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

April 11, 2014

Re: Docket No. PCLOB-2013-0005-0085

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

The Brennan Center for Justice previously has submitted comments on the NSA's surveillance activities under both Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA), part of the FISA Amendments Act of 2008 (FAA). We also provided both written and oral testimony for the PCLOB's March 19, 2014 public hearing focused on Section 702. The following comments are offered to supplement and expound on the Section 702 reform recommendations set forth in these earlier submissions.

Background and Overarching Concerns

In pushing for the passage of the Protect America Act (PAA) and the FAA, officials portrayed the legislation as removing legal barriers, artificially created by changes in technology, to our government's ability to monitor the communications of non-U.S. persons located overseas.[1] Any acquisition of these individuals' communications with U.S. persons was described as "incidental."[2]

With one exception, however, the legislation made no significant changes in the government's ability to acquire "foreign-to-foreign" communications – i.e., the communications of non-U.S. persons abroad with other non-U.S. persons.[3] Instead, the main change wrought by the legislation was to eliminate the requirement of an individualized court order when the government seeks to acquire communications between U.S. persons and foreign "targets." As others have persuasively argued, the legislative history makes clear that facilitating the acquisition of communications involving U.S. persons was the legislation's driving purpose.[4]

This change raises significant legal and policy questions. The constitutionality of the warrantless collection of Americans' communications for foreign intelligence purposes is at best unsettled. While several U.S. courts of appeal have held that the collection of foreign intelligence information is a type of "special need" that justifies warrantless searches in some circumstances,[5] the D.C. Circuit has not recognized such an exception, and has made a thorough and compelling case against doing so.[6]

Moreover, most of the courts that have recognized a foreign intelligence exception have imposed key limits on its scope. "Special needs" cases require a balancing of the government's needs against the privacy interests of the individual. Given the heightened privacy interests at stake in a criminal proceeding, courts have either held or assumed that the foreign intelligence exception does not apply where the information is sought primarily for law enforcement purposes.[7] Similarly, to ensure that the government's interest is sufficiently compelling, courts have limited the exception to cases in which the government seeks information about a foreign power or agent thereof.[8] Section 702 dispenses with both limitations.

There are policy concerns that arise as well. Even if members of the public understood, despite officials' attempts at deflection, that the FAA's main goal was to capture Americans' international communications, they could not have appreciated the scope or nature of programmatic surveillance as actually implemented. We have learned that the government acquires *250 million* internet communications each year.[9] We also have learned that the collection of "upstream" internet traffic pulls in a large number of wholly domestic communications that cannot be filtered out,[10] and that the government and the FISC interpret the FAA to allow searches of other Section 702 data using U.S. person identifiers.[11]

The implications for privacy and civil liberties are enormous. Officials have dismissed the NSA's extensive history of non-compliance with FISC orders,[12] as well as anecdotal evidence of deliberate misuses (for example, running searches on romantic interests),[13] on the ground that there is no evidence of abuse that is both widespread and deliberate. These incidents, however, are alarming precisely because they highlight the potential for even more serious abuse. Moreover, the breadth of collection, combined with the abuse potential, is certain to have a chilling effect. We have begun to see this already. According to a recent Harris poll, 47% percent of Americans have changed their online behavior in the wake of disclosures about the NSA's activities, with a quarter of Americans reporting that they are less inclined to send email. The numbers are even higher for younger age groups.[14]

Finally, it is important to dispel the notion that Congress never recognized or contemplated any privacy interest on Americans' part in their international communications. In 1978, most international communications took place by satellite, and FISA did not regulate surveillance of these communications unless a U.S. person was the target. The legislative history, however, suggests that this omission was due to the complexities raised by superimposing FISA's structure onto a then-existing NSA program, and that Congress intended to fill the gap with later legislation – an effort that the Department of Justice pledged to assist.[15] This intent was never realized, but the committee report accompanying FISA acknowledged the concerns raised by the NSA's activities that the bill left unregulated, and warned that the regulatory gap "should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans."[16]

Reforms

As discussed below, our primary recommendation is to end programmatic surveillance under Section 702 of the FAA. We believe the constitutionality of FISA surveillance cannot be salvaged in any other way. Moreover, even if the PCLOB determines that there is a "foreign intelligence exception" that would allow warrantless surveillance of Americans' international communications, there are reforms that would be necessary in order to bring Section 702 surveillance within the parameters of the exception as delineated by the courts. Although we do not accept the validity of programmatic surveillance, we discuss some of those secondary reforms here,[17] both in the interest of thoroughness and because some of them would be necessary even under a regime of individualized court orders.

End programmatic surveillance

The Brennan Center strongly urges that the Board recommend an end to programmatic surveillance of Americans' international communications. A purpose to acquire foreign intelligence information, on its own, cannot justify dispensing with the Fourth Amendment's warrant requirement. Before 2007, an individualized court order was required to collect such communications in most instances, and that should be the case going forward.

