BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice
At New York University School of Law
Washington, D.C. Office
1730 M Street, N.W.
Suite 413
Washington, D.C. 20036
202.249.7190 Fax 202.223.2683

March 14, 2014

To the members of the Privacy and Civil Liberties Oversight Board:

Thank you for the opportunity to address the board regarding Section 702 of the FISA Amendments Act and to submit these written comments in advance of my testimony. The Board is already familiar with the public disclosures about the programs evidently being carried out pursuant to Section 702 – notably, the PRISM program and so-called "upstream collection" – so I will not repeat that history here. The aim of my written comments is to address the statutory implications of the NSA's collection of communications "about" – rather than to or from – a target, and to suggest matters on which additional transparency is needed.

Board's mandate

Although it is familiar to the Board, let me begin by reiterating the Board's legislative mandate. The Board is directed to review proposed legislation and the implementation of new and existing legislation, and to assist in "ensur[ing] that privacy and civil liberties are appropriately considered in the development and implementation" of legislation.[1] This language provides the Board with a broad platform from which to make observations and recommendations about Section 702. To the extent that privacy and civil liberties may not have been "appropriately considered in the development" of Section 702 – that is, if Section 702 as drafted and passed is insufficient to protect Americans' privacy and civil liberties – that would be within the purview of the board. To the extent that the implementation of Section 702 has revealed defects in the protections for privacy and civil liberties, that would be an appropriate matter for the Board as well.

Collection of communications "about" a foreign intelligence target

Last year saw the disclosure of two sets of procedures – one on targeting and one on minimization – that govern the NSA's acquisition, usage, handling, retention, and destruction of communications obtained pursuant to Section 702. These procedures reveal that the NSA has

construed Section 702 to give it the authority to obtain emails and other communications that mention or refer to a "target," even if the communication is not sent from, or addressed to, the target.

Specifically, the 2009 targeting procedures, which have not been officially declassified, provide that the NSA may "seek[] to acquire communications **about the target** that are **not to or from the target**."[2] In other words, electronic communications between two parties with no connection to terrorism may be acquired if they include a reference to a "target"; those communications could involve United States persons, although the Agency must direct its surveillance at a party believed to be outside the United States.[3] And under the 2011 minimization procedures, which have been declassified by the Office of the Director of National Intelligence, once a communication is acquired and reviewed, "NSA analyst(s) will determine whether it is a domestic or foreign communication **to, from, or about** a target and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed."[4]

The Board has requested input regarding whether Section 702 of the FISA Amendments Act authorizes this "about" collection – that is, collection of communications "about" a target, where the target is not on the "to" or "from" side of the communication.

The statute itself does not explicitly answer this question. Section 702 authorizes the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information," with certain limitations related to the intentional targeting of U.S. persons or persons known to be within the United States.[5] The statute does not, however, resolve *how* a target might be used in acquiring communications; instead, it defers to the targeting and minimization procedures to establish the specific circumstances under which otherwise authorized communications can be acquired.[6] As noted above, the publicly available targeting and minimization procedures then simply state that "about" communications may be collected.

In addition, neither the statute nor the publicly available targeting and minimization procedures define "target."[7] While the statute implies (by referring to the "targeting of persons") that a target must be a person, it appears that a target might in practice be a phone number, email address, or other communications-related identifier.[8]

Nevertheless, an answer to the Board's question may be found in the structure and purpose of the statute. Section 702 effectively imposes two central restrictions on the collection of communications: the acquisition may not target U.S. persons or persons known to be within the United States (a geographic and nationality/residence restriction), and the acquisition must be for the purpose of acquiring foreign intelligence information (essentially a content restriction). Specifically, Section 702 provides that the Attorney General and Director of National Intelligence may jointly authorize "the targeting of persons reasonably believed to be outside the

United States to acquire foreign intelligence information"; enumerates a number of restrictions intended to ensure that communications are not intentionally collected pursuant to this authority from U.S. persons or from anyone located within the United States; and further requires that the Attorney General and Director of National Intelligence provide a certification meeting certain specifications, including both the geographic and nationality restrictions and the requirement that a "significant purpose of the acquisition is to obtain foreign intelligence information."[9]

Under this statutory structure, the *content* that is subject to electronic surveillance is regulated by the "foreign intelligence purpose" restriction, while the *people* who are subject to electronic surveillance is regulated by the targeting restrictions. The collection of "about the target" communications, by contrast, conflates the "who" with the "what." Moreover, the results of this collection are in plain tension with the "foreign intelligence" requirement of the statute: collecting communications that merely mention certain targets is guaranteed to acquire significant quantities of communications that contain no "foreign intelligence information" even under the statute's very generous definition of the term, thus undermining the "significant purpose" requirement. For instance, an electronic communication that mentions "Al-Shabab" or "AQAP" could be collected under the NSA's interpretation of Section 702 even though the email could be, among other things, related to an academic dissertation about terrorism in the Middle East or simply discussing a recent news story. Furthermore, as a practical matter, it appears that the NSA in fact acquires tens of thousands of wholly domestic communications under its ostensible authority to collect "about" communications.[10]

Notably, even the Supreme Court appears to have been under the impression that an American's communications could be collected only if he or she was in direct communication with a foreign intelligence target, and may have relied on representations by the U.S. Solicitor General in reaching this conclusion.[11] This significant misunderstanding suggests that the NSA is interpreting its authority under Section 702 in a way that is at fundamentally odds with the facial meaning of statute.

