawsuits to providers. The Telecommunications Consortium seeks publication authority for the number and nature of demands for user information. The PRG and the PCLOB both recommend rules to allow recipients of orders to disclose general or statistical information, and President Obama committed to enabling such provider disclosure to the public. Four Senate bills and two House bills authorize enhanced voluntary disclosure by companies, including of the numbers of FISA orders they received and complied with, the amount of user information they produced, with a proviso that numbers under 500 should simply be identified as such. Two Senate bills and one House bill provide for immunity from any lawsuits resulting from such disclosure.

**B. AGGREGATE REPORTING BY GOVERNMENT:** The Telecommunications Consortium advocates for government to disclose the same information. The PRG recommends regular public disclosure general data about NSLs, section 215 orders, section 702 orders, and similar order, "unless the government makes a compelling case that such disclosures would endanger the national security," and the PCLOB similarly recommends public disclosure of more detailed statistics to provide a more complete picture of government surveillance operations. Five Senate bills and three House bills require substantial, detailed aggregate reporting of FISA orders by government.

**C. SECRECY OF GOVERNMENT SURVEILLANCE ACTIVITIES:** The PCLOB urges the government to begin developing principles and criteria for transparency including ensuring that the scope of surveillance authorities affecting Americans is public. The PRG promotes a presumption of disclosure for authorities and programs whose existence is unclassified and for programs of the magnitude of the bulk telephony metadata program, unless secrecy serves a compelling governmental interest and the efficacy of the program would be substantially impaired if our enemies were to know if its existence. No proposed congressional legislation addresses this topic.

**D. CONGRESSIONAL REPORTING:** The PRG recommends legislation requiring that Congress and the public be regularly informed about authorities such as those involving NSLs, Sec 215 business records, section 702, pen register and trap and trace, and the section 215 bulk telephony metadata program. Three Senate bills and four House bills expand reporting about FISA-governed activities to Congress.

**E. REVIEW OF IC METHODS AND PRIORITIES:** The PRG recommends that senior policymakers should review all sensitive intelligence requirements and methods on an ongoing basis. President Obama directed that the heads of departments and agencies contributing to signals intelligence priorities and requirements shall on an annual basis review and update their submissions.

**F. IC OVERSIGHT:** The PRG recommends establishment of "a mechanism" to monitor the collection dissemination activities of the IC to ensure they are commensurate with determinations of senior policymakers. President Obama directed the IC to ensure appropriate oversight of itself, to include periodic auditing and facilitation of IG and other relevant oversight entities.

**G. ATTORNEY GENERAL REVIEW:** **S. 1631**, Sen. Feinstein's bill, requires the Attorney General to review every five years all procedures that s/he approved for intelligence collection, including section 702 collection.

**H. IG REVIEW:** Two Senate bills and two House bills direct Inspectors General to conduct oversight of surveillance. **S. 1215**, Sen. Leahy's bill, requires IG audits on the use of Sec. 215 orders, NSLs and other surveillance authorities under the USA PATRIOT Act. The Senate-House Leahy-Sensenbrenner USA Freedom Act[76] requires DOJ IG to report on examination of minimization procedures used with business records requests from 2010 through 2013 and on results of audits of national security letters issued during 2010 through 2013.

Additionally, **H.R. 2399**, the LIBERT-E Act[77] put forth by Congressman Conyers would direct the DOJ IG and the Inspectors General of each IC element "authorized to acquire information pursuant to specified FISA orders" to jointly report to Congress "on the impact of such acquisitions on the privacy interests of U.S. persons."[78] The bill would also require the DOJ IG to make that joint report publically available "with any redactions limited to those necessary to protect properly classified information."[79]

---

[76] S. 1599 and H.R. 3361.
[77] This acronym stands for the "Limiting Internet and Blanket Electronic Review of Telecommunications and Email Act." H.R. 2399.
[78] H.R. 2399.
[79] *Id*.

**I. PRIVACY AND CIVIL LIBERTIES POLICY OFFICIAL:** The PRG recommends that a privacy and civil liberties policy official be placed on the National Security Staff and in OMB. President Obama directed such personnel to be identified to work with the IC and the Attorney General.

**J. PRIVACY AND CIVIL LIBERTIES IMPACT ASSESSMENTS:** The PRG proposes use of this new tool for assessing "big data and data-mining programs directed at communications" in order to "ensure that such efforts are statistically reliable, cost effective, and protective of privacy and civil liberties."[80] The group recommends a "broader and more policy-based" goal in these assessments to build in privacy considerations at every stage of the process.[81]

**K. FUTURE TECHNOLOGICAL DEVELOPMENTS:** The PRG recommends that program-by-program reviews be instituted for new technologies to flag and respond to emerging privacy and civil liberties issues, through the proposed PCLOB successor (the CLPPB) or other agencies.