An extensive discussion of whether a "foreign intelligence exception" should be recognized is beyond the scope of this submission. Instead, we offer our support for the reasoning expressed by the D.C. Circuit in *Zweibon v. Mitchell*. As the court there noted, the fact that the government has a legitimate need to acquire foreign intelligence does not necessarily mean that the "locus of initial decision-making power as to the propriety of a particular surveillance should itself rest with the Executive Branch."[18] Instead, courts must balance the interest served by a warrant requirement against the degree to which such a requirement would in fact subvert the government's interest.

A warrant requirement, the *Zweibon* court observed, would serve the weighty constitutional goal of "protect[ing] free and robust exercise of the First Amendment rights of speech and association by those who might otherwise by chilled by the fear of unsupervised and unlimited Executive power to institute electronic surveillance."[19] In assessing the government's arguments against a warrant requirement, the court cautioned that "such arguments must not be grounded in expediency or utility, but must relate to factors that would cause the warrant procedure to needlessly frustrate legitimate gathering of foreign intelligence information."[20] The court found that none of the several factors cited by the government met that standard. For instance, the government claimed that the delay involved in the warrant procedure could harm national security; the court responded that this was "nothing more than an argument that warrantless electronic surveillance, like many other warrantless searches, may be justifiable in exigent circumstances."[21]

In the absence of a viable exception to the Fourth Amendment's warrant requirement, a warrant should be required in each instance that the government knowingly acquires communications involving a U.S. person. To the extent pre-2007

FISA allowed the acquisition of some international communications without an individualized court order – for instance, those communications transmitted by satellite (which are now a small minority) and those acquired by wiretapping conducted overseas – the statute should be amended to require a court order for these communications, too. The constitutionality of collecting an American's communications without a warrant for foreign intelligence purposes does not turn on the technology by which those communications are transmitted or the location of the acquisition.

Wherever possible, the warrant should be obtained before acquisition. There may be cases in which it is technologically impossible to separate, before collection, a foreign target's communications with non-U.S. persons from his or her communications with U.S. persons. In such cases, the government should be required to identify and destroy the communications involving U.S. persons at the soonest point technologically feasible – or, alternatively, to seek a court order based on probable cause in order to retain and access them. While there may be no existing models for this precise approach in the Fourth Amendment context, that is because there are no existing models for this type of programmatic collection.[22] This solution nonetheless comes closest to approximating the constitutional protections courts have accorded to Americans' communications, short of requiring a warrant for *all* collection on overseas targets whose communications may on occasion involve U.S. persons.

Needless to say, a warrant requirement for international communications involving U.S. persons will substantially increase the workload of both the FISC and the relevant government agencies. The solution is to allocate the resources necessary for the government to meet its constitutional obligation. As Justice Byron White stated in *United States v. Karo*, "The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement."[23]

Narrow the category of communications subject to collection

Regardless of whether programmatic surveillance is ended, the universe of international communications that is subject to acquisition for foreign intelligence purposes is currently far too broad. There are two changes that would help set appropriate boundaries for foreign intelligence collection: restoring the requirement that the target of surveillance be a foreign power or agent thereof (FP/AFP), and narrowing the definition of "foreign intelligence."

FP/AFP requirement

Even assuming the validity of a foreign intelligence exception to the warrant requirement, courts have emphasized that this exception should be a narrow one, reserved for cases in which the executive branch's interests in collection are most compelling. For that reason, the Fourth Circuit, in the influential case of *United States v. Truong Dinh Hung*, held that the subject of foreign intelligence surveillance must be a foreign power or agent thereof:

> [The] foreign intelligence exception to the Fourth Amendment warrant requirement must be carefully limited to those situations in which the interests of the executive are paramount. First, the government should be relieved of seeking a warrant only when the object of the search or the surveillance is a foreign power, its agent or collaborators. In such cases, the government has the greatest need for speed, stealth, and secrecy, and the surveillance in such cases is most likely to call into play difficult and subtle judgments about foreign and military affairs. When there is no foreign connection, the executive's needs become less compelling; and the surveillance more closely resembles the surveillance of suspected criminals, which must be authorized by warrant.[24]

If "foreign power" were narrowly defined to encompass only foreign governments, *Truong*'s holding might create problems in an era in which the United States' primary enemies are stateless actors. But FISA's definitions of "foreign power" and "agent of a foreign power," are, if anything, broader than necessary to accommodate the government's legitimate foreign intelligence interests. "Foreign power[s]" include groups engaged in international terrorism "or activities in preparation therefor," as well as foreign-based political organizations not substantially composed of U.S. persons.[25] "Agent[s] of a foreign power" similarly include any non-U.S. person who engages in international terrorism or preparatory activities, as well as any non-U.S. person who acts in the U.S. as an officer or employee of a foreign power (including, for instance, embassy workers).[26]

No convincing argument has been made for dropping FISA's requirement that the "target" of surveillance must be a foreign power or its agent in cases when the government seeks to obtain international communications involving a U.S. person. Regardless of whether an individualized court order is required, the FP/AFP requirement should be restored.

