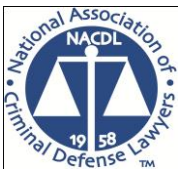

COMMENTS OF NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
Privacy and Civil Liberties Oversight Board
The Surveillance Program Operated Pursuant to
Section 702 of the Foreign Intelligence Surveillance Act
April 11, 2014
Docket ID: PCLOB-2013-0005-0085

The National Association of Criminal Defense Lawyers (NACDL) submits the following comments to the Privacy and Civil Liberties Oversight Board (PCLOB) in response to its hearing regarding the surveillance program operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA).

NACDL applauds the PCLOB for its premiere report on the telephone records program conducted under Section 215 of the PATRIOT Act and the Foreign Intelligence Surveillance Court (FISC). NACDL recognizes that the 702 surveillance program remains subject to more classification authorities than the 215 program, and understands that the PCLOB's report on the 702 program may be more limited in its public analysis than the 215 report. However, NACDL encourages the PCLOB, to the maximum extent consistent with national security, to make its report public, with limited redactions.

NACDL is a nonprofit organization committed to ensuring justice and due process for all persons accused of crime, fostering the integrity, independence and expertise of the criminal defense profession, and promoting the proper and fair administration of criminal justice. Such a policy respects cherished civil rights and liberties that are fundamental to our democracy. Persons have a right to expect privacy in their homes, movements, associations, and communications, and a right not to be deprived of their liberty or property without due process of law. It is within this context that NACDL submits these comments.[1] Additionally, NACDL

[1] NACDL has long opposed overbroad surveillance programs under FISA and the PATRIOT Act. *See* Letter from Coalition to Congress (May 21, 2009), *available at* Coalition Letter Urging Congress to Investigate Domestic Surveillance Laws; Letter from Coalition to United States Senate Committee on the Judiciary (September 30, 2009), *available at* Coalition Letter in Support of Amendments to the Reauthorization of the Patriot Act (S 1686); Letter from Coalition to House Committee on the Judiciary (October 29, 2009), *available at* Coalition Letter in Support of the USA Patriot Amendments Act of 2009 (HR 3845); Letter from Coalition to House Subcommittee on Crime, Terrorism, and Homeland Security (June 11, 2012), *available at* Coalition Sign-On Letter Re: Sunset of FISA Amendments Act of 2008; Brief for National Association of Criminal Defense Lawyers as Amici Curiae Supporting Respondents, Clapper v. Amnesty, 133 S.Ct. 1138 (2013) (No. 11-1025); *available at* https://www.nacdl.org/brief/Clapper-v-Amnesty-International-USA; Brief for National Association of Criminal Defense Lawyers as Amici Curiae in Support of Affirmance, In re Sealed Case, 310 F.3d 717 (For.Intel.Surv.Rev. 2002) (No. 02-001), *available at* https://www.nacdl.org/brief/In-Re-Appeal-from-July-19,-2002-Decision-of-the-Un.

joined a group coalition letter addressed to the PCLOB on June 18, 2013 endorsing several recommendations for reform of the 215 and 702 programs.[2]

The following comments focus on the use of information derived from Section 702 surveillance in criminal cases. While it is extremely difficult to comment on a surveillance program without actually knowing how it works or its full legal rationale, NACDL has a unique perspective on the real-world implications of the 702 surveillance program because its members include criminal defense lawyers, both in private practice and public defenders, who represent defendants in national security cases. Their first-hand experiences inform these comments. Because of the narrow focus of NACDL's expertise and the fact that the PCLOB has already reviewed dozens of comments from NACDL's non-governmental organization colleagues regarding issues with the Section 702 surveillance program, we incorporate by reference the American Civil Liberties Union's comments previously submitted to the PCLOB, which thoroughly address significant statutory, constitutional, and policy concerns associated with the 702 program, as well as cover the history of the FISA and the FISA Amendments Act (FAA) of 2008.[3]

These comments are divided into three sections: statutory issues, constitutional issues, and policy issues. Recommendations for reform are included in each section.

