PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

---

# *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*

**Separate Statement by Board Member Rachel Brand**

**JANUARY 23, 2014**

**Separate Statement by Board Member Rachel Brand**

I commend the Board and our tiny staff for putting together this comprehensive Report while simultaneously struggling to establish our still-infant agency. Although I disagree with much of the Report's discussion and some of its recommendations, this may be the most thorough description and analysis of the Section 215 bulk telephony metadata collection program ("Section 215 program") that has been published to date.

I concur in most of the Board's recommendations, and I am pleased that we were able to achieve unanimity on so many of them. However, I write separately to briefly note several points on which I disagree with the Report. Most importantly, I dissent from the Board's recommendation to shut down the Section 215 program without establishing an adequate alternative.

***Where I agree with the Board's Report***

I join the Board's proposal to create a process for appointing an independent advocate to provide views to the Foreign Intelligence Surveillance Court ("FISC") in important or novel matters. (Recommendations 3-5.) Although I believe the FISC already operates with the same integrity and independence as other federal courts, I agree with the Board that some involvement by an independent third party will bolster public confidence in the FISC's integrity and strengthen its important role.

Of course, the devil is in the details. Meddling in a system that already works well is risky. Any proposal to change the FISC's operations must, among other things, ensure that the FISC can continue to operate very quickly; not jeopardize the security of the sensitive materials reviewed by the court; provide adequate resources to account for an increased burden on the court; and allow the FISC's judges to retain discretion and control over the participation of an independent advocate in any given case. I believe this Board's recommendations account for all of these considerations better than any of the other proposals that have been offered.

I also sign on to most of the Board's recommendations to provide greater transparency about the government's counterterrorism programs. (Recommendations 6-11.) I agree with the Board that additional transparency, where possible, promotes public confidence in our national security agencies. However, it is important to note that the Board recommends that transparency measures be adopted *to the extent consistent with national security*. It is this qualification that enables me to sign on to the core of those recommendations. I suspect I have a different view than some of my colleagues about how

to implement each of the recommendations, but those details will be worked out in the future.

I do not sign on to the Board's discussion concerning Recommendation 12, because I do not believe that an intelligence program or legal justification for it must necessarily be known to the public to be legitimate or lawful.

Finally, I join the Board's recommendations for immediately modifying the Section 215 program (Recommendation 2) because I believe these changes will ameliorate privacy concerns while preserving the operational value of the program.

***Where I disagree with the Board's Report***

I cannot sign on to the substance of much of the Board's analysis. I am concerned that the Report gives insufficient weight to the need for a proactive approach to combating terrorism, and I hope that the Report will not contribute to what has aptly been described as cycles of "timidity and aggression" in the government's approach to national security.[1] After September 11, 2001, the public demanded to know why the government had not stopped those attacks. Fingers were pointed in every direction, and civil liberties and privacy considerations took a backseat in the public debate immediately following the attacks. Of course, the legal structure under which the agencies operated prior to 9/11 had been put into place in the 1970s as a reaction to the Church Committee's revelations of prior excesses and abuses by the Intelligence Community. Since the recent leaks of classified programs, the pendulum seems to be swinging sharply back in that direction. But I have no doubt that if there is another large-scale terrorist attack against the United States, the public will engage in recriminations against the Intelligence Community for failure to prevent it. These swings of the pendulum, though they may be an inevitable result of human nature, are an unfortunate way to craft national security policy, and they do a disservice to the men and women dedicated to keeping us safe from terrorism.

The primary value that this bipartisan, independent Board can provide is a reasoned, balanced approach, taking into account (as our statute requires) *both* civil liberties and national security interests. We should not overreact to the crisis or unauthorized disclosure du jour, but take a longer view.

With these background considerations in mind, I turn to my reasons for dissenting from the Board's recommendation to shut down the Section 215 program.

---

[1] *See, e.g.,* JACK GOLDSMITH, THE TERROR PRESIDENCY, LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 163-64 (2007).

The Board concludes that the Section 215 program is not legally authorized. I cannot join the Board's analysis or conclusion on this point.