**L. LEGISLATIVE SUNSET PROVISIONS: S. 1215** Senator Leahy's bill, shortens the sunset for the FISA Amendments Act to align it with the 2015 sunset of the USA PATRIOT Act and adds a new 2015 sunset for statutes authorizing NSLs. Two Senate bills and two House bills contain legislative sunset provisions.

## TABLE 7. NATIONAL SECURITY AGENCY

a. Leadership
b. Agency Mission
c. U.S. Cyber Command
d. Information Assurance Directorate

These proposals would reform the National Security Agency's organizational structure and leadership. These reforms are meant to enhance the agency's effectiveness,

[80] PRG Report at 22, 38-9, 229-30. The idea stems in part from the E-Government Act of 2002's requirement that federal agencies prepare Privacy Impact Assessments (PIAs) when procuring new or substantially modified IT systems.
[81] *Id*. As an example, the PRG Report states "for instance, policy officials should explicitly consider the costs and benefits of a program if it unexpectedly becomes public." *Id*.

to activate more governmental checks and balances on signals intelligence collection, and strengthen public confidence in the integrity of the intelligence process.

**A. LEADERSHIP:** These proposals would require the Director of the NSA to be appointed by the President and confirmed with the advice and consent of the Senate. The PRG recommends that the NSA Director be a Senate confirmed position,[82] while also suggesting that civilians be eligible for the position, and that the President "give serious consideration to" appointing a civilian as the next director.[83] Their report makes this recommendation "[b]ecause of the great impact of NSA actions, the need for public confidence in the Director, the value of public trust, and the importance of the traditional system of checks and balances. . . ."[84]

Senator Feinstein's bill recommends the Director of the NSA be Senate confirmed, Senator Feinstein's bill, S. 1631 would amend existing law[85] to require the NSA Director be "appointed by the President, by and with the advice and consent of the Senate."[86] The bill would also require the NSA's Inspector General be appointed by the President and confirmed by the Senate.[87]

**b. AGENCY MISSION:** The PRG recommends that "NSA should be clearly designated as a foreign intelligence organization."[88]

**C. U.S. CYBER COMMAND:** These provisions would separate the directorship of NSA and from the directorship of Cybercom. The PRG states that "there is a pressing need to clarify the distinction between the combat and intelligence collection missions" and that "military organization created under Title 10 of the US Code [] should be separate from the foreign intelligence agencies created under Title 50." 89 The group concludes that "[b]ecause the two roles are complementary but distinct, the Director of NSA and the Commander of US Cyber Command in the future should not be the same person." 90 The President has declined to support this proposal. S. 1631, Senator Feinstein's bill, would enact it.

**D. INFORMATION ASSURANCE DIRECTORATE:** The PRG suggests that once the NSA is "clearly designated" as an agency for foreign intelligence, "[o]ther missions (including that of NSA's Information Assurance Directorate) should generally be assigned elsewhere."[91]

---

[82] PRG at 34, 188-89.
[83] *Id*.
[84] *Id*. at 188.
[85] Specifically this section would amend 50 U.S.C. § 3602.
[86] S. 1631 § 8.
[87] *Id*. at § 9.
[88] PRG Report at 21.
[89] PRG Report at 34, 190-91.
[90] PRG Report at 191.
[91] *Id*. at 21.

## TABLE 8. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

a. Jurisdiction
b. Subpoena Authority
c. Whistleblowers
d. Technology Assessment
e. Compliance
f. Reports

These proposals would alter the structure and authorities of the PCLOB.

**A. JURISDICTION:** The PCLOB has jurisdiction to review executive branch actions taken to combat terrorism.[92] The PRG proposes "a newly chartered, strengthened, independent Civil Liberties and Privacy Protection Board (CLPP Board) to replace and "expand beyond the existing statutory limits of the existing"[93] Privacy and Civil Liberties Oversight Board (PCLOB)."[94] The new CLPP Board would have jurisdiction over counterterrorism operations as well as "other foreign intelligence purposes, including anti-proliferation, counter-intelligence, economic policy, and other foreign affairs purposes."[95]

**B. SUBPOENA AUTHORITY:** Two bills, the Leahy-Sensenbrenner USA FREEDOM Act, **S. 1599** and Senator Wyden's Intelligence Oversight and Surveillance Reform Act, **S. 1551** would amend the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to remove the Attorney General as the required intermediary for subpoenas connected to the authorized investigations and activities of the PCLOB.

**C. WHISTLEBLOWERS:** The PRG recommends that the CLPP Board be an authorized recipient for whistleblower complaints from employees of the IC.[96]

**D. TECHNOLOGY ASSESSMENT:** The PRG recommends that the CLPP Board include an Office of Technology Assessment to assess IC technology initiatives and support privacy-enhancing technologies.