Definition of "foreign intelligence"

The courts that have recognized a "foreign intelligence exception" have not grappled with the definition of "foreign intelligence." As noted above, however, they have emphasized that the exception should be narrow and justified by compelling foreign policy considerations.

In light of this emphasis, FISA's definition of "foreign intelligence information" is strikingly amorphous. While the first part of the definition describes information that pertains to specific threats to security or foreign relations, such as "grave hostile acts of a foreign power or agent of a foreign power" or "clandestine intelligence activities,"[27] the second part of the definition encompasses any information with respect to a foreign power or foreign territory "that relates to . . . (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States."[28] In the absence of any constraints on how "security" is defined or on the types of "foreign affairs" at issue, this part of the definition is almost limitlessly broad.

One option for sharpening the definition would be to discard the second part of the statutory definition and retain the first part. Under that approach, the government could collect information to help protect against actual or potential attacks, "grave hostile acts," sabotage, international terrorism, the international proliferation of weapons of mass destruction, or clandestine intelligence activities.[29] This definition is broad enough to allow the U.S. to collect information about, for instance, the Kremlin's plans to invade Ukraine. According to one treatise, "FISA's legislative history . . . makes clear that Congress intended to reach information about terrorism occurring in other countries, threats against other countries, and espionage by one foreign power against another."[30]

Another option is to rely on the restrictions that President Obama recently placed on the permissible uses of signals intelligence information collected in bulk. Presidential Policy Directive 28, issued on January 17 of this year, states that such information shall be used

> only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.[31]

Signals intelligence that takes place under Executive Order 12,333 is subject to fewer constitutional and statutory constraints than any other type of communications surveillance. It accordingly provides the executive branch with the greatest leeway to ferret out foreign intelligence information. The fact that the President feels comfortable imposing the above restrictions in the 12,333 context strongly suggests that imposing those same limits in the context of section 702 collection would not unduly restrict the government's intelligence gathering. More fundamentally, defining "foreign intelligence information" as information relating to the above-listed threats would bring the definition in line with the case law limiting the "foreign intelligence exception" to instances in which the government's interests are paramount.

Furthermore, the statute should be amended to allow the FISC to review the substance of the government's certification of a foreign intelligence purpose. FISA has always required the court to simply accept the accuracy of this certification in cases where the target is a non-U.S. person (if the target is a U.S. person, the court may determine whether the certification is "clearly erroneous"). This judicial passivity runs counter to the case law, which gives the court a critical role in probing the government's assertion of a foreign intelligence purpose. As the Third Circuit stated in *United States v. Butenko*:

> Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and

> that the accumulation of evidence of criminal activity was incidental. If the court, for example, finds that members of a domestic political organization were the subjects of wiretaps or that the agents were looking for evidence of criminal conduct unrelated to the foreign affairs needs of a President, then he would undoubtedly hold the surveillances to be illegal and take appropriate measures.[32]

A concurring judge on the Fifth Circuit echoed the point: "The judiciary must not be astigmatic in the presence of warrantless surveillance; rather, judges must microscopically examine wiretaps in order to determine whether they had their origin in foreign intelligence or were merely camouflaged domestic intrusions."[33] The same logic suggests that the court, in addition to determining whether the government has accurately represented its purpose, should assess whether the government has made a sufficient showing that this purpose will be served by the proposed collection. The "foreign intelligence exception" cannot fairly be said to apply where the government proposes surveillance that is not reasonably likely to produce foreign intelligence.

Restore the "primary purpose" test

To the extent the FISA scheme continues to rest on the existence of a "foreign intelligence exception" to the warrant requirement (either because programmatic surveillance continues or because the individualized court orders do not qualify as "warrants"[34]), it is critical that Congress amend FISA to specify that acquiring foreign intelligence must be the "primary purpose" of surveillance, rather than merely a "significant" purpose.