The statutory question—whether the language of Section 215 authorizes the telephony bulk metadata program—is a difficult one. But the government's interpretation of the statute is at least a reasonable reading, made in good faith by numerous officials in two Administrations of different parties who take seriously their responsibility to protect the American people from terrorism consistent with the rule of law. Moreover, it has been upheld by many Article III judges, including over a dozen FISC judges and Judge Pauley in a thorough opinion in a regular, public proceeding in U.S. District Court.[2]

In light of this history, I do not believe this is a legal question on which the Board can meaningfully contribute. If we were addressing this as a matter of first impression, advising the government on whether to launch the program in the first place, we would need to grapple with this question of statutory construction. But we do not approach this question as a matter of first impression. It has been extensively briefed and considered by multiple courts over the course of several years. Some of those cases are ongoing. This *legal* question will be resolved by the courts, not by this Board, which does not have the benefit of traditional adversarial legal briefing and is not particularly well-suited to conducting *de novo* review of long-standing statutory interpretations. We are much better equipped to assess whether this program is sound as a *policy* matter and whether changes could be made to better protect Americans' privacy and civil liberties while also protecting national security.

Because the Board also concludes that the program should be shut down as a policy matter, it seems to me unnecessary and gratuitous for the Board to effectively declare that government officials and others have been operating this program unlawfully for years. I am concerned about the detrimental effect this superfluous second-guessing can have on our national security agencies and their staff. It not only undermines national security by contributing to the unfortunate "cycles of timidity and aggression" that I mentioned earlier, but is also unfair, demoralizing, and potentially legally harmful to the individuals who carry out these programs.

Turning to the constitutionality of the Section 215 program, I agree with the Board's ultimate conclusion that the program is constitutional under existing Supreme Court caselaw.[3] The Board appropriately states that government officials are entitled to rely on

---

[2] *See* Memorandum & Order, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013).

[3] One federal judge recently reached the opposite conclusion, holding that the Section 215 program is likely unconstitutional. *See* Memorandum Opinion, *Klayman v. Obama,* No. 13-0851 (D.D.C. Dec. 16, 2013). This demonstrates that these are difficult legal questions that ultimately will be resolved by the courts.

current law when taking action. But in speculating at great length about what might be the future trajectory of Fourth Amendment caselaw, it implicitly criticizes the government for not predicting those possible changes when deciding whether to operate the program. Perhaps the Supreme Court will amend its views on the third-party doctrine or other aspects of Fourth Amendment jurisprudence in future cases. But that is beside the point in a Report addressing whether the government's actions were legal at the time they were taken and now. Surely government officials should be able to rely on valid Supreme Court precedent without being second-guessed years later by a Board musing on what legal developments might happen in the future.

Of course, the government must seriously consider whether it *should* take actions that intrude on privacy even if it *can* take them as a legal matter. Whether the Section 215 program should continue as a matter of good policy is a question squarely within the Board's core mandate and one that courts have not addressed and cannot resolve. However, I do not agree with the Board's conclusion that the program should be shut down.

Whether the program should continue boils down to whether its potential intrusion on privacy interests is outweighed by its importance to protecting national security.

Starting with the privacy question, on the one hand, any collection program on this scale gives me pause. As the Board discusses, metadata can be revealing, especially in the aggregate (though I do not agree with the Board's statement that metadata may be even "more" revealing than contents). Whenever the government possesses large amounts of information, it could theoretically be used for dangerous purposes in the wrong hands without adequate oversight. Even if there is no actual privacy violation when information is collected but never viewed, accessed, analyzed, or disseminated in any way, as is true of the overwhelming majority of data collected under the Section 215 program, collection and retention of this much data about American citizens' communications creates at least a *risk* of a serious privacy intrusion.

This is why I join the Board's recommendations for immediate modifications to the program (Recommendation 2), including eliminating the third "hop" and reducing the length of time the data is held. Based in part on the Board's lengthy discussions with government officials, I believe these changes would increase privacy protections without sacrificing the operational value of the program.

On the other hand, the government does not collect the content of any communication under this program. It does not collect any personally identifying information associated with the calls. And it does not collect cell site information that could closely pinpoint the location from which a cell phone call was made. The program is

literally a system of numbers with no names attached to any of them. As such, it does not sweep in the most sensitive and revealing information about telephone communications. This seems to have gotten lost in the public debate.