STATUTORY ISSUES

NACDL has serious concerns that the government has failed to provide notice of the use of Section 702 surveillance to obtain evidence—whether direct evidence or derivative evidence—it intends to use in a criminal trial, in violation of 50 USC Section 1806. Contrary to the Solicitor General's assertions to the United States Supreme Court in *Clapper v. Amnesty Int'l USA*,[4] it has not been the government's practice to provide notice to defendants in criminal cases when the government intends to use evidence originating from 702 surveillance. Media reports indicate that the government had a secret legal interpretation of the statute, namely of the words "obtained from" and "derived from", which did not require it to provide notice of the use of 702 surveillance authority in criminal cases.[5] Since the Snowden disclosures, however, the

[2] Letter from Coalition to Privacy and Civil Liberties Oversight Board (August 1, 2013), *available at* https://www.nacdl.org/Document/Letter-PCLOB-NSASurveillance-06182013.

[3] *Workshop regarding surveillance programs operated pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act*: *Before the Privacy and Civil Liberties Oversight Board* (July 9, 2013) (comments of the American Civil Liberties Union), *available at* http://www.noticeandcomment.com/PCLOB-2013-0005-0032-fcod-337494.aspx.

[4] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1154 (2013).

[5] *See, e.g.*, Charlie Savage, *Justice Dept. Defends Its Conduct on Evidence*, N.Y. Times, Feb. 14, 2014, at A11, *available at* http://www.nytimes.com/2014/02/15/us/justice-dept-defends-its-conduct-on-evidence.html?ref=charliesavage; Charlie Savage, *Warrantless Surveillance Challenged By Defendant*, N.Y. Times, Jan. 29, 2014, at A 15, *available at* http://www.nytimes.com/2014/01/30/us/warrantless-surveillance-challenged-by-defendant.html?ref=charliesavage; Charlie Savage, *Federal Prosecutors in a Policy Shift Cite Warrantless Wiretaps as Evidence*, N.Y. Times, Oct. 26, 2013, at A21, *available at* http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?ref=charliesavage.

government has amended this interpretation, which still remains secret. Therefore, the government argues it has in fact not violated the statute.[6]

Notice in Criminal Cases

50 USC § 1806 governs the use of information obtained pursuant to an individual FISA order (Title I collection) and information obtained under the 702 program (Title VII collection).[7] The standards for collection under the two programs differ. To collect information under an individual FISA order (Section 701), there must be probable cause to believe the "target" is a foreign power or an agent of a foreign power. Under 702, "the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[8] They must also certify that a *significant purpose* of the acquisition is foreign intelligence information, but they do not have to establish probable cause that the target of the 702 surveillance is a foreign power or an agent of a foreign power. Surveillance pursuant to the FAA/702 requires advance court approval of targeting *methods* rather than designation of a particular target based on individualized probable cause.

Unfortunately, Section 702 does not require the government to notify the FISC if it is using information obtained or derived from Section 702 in its application for an individual FISA order (Title I collection), or any other FISA order. This is significant because, as noted, the standards for collection under Title I and Title VII differ greatly. Moreover, the standard under 702 does not adequately protect Fourth Amendment rights of the individuals subject to surveillance.[9] Likewise, the failure to notify defendants of 702/Title VII surveillance implicates constitutional rights under the Fifth and Sixth Amendments.

Subsection (c) of Section 1806 discusses notification by the government of its intent to use information "obtained or derived from" Sections 701 and 702 in a trial. It provides, in part

> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court . . .

[6] In a recent filing in *United States v. Mohamud*, the government explains "The Department has always understood that it is required to notify any 'aggrieved person' of its intent to use or disclose, in a proceeding against such person, any information obtained or derived from Title VII collection as to which that person is an aggrieved person . . . . The Department's determination, however, that information derived from Title I or Title III collection may, in particular cases, also be derived from prior Title VII collection is a relatively recent development." "Prior to recent months, however, the Department had not considered the particular question of whether and under what circumstances information obtained through electronic surveillance under Title I . . . could also be considered to be derived from prior collection under Title VII. After conducting a review of the issue, the Department has determined that information obtained or derived from Title I . . . FISA collection, may in particular cases, also be derived from prior Title VII collection, such that notice concerning both Title I/III and Title VII collections should be given in appropriate cases with respect to the same information." The supplemental notifications the government has provided since the Snowden disclosures "demonstrate[] good faith, not misconduct," argues the government. Government's Response to Defendant's Motion for Full Discovery regarding Surveillance at 6-7, United States v. Mohamud, No. 3:10-CR-00475-KI (D. Oregon February 13, 2014) ECF No. 491.