Under well-established Fourth Amendment jurisprudence, a search of an American's person, property, papers, or communications generally requires a warrant based on probable cause. Courts have recognized, however, that traditional warrants may not be required in cases where the search is intended to meet "special needs" of the government beyond the normal need for law enforcement.[35] In order to avoid an end run around the warrant requirement, however, the special need must predominate in any mixed-motive cases.[36] In accordance with this case law, courts have recognized a "foreign intelligence" exception to the warrant requirement only where obtaining foreign intelligence is the "primary purpose" of surveillance.[37]

In 2002, the FISC took the same approach, but in the government's first appeal to the Foreign Intelligence Surveillance Court of Review (FISCR), the FISCR reversed. The court reasoned that the purpose of foreign intelligence investigations "is to halt the espionage or terrorism efforts, and criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts."[38] Even where foreign intelligence is gathered for use in a criminal prosecution, the ultimate aim is still "to counter the malign efforts of a foreign power. Punishment of the terrorist or espionage agent is really a secondary objective."[39] Accordingly, the FISCR held, acquiring foreign intelligence information for the purpose of bringing a criminal prosecution is consistent with Supreme Court case law holding that only "special needs" beyond law enforcement can justify warrantless searches.

The FISCR's reasoning was flawed in at least two critical respects. As the Supreme Court has warned, "law enforcement involvement always serves some broader social purpose or objective" beyond punishment or deterrence.[40] Prosecutions of gang violence are intended to protect community safety and vitality; prosecutions of drug offenses are intended to promote public health; prosecutions of insider trading are intended to ensure the stability and integrity of the financial system. The Supreme Court has clearly held that such broader motives cease to justify warrantless searches at the moment the "immediate objective" shifts to criminal investigation or prosecution. Thus, for instance, a state hospital's program to test obstetrics patients for drug use was struck down because it involved the threat of criminal referrals, even though the ultimate goal was concededly to improve fetal health.[41]

The FISCR also failed to grapple with the basic reason for drawing this line – namely, the heightened privacy interests at stake when a criminal investigation is initiated. To determine whether a warrantless search is reasonable under the "special needs" doctrine, the court must weigh the government's need against the individual's privacy interest. The FISCR asserted that the existence of criminal prosecution does not lessen the government's foreign policy concerns. Regardless of whether that assessment is accurate, it is clear – as the Fourth Circuit noted in *Truong* – that the individual's privacy interest takes on heightened importance when his or her liberty is at stake. The FISCR did not address this side of the balance, or the *Truong* court's sensible conclusion that "individual privacy interests come to the fore" in a criminal case.[42]

On a more prosaic level, it is simply too easy for the government to dodge the warrant requirement that applies in the normal law enforcement context if foreign intelligence need only be a "significant" purpose of collection under FISA. In any criminal prosecution of espionage or international terrorism, the government can make a plausible argument that gathering evidence against the defendant will also provide useful "foreign intelligence information." In practice, then, the "significant purpose" requirement converts the "foreign intelligence exception" into an exception for any law enforcement activity with international dimensions. Such an approach drives a hole through the protections of the Fourth Amendment.

End back door searches for U.S. person information

In arguing for the passage of the PAA and the FAA, supporters of the bill within the administration and Congress tried to reassure more skeptical lawmakers that the vast increase in the government's access to U.S. person information would be countered by strict limitations on the retention, use, and dissemination of such information, as set forth in the statute's "minimization" requirements. Despite the fact that obtaining communications to and from U.S. persons was the primary goal of the legislation, officials strove to persuade their audiences that the government had no interest in the U.S. person side of these communications. They emphasized that the legislation would prohibit collection if the government had any such interest, through a so-called "reverse targeting prohibition."

The following exchange between then-Director of National Intelligence Michael McConnell and Senator Tom Coburn at a 2007 hearing typifies the official assurances that Section 702 would not be deployed against U.S. persons:

> **Mike McConnell**: And the third point – and this is very important. It is very important to me; it is very important to members of this Committee. We should be required – we should be required in all cases to have a warrant anytime there is surveillance of a U.S. person located in the United States. I think that was the intent of the 1978 law. That is what was included in the Protect America Act passed in August.
>
> ….
>
> **Senator COBURN**: So let me summarize, and you say if you agree with this. If you are an American citizen, you are not going to be *targeted [by] any of this* without approval of a court?
>
> **Mike McConnell**: That is correct.
>
> **Senator COBURN**: Alright. That needs to be said, loud and loud and loud. If you are an American citizen, you have the protection of a court *before you are subject to this law.*
>
> **Mike McConnell**: If you are an American citizen or even a non-citizen in the country, you have the protection of a warrant issued by a court before we could conduct any kind of a surveillance.
>
> Now, sir, so you are aware, some will argue that we are targeting overseas and the person overseas calls into the United States. That is where minimization starts. We cannot control what the overseas target does. We have to have a process to deal with that, and that is where minimization was introduced. It is an elegant solution. We have tried every way we can think of to make that different or stronger or more complete, and those who framed this law in 1978 and all of us that have looked at it since, we can't find a better process.
>
> ….
>
> **Mike McConnell**: As I tried to explain before, you can only target one thing, and so if the U.S. person in this country, for whatever reason—terrorists or whatever the issue is—becomes a target, then you would be required to have a warrant. Now, if you engaged in that process of reverse targeting where you are targeting someone overseas and your real target is in the United States, that would be a violation of the Fourth Amendment. That is unlawful.[43]

Official testimony was replete with such statements about protecting Americans' civil liberties by requiring minimization of U.S. person information and a court order

when the government's interest focused on a U.S. person. Importantly, no official who discussed the bill in public congressional testimony or in public statements ever cited a technical distinction between the government's interest *at the time of collection* and the government's interest *at the time of reviewing the collected information*, suggesting that the same strict protections for U.S. persons would apply at all points.