Unanswered questions about Section 702

One of the significant challenges for both the Board and the public when it comes to analyzing the import and reach of Section 702 is the amount that remains unknown about the programs carried out under its authority. The major surveillance program enabled by Section 215 (the collection and storage of Americans' telephone metadata) is now relatively well known and understood; by contrast, new disclosures regarding the reach of Section 702 continue to emerge. Indeed, some of the documents that have been disclosed raise as many questions as they answer. Without revealing operational sources and methods, the PCLOB could make a significant contribution to the public's understanding of the ways in which Section 702 is used to acquire communications of both U.S. persons and foreigners. These matters include:

Existence and operation of programs under Section 702

- How do programs carried out under Section 702 operate in practice? Much remains obscure about the scope of PRISM and upstream collection, the two programs known to operate pursuant to Section 702 authority. To the extent that additional details regarding these programs can be revealed without disclosing properly classified matters, they would contribute significantly to the public's understanding of the government's widescale surveillance. In addition, what other programs are being carried out under Section 702?

- Is Section 702 being used to carry out "bulk collection"? That is, are all communications acquired using specific selectors (which may nonetheless result in the collection of large amounts of data), or are communications being gathered in bulk for analysis down the line (as with the Section 215 phone metadata program)? This question is particularly relevant in light of Presidential Policy Directive 28, which applies special limitations to the use of signals intelligence collected in bulk.[12]

- What kinds of selectors may be used to gather communications, both in terms of "soft" selectors (e.g., communications in a particular language), and "hard" selectors (e.g., communications mentioning a particular target)? Understanding that the Board may not be able to reveal specific selectors that are currently in use, are the selectors used broad enough to allow collection of any communications referring to, for example, Russian President Vladimir Putin? Or any communications originating from or sent to particular countries or regions? And if they are broad enough to allow such collection in theory, are there any limitations that restrict the collection in practice? If so, how are those limitations overseen, and who has the authority to revise them?

- Relatedly, what is the process by which selectors are determined and overseen? Does the Foreign Intelligence Surveillance Court have any role in reviewing either the selectors themselves or the process by which they are chosen? Are the selectors made known to the relevant House and/or Senate oversight committees so they can help ensure that the selectors – even if responsive to individual intelligence requests – are not resulting in unduly broad collection?

- Is there a distinction between "targets" and "selectors"? In the absence of a statutory definition of "target," is there a working definition that the NSA uses in identifying targets? Are those targets narrower or broader than the selectors that are used to pull out communications for review?

Retention and sharing of information obtained under Section 702

- The 2011 minimization procedures state that U.S. person identifiers may be used as selectors to conduct searches within Section 702 databases, as long as (1) communications acquired via "upstream" collection are not searched and (2) the searches occur in accordance with NSA procedures.[13] Have these procedures been developed and implemented, and have such so-called "back door searches" actually been executed? What criteria, if any, must be met in order to conduct such a search (e.g., "probable cause," "reasonable articulable suspicion," "foreign intelligence purpose," or something else)?

- The minimization procedures permit the retention of domestic communications that are "reasonably believed to contain technical data base information … or information necessary to understand or assess a communications security vulnerability."[14] This provision goes on to state that "[i]n the context of a cryptanalytic effort, maintenance of technical data bases requires retention of **all communications that are enciphered** or reasonably believed to contain secret meaning…."[15] There has been speculation that this allows for retention of *all* communications that are sent via encrypted methods, including Tor or encrypted Gmail or other standard email products.[16] Is this accurate? If not, how is this provision interpreted?

- The minimization procedures indicate that domestic communications may be shared with law enforcement agencies if they are "reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed."[17] Must the actual or anticipated crime be of a certain severity to warrant the dissemination of these warrantlessly obtained communications, or may they be shared for any law enforcement purposes?

- Similarly, the minimization procedures provide that domestic communications may be disseminated or shared if "the communication contains information pertaining to a threat of serious harm to life **or property**."[18] What constitutes "serious harm to property"? Moreover, unlike the other provisions of the section on Domestic Communications, this provision does not contain any additional directives specifying with whom the information may be shared. May it be shared with private parties, if a private entity's property is threatened? If so, what minimization standards apply with respect to identifiable U.S. person information within that communication, and what limitations are there upon further sharing or dissemination by the recipient?

- The minimization procedures indicate that unminimized communications may be provided to the CIA and/or FBI, at which point they will be processed in accordance with those agencies' own minimization procedures.[19] Those minimization procedures have not been made public. What are the provisions of those procedures? Under what circumstances may the FBI and CIA use or share unminimized communications involving U.S. persons?