[7] 50 USC § 1881e provides "Information acquired from an acquisition conducted under section 1881a of this title shall be deemed information acquired from an electronic surveillance pursuant to subchapter I for purposes of section 1806 of this title . . . ."

[8] 50 USC § 1881a(a).

[9] This is the case whether the acquisition is incidental or deliberate.

> against an aggrieved person, any information *obtained or derived from* an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial . . . notify the aggrieved person and the court . . . that the Government intends to so disclose or so use such information.[10]

It should be noted that this subsection does not specify if disclosure must state which section of FISA, (e.g., 701 or 702) was utilized to obtain the information the government seeks to introduce into evidence.[11] This matters because, as noted above, the standards for collection of the information are significantly different. This is also one of the reasons that there have not been any successful challenges to Section 702.[12] Prior to enactment of the FAA, all challenges were brought to individual FISC orders under Section 701 or other individual and particularized authorities. Post FAA enactment, defendants never know if information obtained pursuant to 702 (or 215 for that matter) was used to secure the individual order (or whether the evidence used to secure the individual order was derived from the same), leaving those sections free from meaningful challenge, at least until the June 2013 disclosures.

Motions to Suppress and Judicial Review

Subsection (e) of Section 1806 provides that the aggrieved person may move to suppress the evidence the government intends to introduce "on the grounds that (1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval."[13] Diligent defense lawyers file motions to suppress evidence obtained or derived from FISA surveillance even though they are never permitted to see the underlying application for the FISC order and the actual FISC order that authorized the surveillance.[14] For nearly 40 years, these lawyers have been arguing in the dark—asking courts to suppress evidence that they argue was not collected in conformity with the court's order, even though they will never see the order they are challenging.[15]

> "When there is such a motion or a discovery request for such documents, and once the Attorney General files an affidavit attesting that disclosure or an adversary hearing would harm national security, the District Court *must* review in

[10] 50 USC § 1806(c) (emphasis added).

[11] It should also be noted that 1806(c) as it stands may be incorrectly read not to mandate provision of notice where the information obtained or derived is from electronic surveillance of other persons that are not a party to the case.

[12] Since *Amnesty v. Clapper* and the Snowden disclosures, the government has amended its definition of "obtained and derived from" and provided notice in four cases of the use of evidence derived from Section 702 authorities. One of those cases, *United States v. Muhtorov*, is the first to challenge the constitutionality of section 702 in a confirmed case where the authorities have been used. *See* Defendant's Motion to Suppress Evidence Obtained or Derived From Surveillance Under the FISA Amendments Act and Motion for Discovery, United States v. Muhtorov, No. 12-cr-00033-JLK-1 (D. Colorado Jan. 29, 2014) ECF No. 520. *See also*, Ken Dilanian, *Use of overseas NSA wiretaps in domestic criminal cases facing legal challenges*, LA Times, April 6, 2014, *available at* http://www.latimes.com/nation/la-na-nsa-americans-20140407,0,629951.story#axzz2yPEtj8Wk

[13] 50 USC § 1806(e).

[14] *See, e.g., infra* note 13.

[15] For an example of this motion practice *see* defendant's motion to suppress evidence in the Bassaly Moalin case, prior to disclosures by Members of Congress that 215 and/or 702 surveillance may have been used in that case. Statement of Facts and Memorandum of Points and Authorities in Support of Motions, United States v. Moalin, No. 10-CR-4246 (SD Cal. Dec. 9. 2011) ECF No. 92-1, *available at* http://www.wired.com/images_blogs/threatlevel/2013/06/suppress.pdf (hereinafter *Moalin Memo*).

> camera and ex parte the application, order and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted."[16]

"In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 USC 1806(f). There is no similar discussion of such a process for section 215 (50 USC 1861). To date, no such information has been disclosed to an aggrieved person or his or her security cleared counsel,[17] even though access to traditional warrants and the underlying applications is routinely granted in the Title III wiretapping context.

If the surveillance was not lawfully authorized or conducted, it shall be suppressed; however, the statute says nothing about derivative evidence (which would likewise be precluded pursuant to the "fruit of the poisonous tree" doctrine).[18] The process for District Court review outlined in the FISA statute is different from the process courts follow to protect classified information in every other context, the Classified Information Procedures Act (CIPA).