In accordance with this testimony and understanding, the minimization procedures proposed by the government and adopted by the court prohibited the government from using U.S. person identifiers to search communications collected through programmatic surveillance.[44] In 2011, however, the prohibition was lifted.[45] Today, the government can and does[46] conduct searches for U.S. person information acquired under Section 702. Indeed, this practice is sufficiently common that the ODNI general counsel has testified that it would impose an unworkable burden to require the government to obtain court orders before conducting these searches.[47]

Government officials have justified this practice on the ground that there are no constitutional restrictions on the government's ability to make use of "lawfully collected" information. At the PCLOB's March 19 public hearing, a Justice Department official testified that "[o]nce you've lawfully collected that information, subsequently querying that information isn't a search under the Fourth Amendment, it's information already in the government's custody."[48] The same official rejected the notion that there might be policy reasons for requiring court orders to run U.S. person queries, stating: "[O]nce we've collected it, we've gotten the necessary court approvals to obtain the information, we don't then have to go back to court to query the same information that we've already collected lawfully a second time to say is it okay to look at it. We've already gotten the conclusion that it's legal to collect it."[49] The NSA's general counsel similarly testified:

> [O]nce information is collected pursuant to 702, the government can and often will review what it needs to in that information. Querying that lawfully collected information, one way to think about that is a way to more efficiently review that which the government already has in its possession and can review all of.
>
> And so to get to your question about policy limits on querying that data, one also needs to understand that that information is at the government's disposal to review in the first instance, and querying it is just a way to organize it.[50]

There may well be contexts in which the Constitution imposes no limits on the government's use of information that is otherwise lawfully collected. Section 702 is decidedly not such a context. In a 2011 FISC opinion that held aspects of the government's "upstream collection" under Section 702 to be unconstitutional, Judge Bates unambiguously stated: "The Court of Review and this Court have recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[51] In other words, the Constitution does indeed place limits on the use of the information that is otherwise appropriately collected under section 702. (Another way to view the matter is that the warrantless collection of foreign intelligence

information is *not* lawful – since the entire program fails the Fourth Amendment's reasonableness test – if the subsequent use of incidentally collected U.S. person information is not properly regulated).

In the 2011 decision, Judge Bates invalidated the NSA's proposed measures for handling certain information that it collected under Section 702 precisely because these measures failed to appropriately minimize the retention of non-target information, "including information of or concerning U.S. persons."[52] He held open the possibility that "more stringent post-acquisition safeguards" might satisfy the Fourth Amendment's reasonableness requirement.[53] This ruling confirms that limitations on the use of U.S. person information are central to the constitutionality of the program.

The idea that the government should not be limited in its use of information collected under Section 702 also flies in the face of the statutory "minimization" requirements that form the cornerstone of the statute. A directive to "minimize" the retention or sharing of certain information is the very opposite of a license to use it for any otherwise lawful purpose. In light of the clear barrier that minimization was intended to impose, it is unsettling to hear the ODNI's general counsel defend back-door searches on the ground that "we need to eliminate barriers to making use of the information that's lawfully in our possession."[54] Nor can such statements be reconciled with the assurances provided by the DNI at the time of the PAA/FAA's passage that there would be strict limits on the use of U.S. person information.

Unfortunately, the statute's definition of "minimization procedures" does not create any bright line tests, and the FISC has held – erroneously, in our view – that back-door searches are consistent with the statute's minimization requirements.[55] An argument indeed can be made that the government should be permitted to retain and use certain U.S. person information that it comes across in the course of reviewing communications retrieved through non-U.S. person queries – for instance, if that information qualifies as, or is necessary to understand, significant foreign intelligence information. After all, the statute requires the government to minimize the retention and prohibit the dissemination of U.S. person information "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[56] It is difficult to comprehend, however, how a practice of querying unminimized data for the specific purpose of locating and reviewing U.S. person information could comport with a minimization requirement. The existence of a foreign intelligence purpose cannot legitimize this practice under the statute; there is no purpose-based language in the minimization provision.

