PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Separate Statement by
Board Members Rachel Brand and Elisebeth Collins Cook

JULY 2, 2014

Separate Statement by Board Members Rachel Brand and Elisebeth Collins Cook

I. The Program is Legal and Effective

We hope that the length of the Board's report and its comprehensive discussion of the legal considerations surrounding the program will not obscure the Board's unanimous bottom-line conclusion: The core Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool.

To the extent that the Board had concerns about the program after our thorough review, they focused primarily on two particular aspects to the program's current operation: the practice of searching the database using a U.S. person identifier, and so-called "about" collection, both of which are discussed at length in the Board's report. The Board makes a few targeted recommendations to address concerns raised by these two aspects of the program. We stress that these are *policy*-based recommendations designed to tighten the program's operation and ameliorate the extent to which these aspects of the program could affect the privacy and civil liberties of U.S. persons. We do not view them to be essential to the program's statutory or constitutional validity.

II. Queries of Section 702 Information

The extent to which additional restrictions should apply to agencies' ability to query information collected pursuant to Section 702 using U.S. person identifiers has divided the Board. In the case of the FBI, this issue is intertwined with questions about querying Section 702 information for non–foreign intelligence purposes, the potential use of Section 702 information in criminal proceedings, and longstanding efforts to ensure information sharing within the agency. Specifically, the Board grappled with what to do about the fact that it is theoretically possible for a database query by an FBI analyst in a non–foreign intelligence criminal matter to return Section 702 information and for this information to be further used in the investigation and prosecution of that crime.[1] In addressing this issue, we believe it important to adopt a policy that matches the scope of the problem, can work as a practical matter, and will not unnecessarily impair the government's ability to conduct counterterrorism and other national security–related investigations.

[1] The FBI receives only a small portion of Section 702 information and receives no information collected upstream. *See* Letter from Deirdre M. Walsh, Director of Legislative Affairs, to Hon. Ron. Wyden, United States Senate (June 27, 2014) (responding to question regarding number of queries using U.S. person identifiers of communications collected under Section 702).

The concern: As discussed at length in the Board's Report, Section 702 collection differs from traditional electronic surveillance in a few key ways, including a lower standard for collection and the absence of a particularized judicial finding for targeting decisions. Moreover, Section 702 has an explicit foreign intelligence purpose requirement for authorized collection, consistent with the longstanding distinction between foreign intelligence and criminal purposes reflected elsewhere in FISA. Given these factors, our key concerns were the querying of Section 702 collection for *non–foreign intelligence* purposes, and the potential subsequent use of that information to further a non–foreign intelligence criminal investigation or prosecution.[2]

Scope: According to initial information provided by the FBI, it seems clear that FBI agents and analysts routinely conduct queries across all FBI databases in non–foreign intelligence investigations and assessments. This is unsurprising, given that the FBI has traditionally considered the querying of information already within its possession to be among the least intrusive investigative techniques available, and the agency's overall efforts since 9/11 to foster information sharing and eliminate stovepipes. But the story is far different for the potential *use* of Section 702 information in the investigation or prosecution of non–foreign intelligence crimes. We are unaware of any instance in which a database query in an investigation of a non–foreign intelligence crime resulted in a "hit" on 702 information, much less a situation in which such information was used to further such an investigation or prosecution.

Our proposal: As stated in the Board's Report, we would not place limitations on the FBI's ability to include its FISA database among the databases *queried* in non–foreign intelligence criminal matters. We believe that querying information already in the FBI's possession is a relatively non-intrusive investigative tool, and the discovery of potential links between ongoing criminal and foreign intelligence investigations is potentially critical to national security.[3] Instead, we would require an analyst who has not had FISA training to seek supervisory approval before *viewing* responsive Section 702 information, to ensure that the information continues to be treated consistent with applicable statutory and court-imposed restrictions.

We believe that placing some additional limitations on the *use* of Section 702 information in non–foreign intelligence criminal matters may also be warranted because of the increased civil liberties concerns raised by the use of FISA information outside the foreign intelligence context. Conceptually, the appropriate point at which to potentially limit the use of that information is where it could infringe on a person's liberty by, for

---

2 *See In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. November 18, 2002).

3 See pages 108-10 of this Report. *See generally*, The Webster Commission, *Final Report of the William H. Webster Commission on the Federal Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas, on November 5, 2009* (2012).

example, being used as the basis for obtaining a search warrant, wiretap, or other intrusive investigative tool, as the basis for a criminal indictment in a grand jury proceeding, or as evidence in a criminal prosecution. Where current policy does not already require the approval of at least the Assistant Attorney General,[4] we would require such approval before Section 702 information could be used in these contexts.

We note that it is already very unlikely that Section 702 information would be used in this way because of the existing significant hurdles to the use of *any* FISA-derived information in a criminal proceeding.[5] FISA requires the personal approval of the Attorney General, Deputy Attorney General, or Assistant Attorney General for National Security before FISA-derived information can be used as evidence at trial or in some of the more preliminary stages of the criminal process, such as before the grand jury.[6] FISA also requires that criminal defendants be notified if FISA-derived information will be used against them in a criminal proceeding. And since any decision to use Section 702 information risks revealing the intelligence community's sources and methods, there is always a strong disincentive to permit it. The hurdles imposed by these existing requirements result in Section 702 information being used rarely in the prosecution of even national security–related crimes, and perhaps never in the prosecution of other crimes. As such, our proposal would not create an entirely new and unknown set of rules, but would build an added level of protection for civil liberties into the existing structure.