Just like the Foreign Intelligence Surveillance Court, a District Court following the above described procedure never has the benefit of an informed defense perspective in determining whether the surveillance was lawful. The initial order stage is non-adversarial and so are all intermediate phases, including the last step of the legal/constitutional challenge to the collection (individual and programmatic) that occurs pretrial in a criminal prosecution. While the need for an adversarial hearing at the time of the FISC's initial consideration of broad scale surveillance programs may be debatable, in NACDL's view it is indisputable that, an adversarial viewpoint is essential in Article III proceedings in which a defendant faces criminal charges and a potential loss of liberty.

This is particularly the case because of the extremely technical nature of modern surveillance capabilities, and corresponding need for expertise. Moreover, often times the relevant compliance mechanisms are also technical in nature, or integrated into the NSA's IT infrastructure.[19] Additionally, in the event of a mistake or error it is not clear whether the NSA has a process to remedy tainted information that has already been disseminated to other agencies. An adversarial setting is essential for the introduction of technical expertise into the procedural process. This will help the courts' understanding of programmatic surveillance under non-particularized authorities, such as Section 702, including whether the relevant minimization procedures have been complied with.

---

[16] 50 USC § 1806(f) (emphasis added).

[17] In a Government filing from a terrorism-related case, the Government asserted "Indeed, to the Government's knowledge, no court has ever suppressed FISA-obtained or-derived information, or held an adversarial hearing on motions to disclose or to suppress." Kevin Poulsen, *Justice Department Fought to Conceal NSA's Role in Terror Case From Defense Lawyers*, Wired, June 18, 2013, *available at* http://www.wired.com/threatlevel/2013/06/nsa-defense-lawyers/ (includes link to government filing). However, a District Court Judge in Illinois has granted a defendant's motion to compel the underlying FISC documents in that case. That ruling is currently stayed pending appeal to the Seventh Circuit. United States v. Daoud, No. 1:12-cr-00723 (7th Cir. 2014).

[18] 50 USC § 1806(g).

[19] *See* John M. Delong, *For Agencies, the Intersection of Technology and Compliance Is Complex*, FedTech Mag., Feb. 4, 2013, *available at* http://www.fedtechmagazine.com/article/2013/02/agencies-intersection-technology-and-compliance-complex.

Meaningful reform of this provision would actually allow a traditional Article III court to review the legality and constitutionality of the FISA surveillance programs. NACDL believes the government's perfect record in FISA litigation in Article III courts is a function of the lack of adversary proceedings therein, and merely proves the point that ex parte proceedings are antithetical to fairness and justice.

Thus, surveillance under this program raises constitutional issues different from those implicated by the pre-existing FISA (Title I) provisions. Prohibiting challenge to the collection of information under Section 702 denies a fair trial by depriving the defendant of any meaningful opportunity to contest the acquisition and admissibility of evidence that may have been obtained unlawfully.

Classified Information Procedures Act

As noted previously, a court reviewing a motion to suppress or motion to compel discovery of FISA-derived information must follow the procedures outlined in the statute for in camera, ex parte review of the government's classified information. In 1984, six years after passage of FISA in 1978, Congress passed the Classified Information Procedures Act (CIPA) in order to address the issue of "grey mail."[20] However, Congress failed – and has since failed – to harmonize the provisions of CIPA with the pre-existing FISA framework. As a result, while CIPA creates and implements a system in which security-cleared defense counsel can review classified materials, that protocol – essential to due process – has not been applied to FISA.

In general, CIPA allows the Government to request a protective order from the court to protect against the disclosure of classified information disclosed by the Government to the defendant in a criminal case. The Government may then request to share redacted versions of documents including classified information, summaries of the documents, or substitutions of the documents, which only the judge sees in making a determination about whether or not that information may be shared with the defendant rather than the actual classified information.[21]

If a defendant intends to disclose classified information, he or she must first notify the government of the intention to do so, so that the government may request a hearing to address the issue prior to the disclosure of the information. If the Attorney General certifies that a public hearing may result in the disclosure of classified information, the hearing may be held in camera.[22]

If the judge determines that the classified information at issue is relevant and can be used in the case, the government can request to instead share a substitution or summary of the classified information rather than the actual classified information. A judge will permit this if he

[20] For a discussion of how CIPA should be amended to apply to FISA, *see* Josh Dratel, *Sword or Shield? The Government's Selective Use of Its Declassification Authority for Tactical Advantage in Criminal Prosecutions*, 5 Cardozo Pub. L. Pol'y & Ethics J. 171 (2006).