Back-door searches also make a mockery of the reverse targeting prohibition. Recognizing that an individualized court order is required when the government wishes to target a U.S. person under FISA, the statute prohibits targeting a non-U.S. person if the government's actual purpose is to target a particular, known U.S. person on the other end of the communication.[57] The government argues that this prohibition applies at the time of collection, but ceases to have any application at the time of actual review, even if those actions are separated by mere minutes.[58] This interpretation is nonsensical. The government is quick to acknowledge in other contexts (such as the bulk collection of telephone records under Section 215 of the Patriot Act)[59] that it is the *review* of personal

information, far more than the fact of collection, that implicates civil liberties concerns.[60] It would be perverse for Congress to adopt protections for as-yet-unreviewed U.S. person information and then abandon those protections at the point of review.[61]

Regardless of whether back-door searches are deemed consistent with the letter of the reverse targeting prohibition, they are clearly inconsistent with its spirit and intent. The FISC has no role in assessing the government's actual purpose either at the point of collection or review, but even if it did, there would often be no viable way to establish whether the government's interest in the U.S. person developed before or after collection. Back-door searches provide an easy end-run around the reverse targeting ban, rendering it effectively unenforceable.

They also gut FISA's requirement of an individualized court order for surveillance targeting U.S. persons. There is a massive amount of information collected under Section 702 – 250 million internet communications a year, and an unknown number of other types of communications – the vast majority of which is currently subject to back-door searches. As this information continues to accumulate, the government, in cases where it lacks probable cause to obtain a court order, will increasingly be able to obtain the same information or its equivalent by searching the pool of communications acquired under Section 702. Indeed, this option provides a tempting incentive to collect as much international traffic as possible through programmatic surveillance, in order to provide a fertile database for warrantless searches. Back-door searches thus undermine the basic premise at the heart of FISA: if the government wishes to access U.S. person information contained in communications to or from Americans, it must have an individualized court order.

Conclusion

We urge the PCLOB to be forward-thinking in its analysis of Section 702. We appreciate the sensitivities involved in expressing constitutional doubts about a program that Congress sanctioned and that has been in operation for several years. Similarly, we understand that there may be a natural reluctance to question the adequacy, from a privacy and civil liberties standpoint, of legislation that was enacted after open debate – even where, as here, officials repeatedly mischaracterized the nature of the legislation, and even where the details of the statute's actual implementation could not have been foreseen at the time. Nonetheless, such actions may on occasion be necessary for the PCLOB to fulfill its statutory mandate. We believe they are necessary here.

Respectfully submitted,

Elizabeth Goitein
Co-Director, Liberty and National Security Program
Brennan Center for Justice

---

[1] *See, e.g.*, *FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 18-19 (2012), *available at*

https://www.fas.org/irp/congress/2012_hr/faa.pdf (statement of Kenneth Wainstein, Partner, Cadwalader, Wickersham & Taft LLP); *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 8 (2007), *available at* http://www.fas.org/irp/congress/2007_hr/strengthen.pdf (statement of J. Michael McConnell, Director, Office of National Intelligence); *Legislative Proposals to Update the Foreign Intelligence Surveillance Act: Hearing Before the Subcomm. On Crime, Terrorism and Homeland Security of the H. Comm. on the Judiciary*, 109th Cong. 22 (2006), *available at* http://commdocs.house.gov/committees/judiciary/hju29746.000/hju29746_0f.htm (statement of Robert Dietz, General Counsel, NSA).

[2] *See, e.g.*, *FISA Hearing: Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. 71 (2007), *available at* http://www.fas.org/irp/congress/2007_hr/fisa092007.pdf (statement of J. Michael McConnell, Director, Office of National Intelligence).

[3] The exception is stored e-mails that reside on U.S. servers. *See* 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2d § 16.3, at 531-32 (2d ed. 2012).

[4] *See* JAMEEL JAFFER, ACLU, SUBMISSION TO PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD PUBLIC HEARING ON SECTION 702 OF THE FISA AMENDMENTS ACT 13, 13 n.69 (2014), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf; Jennifer Granick, *The FISA Amendments Act Authorizes Warrantless Spying on Americans*, STANFORD CENTER FOR INTERNET AND SOCIETY (Nov. 5, 2012, 2:49 PM), http://cyberlaw.stanford.edu/blog/2012/11/fisa-amendments-act-authorizes-warrantless-spying-americans; Elizabeth Goitein, *The NSA's Backdoor Search Loophole*, BOSTON REVIEW BLOG (Nov. 14, 2013), http://www.bostonreview.net/blog/elizabeth-goitein-nsa-backdoor-search-loophole-freedom-act.

[5] *See* U.S. v. Brown, 484 F.2d 418 (5th Cir. 1973); U.S. v. Butenko, 494 F.2d 593 (3d Cir. 1974) (en banc); U.S. v. Buck, 548 F.2d 871 (9th Cir. 1977); U.S. v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

[6] *See* Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975).

[7] *See Truong*, 629 F.2d at 915; U.S. v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984); U.S. v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); U.S. v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); U.S. v. Johnson, 952 F.2d 565, 575 (1st Cir. 1991).