In addition, the program operates within strict safeguards and limitations. The Board's Report describes these procedures, but it bears repeating just how hard it is for the government to make any use of the data collected under this program. For example, before even looking at what the database holds on a particular phone number, an NSA analyst must first be able to produce some evidence—enough to establish "reasonable, articulable suspicion" or "RAS"—that that particular phone number is connected to a specific terrorist group listed in the FISC's order. Only a handful of trained analysts are authorized do this. Before typing the phone number into a search field, the analyst must document the "RAS" determination in writing. And if the results of the query reveal a pattern of calls that seems worth investigating further, the analyst must jump through a series of additional hoops before gathering more information about the communications or distributing that information to other agencies. As a result, only an infinitesimal percentage of the records collected are ever viewed by any human being, much less used for any further purpose. [4]

With the safeguards already in place and the additional limitations this Board recommends, I believe the *actual* intrusion on privacy interests will be small.

On the other side of the equation is the national security value of the program. The Board concludes that the program has little, if any, benefit. I cannot join this conclusion.

There is no easy way to calculate the value of this program. But the test for whether the program's potential benefits justify its continuation cannot be simply whether it has already been the key factor in thwarting a previously unknown terrorist attack. Assessing the benefit of a preventive program such as this one requires a longer-term view.

The overwhelming majority of the data collected under this program remains untouched, unviewed, and unanalyzed until its destruction. But its immediate availability *if it is needed* is the program's primary benefit. Its usefulness may not be fully realized until we face another large-scale terrorist plot against the United States or our citizens abroad. But if that happens, analysts' ability to very quickly scan historical records from multiple

[4] As the Board discusses, there have been lapses in compliance with the program's limitations. Most of these violations have been minor and technical. A few have been significant, though apparently unintentional. Compliance problems are always a matter of concern and demonstrate the need for robust oversight. But it is important to remember that the lapses the Board mentions came to light only because the government *self-reported* violations to the FISC. Those problems were then corrected, under the supervision of the FISC. And these corrective measures and self-reporting occurred *before* these programs were publicly disclosed. That is, they were identified and fixed not because of the scrutiny brought about by an unlawful leak of classified information, but because existing oversight mechanisms worked.

service providers to establish connections (or avoid wasting precious time on futile leads) could be critical in thwarting the plot.

Evidence suggests that if the data from the Section 215 program had been available prior to the attacks of September 11, 2001, it could have been instrumental in preventing those attacks.[5] The clear implication is that this data could help the government thwart a future attack. Considering this, I cannot recommend shutting down the program without an adequate alternative in place, especially in light of what I view to be the relatively small actual intrusion on privacy interests.

That said, if an adequate alternative that imposes less risk of privacy intrusions can be identified, the government should adopt it. The President appears to believe that the government can craft an alternative that retains the important intelligence capabilities of the program but reduces privacy concerns by storing the data outside the government. Although I expect this Board to have a role in crafting any such alternative and I look forward to those discussions, I doubt I could support a solution that transfers responsibility for the data to telephone service providers. This approach would make sense only if it both served as an effective alternative and assuaged privacy concerns, but I am skeptical it would do either. Because service providers are not required to retain all telephony metadata for any particular length of time, asking the service providers to hold the data could not be an effective alternative without legislatively mandating data retention. But data retention could increase privacy concerns by making the data available for a wide range of purposes other than national security, and would raise a host of questions about the legal status and handling of the data and the role and liabilities of the providers holding it. In my view, it would be wiser to leave the program as it is with the NSA than to transfer it to a third party.

Whatever happens to the Section 215 program in the short term, the government should frequently assess whether it continues to provide the potential benefits it is currently believed to have, including whether the incremental benefit provided by the program is eroded by the development of additional investigative tools. This process of re-evaluation should not consist merely of ad hoc conversations among individuals involved in the programs, but should be formalized, conducted at regular intervals with involvement by this Board, approved by officials at the highest levels of the Executive Branch, and

---

[5] *See, e.g., Oversight of the Federal Bureau of Investigation: Hearing before the H. Comm. on the Judiciary*, 113th Cong. 25-26 (2013) (statement of Robert S. Mueller III, Director, Federal Bureau of Investigation) (testifying that if the data from the Section 215 program had been available to investigators before 9/11, it would have provided an "opportunity" to prevent those attacks); Decl. of Teresa H. Shea, Signals Intelligence Director, Nat'l Sec. Agency, ¶ 35, Dkt. 63, in *Am. Civil Liberties Union v. Clapper*, *supra* note 2; Michael Morell, *Correcting the Record on the NSA Review*, WASH. POST, Dec. 27, 2013 (had data from the Section 215 program been available at the time, "it would likely have prevented 9/11").

briefed to the Intelligence and Judiciary Committees. I look forward to working with the intelligence agencies in conducting this analysis.