[21] 18 USC app. III §§ 3-4.

[22] *Id*. at §§ 5-6.

or she "finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information."[23]

If the court denies the government's motion, it orders the defendant not to disclose the classified information. The government then must decide to either appeal the decision or share the classified information/declassify the information. If the government loses its appeal and refuses to share the classified information, the judge may dismiss the case, or in the interest of justice take a less extreme measure and maybe instead dismiss certain charges, enter a finding against the United States on a particular issue to which the classified information relates, or strike part of the testimony of a witness (related to the classified information).[24]

Unfortunately, neither FISA nor CIPA have been amended – the former to incorporate CIPA's provisions for cleared defense counsel access to classified material, and/or the latter to apply explicitly to FISA materials—and the anomaly of security-cleared counsel uniformly being denied access to FISA materials continues.[25] Even though this process has been utilized in hundreds of national security cases and even in the Guantanamo military commissions, Congress has failed to apply it to FISA.

Recommendations for Reform

- The PCLOB should find that the plain meaning of the words "obtained from" and "derived from" apply to Section 1806, much like the Board's analysis of the word "relevant" in Section 215.
- The PCLOB should recommend that the government's secret interpretation of Section 1806 be released to the public.
- The PCLOB should recommend that Congress enact a clear statutory requirement that the government must provide notice to every defendant in every criminal case in which it intends to introduce into evidence (or use in any other way in any trial or proceeding) any information discovered through or derived from the use of surveillance under non-particularized authorities, such as Section 702 and/or Section 215.
- The PCLOB should recommend that the government immediately provide notice to every defendant—whether currently in the pre-trial, post-conviction, or post-sentence phases of a criminal case—of the use of surveillance under non-particularized authorities, such as Section 702 and/or Section 215, in their cases.
- The PCLOB should recommend that Congress enact a statutory requirement that the Government must disclose and identify to the FISC in its application for a 701 order, or any other individual order, any information it relies on in the application that was obtained by or derived from the use of surveillance under non-particularized authorities, such as Section 702 and/or Section 215.[26]

[23] *Id*. at § 6(c)(1).

[24] *Id*. at § (6)(e)(2)(A-C).

[25] While CIPA is not perfect in our view, it currently provides the government protection of the surveillance sources and methods it would like to keep secret.

[26] 50 USC § 1804(a)(3).

- The PCLOB should recommend that Congress amend FISA's suppression process under Section 1806 to reflect current CIPA practice. This must apply to Sections 215, 702 and 701, including a recommendation that Congress enact a statutory requirement that the government's underlying application for a FISA order, whether under 215, 701, or 702, and the resultant order be disclosed to security cleared counsel in criminal cases.
- The PCLOB should recommend that Congress enact a statutory requirement that derivative evidence discovered from unlawfully obtained or conducted FISA surveillance should also be suppressed, unless one of the traditional Fourth Amendment exceptions applies.

CONSTITUTIONAL ISSUES

As noted above, the standard for general collection under Section 702 does not adequately protect Fourth Amendment rights of the individuals subject to surveillance. Likewise, the failure to notify defendants of 702 surveillance, including surveillance used by way of "parallel construction," implicates constitutional rights under the Fifth and Sixth Amendments. Finally, infringements on the attorney-client relationship implicate the Sixth Amendment right to effective assistance of counsel and right to a fair trial, and the Fifth Amendment right to due process and a fair trial.

"Parallel Construction"

On August 5, 2013, *Reuters* reported that "[a] secretive U.S. Drug Enforcement Administration unit is funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans. Although these cases rarely involve national security issues, documents reviewed by *Reuters* show that law enforcement agents have been directed to conceal how such investigations truly begin - not only from defense lawyers but also sometimes from prosecutors and judges."[27]

A document reviewed by *Reuters* from the DEA Special Operations Division (SOD) to partner agencies, such as the FBI, CIA, NSA, IRS and DHS, instructs that no information gleaned from the SOD information sharing program should ever be mentioned in "any investigative function," like "investigative reports, affidavits, discussions with prosecutors and courtroom testimony."[28] Agents are then instructed to use "parallel construction" to cover up the source of the information—normal law enforcement investigative techniques that lead to the discovery of the crime at issue without disclosing the use of the shared information. For instance, if NSA obtained information is shared by the DEA SOD with the FBI to tip them off to drug trafficking, the FBI agents are instructed not to disclose that they learned of the suspect

[27] John Shiffman and Kristina Cooke, *Exclusive - U.S. directs agents to cover up programme used to investigate Americans*, Reuters, Aug. 5, 2013, *available at* http://uk.reuters.com/article/2013/08/05/uk-dea-sod-idUKBRE9740HP20130805.