- Finally, the minimization procedures impose strict limitations on the sharing of communications acquired under Section 702 with foreign governments. Specifically, the procedures state that the NSA may disseminate unminimized communications to a foreign government only for technical or linguistic assistance, the foreign government may not make any further use of the information it receives, and the foreign government may not retain the information it receives.[20] Reporting has indicated, however, that unminimized communications were shared with at least one government for that government's use for its own purposes.[21] If true, how would such an agreement square with the declassified minimization procedures? And how does the NSA ensure that foreign governments comply with any commitments they undertake?

Recommendations to the Board

Finally, the Brennan Center has previously submitted comments to the Board, making a number of recommendations for the Board's consideration.[22] We reiterate those recommendations here and reserve the opportunity to submit further recommendations or other comments before the end of the comment period.

Thank you again for the opportunity to submit initial written comments. I look forward to speaking with the Board on March 19.

Sincerely yours,

Rachel Levinson-Waldman
Counsel, Liberty and National Security Program

[1] 42 U.S.C. § 2000ee(d)(1)(A)-(C).
[2] ERIC H. HOLDER, JR., U.S. DEP'T OF JUSTICE, 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 1 (2009), *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document (emphasis added).
[3] *Id.* at 1-2.

[4] ERIC H. HOLDER, JR., U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4 (2011) [hereinafter 2011 MINIMIZATION PROCEDURES], *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf (emphasis added).
[5] 50 U.S.C. § 1881a(a), (b).
[6] 50 U.S.C. § 1881a(c)(1).
[7] *See* 2 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2d, at § 17.5 (2d ed. 2012) (noting that Congress chose not to define the term "target" in the statute).
[8] *See*, *e.g.*, 2 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2d, at § 17.5 (2d ed. 2012) (explaining that even though "the target of a surveillance is the individual or entity about whom or from whom information is sought," a target could include not only the individual or entity but his or her phone number, email account, or other communications-related identifier); Margaret Hartmann, *NSA Collects Data 'About' Foreign Targets, Not Just Direct Communications*, NEW YORK MAGAZINE, Aug. 8, 2013, *available at* http://nymag.com/daily/intelligencer/2013/08/nsa-seeks-indirect-data-about-targets-abroad.html (quoting a former intelligence official acknowledging "an ambiguity in the law about what it means to 'target' someone"); Charlie Savage, *N.S.A. Said to Search Content of Messages To and From U.S.*, N.Y. TIMES, Aug. 8, 2013, *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?hp&pagewanted=all&_r=0 (citing a senior intelligence official indicating that the N.S.A. is "casting a far wider net for people who cite *information* linked to those foreigners, like a little used *e-mail address*") (emphasis added).
[9] 50 U.S.C. § 1881a(a), (b) (g)(2).
[10] [REDACTED NAME], [REDACTED NO.], slip op. at 34 & n.32 (FISA Ct. Oct. 3, 2011), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf (observing that the NSA's upstream collection "will acquire a wholly domestic 'about' SCT [Single Communication Transaction] if it is routed internationally" and estimating that the NSA "may be acquiring as many as 46,000 wholly domestic 'about' SCTs each year"); *id.* at 42-43 (noting that the collection of "about" MCTs (or Multi-Communication Transactions) likely involves the acquisition of "tens of thousands of additional communications of non-targets each year, many of whom have no relationship whatsoever with the user of the tasked selector").
[11] *See*, *e.g.*, Press Release, Office of Senator Ron Wyden, *Udall, Wyden, Heinrich Urge Solicitor General to Set Record Straight on Misrepresentations to U.S. Supreme Court in Clapper v. Amnesty* (Nov. 21, 2013), *available at* http://www.wyden.senate.gov/news/press-releases/udall-wyden-heinrich-urge-solicitor-general-to-set-record-straight-on-misrepresentations-to-us-supreme-court-in-clapper-v-amnesty.
[12] WHITE HOUSE, PRESIDENTIAL POLICY DIRECTIVE – SIGNALS INTELLIGENCE ACTIVITIES, Jan. 17, 2014, *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (defining "signals intelligence collected in 'bulk'" as "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants").
[13] 2011 Minimization Procedures at 6.
[14] *Id.* at 8.
[15] *Id.*
[16] *See, e.g.*, Andy Greenberg, *Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It*, FORBES, June 20, 2013, *available at* http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/; John P. Mello, Jr., *Encryption Lets NSA Store Your Email Forever*, TECHNEWSWORLD, Oct. 8, 2013, *available at* http://www.technewsworld.com/story/79117.html.
[17] 2011 Minimization Procedures at 8.
[18] *Id.* at 9 (emphasis added).
[19] *Id.* at 11.
[20] *Id.* at 12.
[21] *See* Glenn Greenwald, Laura Poitras, and Ewan MacAskill, *NSA shares raw intelligence including Americans' data with Israel*, THE GUARDIAN, Sept. 11, 2013, *available at* http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[22] BRENNAN CENTER FOR JUSTICE, COMMENTS TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, Sept. 18, 2013, *available at* http://www.noticeandcomment.com/PCLOB-2013-0005-0049-fcod-338144.aspx.