Concerns with requiring court approval prior to querying: Chairman Medine and Member Wald would require the FBI to obtain FISC approval prior to querying FISA-obtained information, regardless of whether the query relates to a U.S. person, and even in the investigation of foreign intelligence crimes such as terrorism or espionage. For an FBI query for foreign intelligence purposes (not including investigation of foreign intelligence crimes), the FISC would have to first determine that the query was likely to return foreign intelligence information. For an FBI query in the investigation of any crime—including foreign intelligence crimes—the FISC would have to first determine that the query was likely to return evidence relevant to the investigation.[7] We have significant concerns

---

4 *See* Memorandum from Michael B. Mukasey, Attorney General, to all Federal Prosecutors, *Revised Policy on the Use or Disclosure of FISA Information*, at 2-7 (January 10, 2008).

5 50 U.S.C. § 1806(b).

6 *Id*. at §1806(c). We note that the Department of Justice has recently clarified its view of when information used in a criminal proceeding may be "derived from" prior Title VII FISA collection. *See, e.g., United States v. Mohamud*, No. 3:10-CR-475 slip op. at 3 (D. Or. June 24, 2014) (quoting government filing). In addition, the Department's FISA Use Policy imposes additional restrictions to the use of Section 702 information in the context of more routine criminal investigative activities.

7 Foreign intelligence investigations routinely encompass foreign intelligence crimes. How the FBI or the FISA Court would determine which of these standards applied is unclear.

about the implications of this approach, which would likely have significant detrimental consequences far greater than acknowledged (or perhaps intended) by our colleagues.

First and foremost, although the apparent motivation of this proposal is to protect U.S. persons, it could not be limited to U.S. persons in practice. The FBI (our domestic law enforcement agency) naturally does not distinguish between U.S persons and non-U.S. persons, which means this proposed requirement would apply by default to *all* queries of the FISA database, by *all* FBI personnel, in *any* FBI investigation of *any* crime. And requiring the FBI to determine whether the subject of a query is a U.S. person could result in more intrusive investigation of that person than would otherwise occur.[8]

Similarly, although the motivation of the proposal is to address incidental collection of U.S. person information through the Section 702 program, the FBI currently combines all FISA-obtained information in one database, which means that as a practical matter the proposal would prohibit the FBI from searching any FISA-obtained information without first obtaining a court order.

Although Chairman Medine and Member Wald reference a requirement for "judicial approval for queries in ordinary crime situations," the text of their proposal covers even foreign intelligence crimes, meaning that an FBI agent investigating an al Qaeda operative for terrorism would have to go to the FISA court to run a query of any FISA-obtained information. Requiring the FBI to undertake the lengthy and burdensome FISC approval process before an FBI analyst could even query the information would create practical challenges so daunting that it likely never would be pursued. Even if the FBI could obtain prior approval, this would result in significant delay of the investigation and potentially enormous burdens on the FISC. The practical effect of this proposal would be to prevent the FBI from using one of our most valuable foreign intelligence tools to investigate foreign intelligence crimes. It is hard to imagine adopting a rule that is so at odds with the recommendations of the 9/11 Commission, the Webster Commission, and others in the years following 9/11.[9]

In addition to requiring judicial approval, the proposal would impose a standard for the court's approval in investigations of crime that would be unworkable in many circumstances. Database queries are often used at the earliest stages of an investigation – such as during an assessment, perhaps to follow up on a tip. At this stage, an analyst knows very little and conducts a query to see if there is anything at all that creates a reason to

---

[8] Although apparently grounded in Fourth Amendment principles, the proposal makes no distinctions between contents of communications and metadata—as to which there is *no* currently recognized Fourth Amendment interest.

[9] *See* National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States,* at 78-80, 416-418 (2004); The *Webster Commission Report,* at 94-95 and 136-39.

further pursue the investigation. It is hard to imagine the basis on which the FISC could assess what, if anything, will be returned in a database query at this stage, which would require the FISC to deny the application.

Finally, the proposal could actually exacerbate civil liberties concerns in at least two respects. First, a query of information already in the FBI's possession has been considered one of the least intrusive investigative means available, and is therefore one of the first steps taken in any assessment or investigation. But now in order to use this preliminary investigative tool, our colleagues would require the FBI to assemble information sufficient to facilitate meaningful judicial review, which will inevitably require the use of *more* intrusive means. Second, because queries at the early stages of an investigation are often used to eliminate individuals from suspicion, discouraging queries could prevent the discovery of exculpatory information that otherwise might establish an individual's innocence.

NSA and CIA: Our colleagues also would require prior court approval for NSA and CIA queries of Section 702 information when they involve U.S. person identifiers. Based on our review of the current use and extensive oversight of U.S. Person queries at the NSA and CIA, which we have accurately characterized at "rigorous,"[10] the majority has declined to recommend such a requirement.[11]

[10] Board Report at Recommendation 4.

[11] We are also concerned about the potential implications of Chairman Medine and Member Wald's proposal regarding minimization. To the extent that their approach requires an analyst to review U.S. Person communications that the analyst would not otherwise review, we think it far from clear that it is more protective of privacy than leaving those communications in the database unreviewed until the end of the retention period.