[28] *Id*.

from the shared information, but rather through legitimate law enforcement techniques, such as a valid stop of a vehicle, followed by a dog sniff, which lead to the discovery of contraband.

Also on August 5, 2013, the *Houston Chronicle* revealed that information sharing from the DEA SOD has also resulted in the prosecution of non-drug-related crimes, such as Foreign Corrupt Practices Act violations.[29] A few days later, *Reuters* revealed that the IRS manual from 2005-2006 included 350 words on this SOD information sharing and "parallel construction" program.[30] The manual was discovered by Reuters on Westlaw, a sister company to Reuters.[31] The IRS manual (dated 2004) provides in part:

> Special Operations Division disseminates intelligence in the form of work products, leads, and tips. Department of Justice closely guards the information provided by SOD with strict oversight. The classified nature of all of these leads prevents their utilization in investigative or court reports. Usable information regarding these leads must be developed from such independent sources as investigative files, subscriber and toll requests, physical surveillance, wire intercepts, and confidential source information. Information obtained from SOD in response to a search or query request cannot be used directly in any investigation (i.e. cannot be used in affidavits, court proceedings or maintained in investigative files) because the information received from SOD will constitute confidential level "classified information."[32]

Parallel Construction and 702 Surveillance

As discussed previously, 50 USC §1806 governs the use of information acquired from electronic surveillance pursuant to an individual FISA order/Title I collection and a 702 FISA order. 1806(a) provides that information collected under an individual order or 702 "concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person *only in accordance with the minimization procedures required by this subchapter*."[33] (emphasis added).

Additionally,1806(b) requires a statement for disclosure and provides "No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such a disclosure is accompanied by a statement that such information, or any information derived

---

[29] Stewart W. Powell, *NSA Shares Crime Data with Justice Department*, Houston Chronicle, Aug. 3, 2013, *available at* http://www.houstonchronicle.com/news/politics/article/NSA-shares-crime-data-with-Justice-Department-4705274.php.

[30] John Shiffman & David Ingram, *Exclusive: IRS manual detailed DEA's use of hidden intel evidence*, Reuters, Aug. 7, 2013, *available at* http://mobile.reuters.com/article/idUSBRE9761AZ20130807?irpc=932.

[31] IRM-AA § 9.4.2.7 (2004).

[32] *Id*.

[33] 50 USC 1801 (h) defines minimization procedures and provides in paragraph 3 that minimization procedures may "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."

therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General." Information sharing under the theory of "parallel construction" may be sidestepping this section because, as *Reuters* reported, law enforcement entities are instructed *not* to use the information in investigative functions/criminal proceedings. So, the information is likely shared with the required statement that the Attorney General must approve the use of the information in a criminal proceeding, but law enforcement entities are instructed not to use the information in a criminal proceeding because it is classified.

Instead, according to *Reuters*, the DEA instructs the law enforcement entity to embrace "parallel construction" and never even mention the intelligence information in any step of a case—investigation or prosecution. This then means that it is never disclosed in a criminal prosecution that FISA derived information was in fact the basis for the investigation (or evidence derived therefrom), which enables the government to avoid disclosure and any legal and constitutional challenges in court.

***Brady* and Exculpatory Evidence**

Failure to notify prosecutors that evidence, or even probable cause for the crime itself, may have been derived from Section 702 surveillance, raises serious concerns under the Fifth and Sixth Amendments. Pursuant to *Brady v. Maryland*[34], prosecutors have an obligation to turn over to the defense evidence of an exculpatory nature—whether on the merits or punishment—and impeachment evidence under the Fifth and Sixth Amendments to the United States Constitution. Because the constitutionality of Section 702 surveillance has not yet been tested by the courts in an adversarial setting, such information is *per se* exculpatory. In traditional criminal cases, when prosecutors fail to abide by their discovery responsibilities, they may be held accountable by dismissing a case or overturning a conviction. In the context of "parallel construction," however, even prosecutors are not being told that information derived from intelligence collection authorities, like 702, was used in a criminal case. This raises the same constitutional concerns, but without a possible remedy. This cannot continue.