[8] *See Truong*, 629 F.2d at 915.

[9] *See* [REDACTED NAME], [REDACTED NO.], slip op. at 29 (FISA Ct. Oct. 3, 2011), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf.

[10] *Id.* at 33.

[11] *Id.* at 22-23.

[12] *See In re* Production of Tangible Things From [REDACTED], No. BR 08-13, slip op. at 4-11 (FISA Ct. Mar. 2, 2009), *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf; [REDACTED NAME], [REDACTED NO.], slip op. at 15-16, 16 n.14 (FISA Ct. Oct. 3, 2011), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf; *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 09-06, slip op. at 4-7 (FISA Ct. n.d.), *available at* https://www.aclu.org/files/natsec/nsa/FISC%20Order%20-and%20Supplemental%20Order.pdf; *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 13-109, slip op. at 5 n.8 (FISA Ct. Oct. 11, 2013), *available at* https://www.aclu.org/files/natsec/nsa/br13-09-primary-order.pdf.

[13] *See, e.g.*, Adam Gabbatt and agencies, *NSA Analysts 'Wilfully Violated' Surveillance Systems, Agency Admits*, GUARDIAN, Aug. 24, 2013, *available at* http://www.theguardian.com/world/2013/aug/24/nsa-analysts-abused-surveillance-systems; Chris Strohm, *Lawmakers Probe Willful Abuses of Power by NSA Analysts*, BLOOMBERG, Aug. 24, 2013, *available at* http://www.bloomberg.com/news/2013-08-23/nsa-analysts-intentionally-abused-spying-powers-multiple-times.html; *see also* Press Release, Sen. Chuck Grassley, Grassley Presses for Details about Intentional Abuse of NSA Authorities (Aug. 28, 2013), *available at* http://www.grassley.senate.gov/news/Article.cfm?customel_dataPageID_1502=46858.

[14] Stephen Cobb, *New Harris polls shows NSA revelations impact online shopping, banking, and more*, WELIVESECURITY.COM (Apr. 2, 2014, 9:24 AM), http://www.welivesecurity.com/2014/04/02/harris-poll-nsa-revelations-impact-online-shopping-banking/.

[15] *Foreign Intelligence Surveillance Act of 1976*: *Hearing Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary*, 94th Cong. 15 (1976); *Foreign Intelligence Surveillance Act: Hearing Before the Subcomm. on*

Courts, Civil Liberties, and the Administration of Justice of the S. Comm. on the Judiciary, 94th Cong. 98-99 (1976); *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearing Before the Subcomm. on Intelligence and the Rights of Americans of the S. Select Comm. on Intelligence*, 94th Cong. 80 (1976); S. REP. NO. 95-701, at 34 (1977); S. REP. NO. 95-604, pt. 1, at 34 (1977); *Foreign Intelligence Surveillance Act: Hearing Before the Subcomm. on Intelligence and the Rights of Americans of the S. Select Comm. on Intelligence*, 95th Cong. 16 (1977); *Foreign Intelligence Electronic Surveillance: Hearing Before the Subcomm. on Legislation of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 12 (1978).

[16] S. REP. NO. 95-701, at 35.

[17] We have discussed other reforms that we support – such as interpreting the term "target" to include the parties to a communication but not the subject matter – in our other submissions.

[18] Zweibon v. Mitchell, 516 F.2d 594, 633 (D.C. Cir. 1975).

[19] *Id.* at 633.

[20] *Id.* at 636.

[21] *Id.* at 649-50.

[22] The government has compared the collection of Americans' international communications with the "incidental" surveillance that occurs when the government has a warrant to obtain a person's communications and ends up overhearing the other side of the conversation. As the ACLU has pointed out, there are key differences in these scenarios – such as the absence of any warrant in the Section 702 context – that render the analogy wholly inapt. *See* JAFFER, *supra* note 4, at 13-15.

[23] U.S. v. Karo, 468 U.S. 705, 718 (1984); *see also Zweibon*, 516 F.2d at 70 (noting that the administrative burden of obtaining warrants for foreign intelligence surveillance was "an argument grounded in expediency" that could not serve as a basis for resolving the constitutional inquiry).

[24] U.S. v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980) (internal citation omitted).

[25] 50 U.S.C. § 1801(a)(4) &(5).

[26] 50 U.S.C. § 1801(b)(1)(A)&(C).

[27] 50 U.S.C. § 1801(e)(1)(A)&(C).

[28] 50 U.S.C. § 1801(e)(2).

[29] *Id.*

[30] KRIS & WILSON, *supra* note 3, § 8.31, at 301-02.

[31] EXEC. OFFICE OF THE PRESIDENT, PRESIDENTIAL POLICY DIRECTIVE/PPD-28, at 4 (2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/2014sigint.mem_.ppd_.rel_.pdf.