**E. COMPLIANCE:** The PRG recommends that the CLPP Board absorb some compliance functions currently performed by NSA and other intelligence agencies.

---

[92] 42 U.S.C. § 2000ee.
[93] PRG Report at 178.
[94] *Id*. at 29.
[95] *Id*. at 196.
[96] *See* PRG Report 196-200.

**F. REPORTS:** The PCLOB recommends that the "Attorney General should fully inform the PCLOB of the government's activities under FISA and provide the PCLOB with copies of the detailed reports submitted under FISA to the specified committees of Congress." The PCLOB also states that this "should include providing the PCLOB with copies of the FISC decisions required to be produced under statute."[97]

## TABLE 9. MISCELLANEOUS REFORMS

a. Evidentiary reforms
b. Other legislative changes

These are other significant proposals that appear in at least one report or bill but do not fit into the above delineated classifications.

**A. EVIDENTIARY REFORMS:** These provisions would limit the ability of various fora to receive in evidence information obtained via impermissible collection, acquisition, or searching. Some bills would change FISA provisions that address receipt of evidence by either expanding or narrowing their scope, others would make changes to the Federal Rules of Civil Procedure or the Classified Information Procedures Act (CIPA). For example, S. 1599, the USA FREEDOM Act specifies that where an application for a 215 order is denied or "or in any other case in which the emergency production of call detail records under this section is terminated and no order under section 501 is issued approving the required production of such records" then no "information obtained or evidence derived from" the records shall be "received in evidence or otherwise disclosed in any proceeding[98] and no information concerning a U.S. person "shall be subsequently used or disclosed in "any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person."[99]

**B. OTHER LEGISLATIVE CHANGES:** Several bills make changes that would not fit into other categories in the matrix, for example, two bills would reform ECPA to prohibit the collection of customer password information. Highly relevant to the debate is Senator Rand Paul's Fourth Amendment Preservation and Protection Act of 2013, S. 1027, which would overturn the Third Party Doctrine in all instances under Federal law; among its many legal repercussions, this bill would have the effect of prohibiting bulk collection as

[97] PCLOB Report at 20. The statute at issue is 50 U.S.C. § 1871(a)(5). This "requires the congressional intelligence and judiciary committees to be provided with decisions, orders, and opinions from the FISC, and from its companion appellate court, that include significant construction or interpretation of FISA provisions." PCLOB Report at 20 n.24.
[98] PCLOB Report at 20. The bill specifies that such information shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof." *Id*.
[99] *Id*.

well as requiring more particularized collection of information under FISA from telecommunications providers.

## SUMMARY OF PROPOSED REFORMS

Most of the proposals described in the matrix bow to the government's extension of surveillance methods to new technologies and to greater collection of U.S. person information. Post-9/11 statutes expanded the types of materials that could be requested and collected, limited the judicial review to procedures for collecting and managing signals intelligence, and lowered the standard for FISC approval of applications. The pending proposals build on the expansion of access to information about individuals that the PATRIOT Act and the FISA Act Amendments grafted onto the original FISA.

The proposals are relatively narrowly conceived, designed to provide a framework for certain types of surveillance programs that have been implemented by the government, especially telephone metadata collection about U.S. persons and foreign intelligence programs focused on internet content and telephone call information that inevitably gather U.S. person information. The impact on future technological innovation is unclear. The bills differ as to the necessary predicates for collection, most providing some real if relatively modest constraints. Most of the proposed legislation would not alter the current use of geography as a proxy for U.S. personhood thus, the impact on intelligence and law enforcement community access to U.S. person information remains somewhat unclear. Outlier bills would end any intelligence community access to third party records or otherwise end bulk collection as applied to U.S. persons.

Along with expanding intelligence community authorities, many of the bills seek to strengthen executive branch, administrative, and FISC review, including by a strengthened FISC and FISCR and by the PCLOB or a more broadly conceived successor entity, by Congressional oversight, and through more government transparency to the public. In the wake of the Snowden revelations, the bills devote greater attention to balancing transparency with secrecy needs, and while the oversight field remains crowded with overseers and it is not thoughtfully developed.

Overall the proposals are worth reviewing carefully for practical, consensus steps as well as problem points, including for the intelligence community. They are an important reflection of the Congressional response to public opinion, especially with regard to domestic surveillance, and given the bills' similarity on some points, a collation of them has the potential to pass Congress. Nevertheless, SCLNS is unlikely to be able to simply ratify a basket of these proposals. For the most part they lack a deeper conceptualization taking into account technological developments, the security issues, or a consensus vision of the constitutional principles at stake. Their calibration of the intelligence process is therefore unreliable. As has been discussed in SCLNS a more "blue sky" approach is likely required.