Attorney-Client Confidences

A criminal defense attorney has an ethical and constitutional duty to pursue affirmative means of protecting confidential attorney-client communications from government surveillance and interception, including a duty to challenge the substance of administrative orders that prevent a lawyer from having meaningful communications, and therefore prevent the lawyer from providing competent representation.[35] That includes seeking judicial review and remedies,

[34] Brady v. Maryland, 373 U.S. 83 (1963).

[35] For a full discussion of the ethical obligations of an attorney to protect client confidences from a third-party, and the Fifth, Sixth, and Fourth Amendment implications of infringing on attorney-client confidences *see* NACDL Ethics Advisory Comm. Op. 12-01 (2012) (discussing disclosure of attorney-client privileged communications to third-party (Guantanamo Bay, Cuba)), *available at* https://www.nacdl.org/Document/No12-01Disclosureofattorney-clientprivilegedcommun.

and/or, if necessary, appropriate protective orders. Likewise, defense counsel may not rely simply on the prospect of *post hoc* relief provided by the exclusionary rule.

The minimization procedures disclosed by the government—from a 2011 FISC opinion—create a conflict between defense counsels' duty to not disclose client confidences without the client's informed consent and counsels' duty to provide competent representation. Lawyers cannot ethically communicate with their clients in a manner that gives third parties access to the communications. This is an impossible situation for an American lawyer and every notion of American criminal justice.

The 702 minimization procedures, Section 4, cover Attorney-Client Communications.[36] The minimization procedures only address communications between an *indicted defendant and his attorney in that case,* completely ignoring the traditional concept of privileged attorney-client communications—from the inception of the relationship about matters relating to the representation, not just a case for which there is an indictment.[37]

FISA barely addresses the category of privileged information and is silent on attorney-client communications specifically. The statute only provides that "no otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall loose its privileged character."[38] The statute, instead, relies on the executive branch to create and enforce minimization procedures regarding the collection, dissemination, and retention of privileged information.[39] Based on the 2011 minimization procedures that have been declassified and shared with the public, the government has not satisfied this statutory mandate.

Recommendations for Reform

- The PCLOB should recommend that the use "parallel construction" end.
- The PCLOB should recommend that Congress amend the definition of minimization procedures (50 USC 1801(h)) to provide specific minimization procedures that prohibit the dissemination or retention of the contents of any attorney-client privileged communication, regardless of whether the communication is between a person who is known to be under criminal indictment in the United States and an attorney who

[36]Minimization Procedures used by the NSA in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of FISA (Oct. 31, 2011), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf

[37] *See* Model Rules of Prof'l Conduct Rule 1.6 cmt. 3 (2013). Comment 3 to ABA Model Rule of Professional Responsibility provides "The principle of client-lawyer confidentiality is given effect by related bodies of law: the attorney-client privilege, the work product doctrine and the rule of confidentiality established in professional ethics. The attorney-client privilege and work product doctrine apply in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule, for example, applies not only to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source." *See also* Model Rules of Prof'l Conduct Rule 1.18 (2013) (requires lawyers to protect the confidences of prospective clients).

[38] 50 USC § 1806(a).

[39] *See* 50 USC § 1881a(e).

represents that individual in a matter under indictment (or someone acting on behalf of the attorney). A communication identified as an attorney-client communication must not be disseminated or retained, and shall be destroyed upon recognition.

- The PCLOB should recommend continuing, non-classified, public disclosure of the minimization procedures for FISA programs, including individual orders, Section 702 surveillance, and Section 215 collection.
- The PCLOB should recommend that Congress amend Section 1806 such that any evidence obtained or derived from Section 702 surveillance—including that "obtained" via parallel construction techniques—be identified as such in any trial, hearing, or other proceeding.
- The PCLOB should recommend that Congress amend 50 USC 1801(h) (definition of minimization procedures) to reflect the specific crimes for which information may be shared with law enforcement entities, and specify that information of other crimes shall not be shared with law enforcement entities. It is currently too broad and is only limited by the minimization procedures implemented by the government at the time of collection.
    - A recommendation that the information may be shared with law enforcement entities for violent crimes is far too broad.
    - A recommendation that the information may be shared with law enforcement for national security crimes is far too broad.