[32] U.S. v. Butenko, 494 F.2d 593, 606 (3d Cir. 1974) (en banc).

[33] U.S. v. Brown, 484 F.2d 418, 427 (5th Cir. 1973) (Goldberg, J., concurring).

[34] Whether individualized surveillance orders under FISA satisfy the substantive criteria for a warrant – namely, whether they are sufficiently particular and based on probable cause – is unclear at best. *See* KRIS & WILSON, *supra* note 3, § 11.2, at 391, § 11.4-11.6, at 394-408.

[35] *See* Griffin v. Wisconsin, 483 U.S. 868, 873 (1987).

[36] *See, e.g.*, Ferguson v. City of Charleston, 532 U.S. 67 (2001).

[37] *See* cases cited *supra* note 7.

[38] *In re* Sealed Case, 310 F.3d 717, 743 (FISA Ct. Rev. 2002).

[39] *Id.* at 744-45.

[40] *Ferguson*, 532 U.S. at 84.

[41] *Id.* at 83-84.

[42] *Truong*, 629 F.2d at 915.

[43] *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 11, 24, 32 (2007) (emphasis added), *available at* http://www.fas.org/irp/congress/2007_hr/strengthen.pdf (statement of J. Michael McConnell, Director, Office of National Intelligence).

[44] 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 § 3(b)(5), at 3 (2009), *available at* https://www.aclu.org/files/natsec/nsa/FAA%20Minimization%20Procedures.pdf.

[45] 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

§ 3(b)(6), at 6 (2011), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

[46] Letter from James Clapper, Dir., National Intelligence, to Senator Ron Wyden (Mar. 28, 2014), *available at* https://www.documentcloud.org/documents/1100298-unclassified-702-response.html.

[47] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, PUBLIC HEARING REGARDING SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 30 (2014) [hereinafter PCLOB HEARING], *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf (statement of Brad Wiegmann, Deputy Assistant Att'y Gen., U.S. Dep't of Justice).

[48] *Id.* at 28.

[49] *Id.* at 29.

[50] *Id.* at 31 (statement of Raj De, General Counsel, NSA).

[51] [REDACTED NAME], [REDACTED NO.], slip op. at 77 (FISA Ct. Oct. 3, 2011), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf.

[52] *Id.*

[53] *Id.* at 79.

[54] PCLOB HEARING, *supra* note 47, at 34 (statement of Robert Litt, General Counsel, Office of the Director of National Intelligence).

[55] [REDACTED NAME], [REDACTED NO.], slip op. at 22-24 (FISA Ct. Oct. 3, 2011), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf.

[56] 50 U.S.C. § 1801(h)(1).

[57] 50 U.S.C. § 1881a(b)(2).

[58] *See* PCLOB HEARING, *supra* note 47, at 27-30; *id.* at 30-32 (statement of Raj De, General Counsel, NSA).

[59] Intelligence officials attempted to reassure Congress that the bulk collection program does not constitute a violation of Americans' privacy because, among other things, "[o]nly a very small fraction of the metadata acquired under the program is ever reviewed." Ellen Nakashima, *Call records of fewer than 300 people were searched in 2012, U.S. says*, WASH. POST, June 15, 2013, *available at* http://www.washingtonpost.com/world/national-security/call-records-of-fewer-than-300-people-were-searched-in-2012-us-says/2013/06/15/5e611cee-d61b-11e2-a73e-826d299ff459_story.html.

[60] This is not to say that collection itself does not present privacy concerns or trigger the Fourth Amendment. Some of the most powerful civil liberties concerns, however – such as the potential to use the information for political or other illegitimate concerns – are contingent on the government's knowing the content of the information. While it makes little sense to say that no privacy invasion occurs at the point of collection, it makes even less sense to say that no additional privacy invasion accrues at the point of review.

[61] Director of National Intelligence James Clapper has suggested that Congress implicitly approved back-door searches, based in part on the Senate intelligence committee's rejection of an amendment that Senator Ron Wyden offered when the FAA was reauthorized in 2012 to explicitly ban the practice. The committee's action cannot be construed as endorsement of back door searches, however. Sen. Wyden offered his amendment to "clarif[y]" that the legislation does not permit back-door searches – a point he clearly believed to be implicit, if inadequately spelled out, in other parts of the FAA. *See* S. REP. NO. 112-174, at 11 (2012) (minority views of Sen. Ron Wyden and Sen. Mark Udall). After the amendment was rejected, Sen. Dianne Feinstein indicated her belief that the FAA did not prohibit back-door searches in all instances. *See* S. REP. NO. 112-174, at 9 (2012). Whether other committee members who voted against the amendment felt that no clarification was necessary because the statute already prohibited them, or whether they felt that back-door searches were and should be lawful, is an exercise in guesswork as the committee conducts its mark-ups behind closed doors.