POLICY ISSUES

As broad national security policies are considered, the government often assures Congress and the American people that new authorities will be used to fight terrorism, not to spy on citizens. The government is then often trusted to implement its own policies for protecting privacy and create use limitations for intelligence information collected, which, they assure us, strike the proper balance between national security and civil liberties. Later, however, the government argues that it should be able to use information that is lawfully collected however it sees fit—without intervening judicial authorization.[40] This is bad policy and cannot continue. The PCLOB should make clear that information collected for intelligence purposes under Section 702 and other non-particularized authorities that do not meet traditional Fourth Amendment standards for search and seizure cannot be used in criminal cases under any circumstance.

Such a recommendation would be consistent with a similar recommendation made by President's Review Group on Intelligence and Communications Technologies.

> We recommend that, if the government legally intercepts a communication under section 702, or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States person who

[40] Ellen Nakashima, *Obama administration had restrictions on NSA reversed in 2011*, Wash. Post, Sep. 7, 2013 (quoting Office of the Director of National Intelligence General Counsel Robert Litt: "If we're validly targeting foreigners and we happen to collect communications of Americans, we don't have to close our eyes to that," Litt said. "I'm not aware of other situations where once we have lawfully collected information, we have to go back and get a warrant to look at the information we've already collected."), *available at* http://www.washingtonpost.com/world/national-security/obama-administration-had-restrictions-on-nsa-reversed-in-2011/2013/09/07/c26ef658-0fe5-11e3-85b6-d27422650fd5_story.html.

> is located outside the United States, and if the communication either includes a United States person as a participant or reveals information about a United States person: . . . (2) any information about the United States person may not be used in evidence in any proceeding against that United States person.[41]

The Review Group's report goes on to recognize that the "features of the system established by FISA reflect Congress' understanding at the time of the central differences between electronic surveillance for foreign intelligence purposes and electronic surveillance for traditional criminal investigation purposes."[42] It is these differences that justify a policy that prohibits the use in criminal cases of information obtained for foreign intelligence purposes.

When Congress makes a collective decision to lower the standards under which information can be obtained for national security purposes, it does so with an acknowledgement that these interests are different from the interests already addressed in current law, i.e. the Wiretap Act. It is not the intention of Congress, unless explicitly expressed, to substitute such authorities for other existing authorities that satisfy other government interests, i.e. collection of information for traditional criminal investigation purposes. Such "exceptions" in the law for foreign intelligence collection must not be permitted to effect an end run around other existing statutes and the Constitution.

Additionally, the PCLOB should recommend that the entity seeking to (1) use information about US Persons collected under 702, (2) use information collected under 702 in an investigation of a US Person, or (3) search information collected under 702 using US Person selectors, secure a warrant based on probable cause, consistent with the Fourth Amendment. Currently, the threshold that must be met is that the use or search is likely to yield foreign intelligence information, a requirement that satisfies itself given the incorrect assumption that all information collected under 702 constitutes foreign intelligence.

Again, the government argues that it should not have to obtain a warrant to search through lawfully collected information, but this type of information was not the type of information Congress intended to be collected under Section 702. Such a requirement would be sound policy and help to ensure that 702 surveillance remains within the parameters specified by Congress, not those created by the executive branch to further executive branch interests.

---

[41] Richard A. Clarke, Michael J. Morell , Geoffrey R. Stone, Cass R. Sunstein & Peter Swire, Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies 28-29 (Dec. 12, 2013).

[42] *Id*. at 67.

Recommendations for Reform

- The PCLOB should recommend that information collected for intelligence purposes under Section 702 and other non-particularized authorities that do not meet traditional Fourth Amendment standards for search and seizure cannot be used in criminal cases.
- The PCLOB should recommend that the entity seeking to search and/or use information collected under 702 secure a warrant based on probable cause, consistent with the Fourth Amendment, to search for information about US persons obtained through 702 surveillance.

Thank you for your consideration of these comments. For additional information, please contact NACDL's National Security and Privacy Counsel Mason Clutter at (202) 465-7658 or mclutter@nacdl.org.