NSA PROGRAMS

Hearing Before the House Permanent Select Committee on Intelligence

Tuesday, October 29, 2013

Written Testimony of Stephen I. Vladeck

Professor of Law and Associate Dean for Scholarship,
American University Washington College of Law;
Co-Editor-in-Chief, @Just_Security

Chairman Rogers, Ranking Member Ruppersberger, and distinguished members of the Committee:

Thank you for inviting me to testify today—and for inviting the views of outsiders like me on what have historically been such a closely held series of conversations.

Reasonable people will certainly continue to disagree about the proper scope of the NSA's surveillance authorities, especially those undertaken pursuant to section 702 of the Foreign Intelligence Surveillance Act (FISA),[1] and section 215 of the USA PATRIOT Act.[2] Rather than devote my time to taking sides in a debate that has been thoroughly joined,[3] I would like to focus my testimony today on three different, but related propositions—points on which I hope we all have common cause:

First, it is important to keep in mind the extent to which these surveillance authorities should be calibrated—as FISA was in 1978—in order to work around and avoid resolution of *unresolved* tensions in the Supreme Court's Fourth Amendment jurisprudence. Of course, Congress is free to—and oftentimes must—legislate in the shadow of the Constitution, and in the gaps created by the Supreme Court's jurisprudence. But there is a significant risk when Congress does so: Whereas such drafting-into-gaps empowers the government to act, the more expansively the Executive Branch *fills* those gaps, the more likely it is to invite judicial intervention—and even circumscription, if the courts are uneasy about the adequacy of the statutory limitations that the legislature has prescribed. Indeed, as

1. Foreign Intelligence Surveillance Act Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438–48 (codified at 50 U.S.C. § 1881a).

2. Uniting and Strengthening America By Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861).

3. *Compare, e.g.*, Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, LAWFARE RESEARCH PAPER SERIES NO. 3 (Sept. 1, 2013), http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf, *and* David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RESEARCH PAPER SERIES NO. 4 (Sept. 29, 2013), http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf, *with* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 HARV. J. L. & PUB. POL'Y (forthcoming 2013), available at http://justsecurity.org/wp-content/uploads/2013/10/Just-Security-Donohue-PDF.pdf, *and* Marty Lederman, *The Kris Paper, and the Problematic FISC Opinion on the Section 215 "Metadata" Collection Program*, JUST SECURITY, Oct. 1, 2013 (5:25 p.m.), http://justsecurity.org/2013/10/01/kris-paper-legality-section-215-metadata-collection/.

the pending lawsuits filed by the ACLU[4] and EPIC[5] (among others) illustrate, we may already be reaching the point in which the federal judiciary beyond the FISA Court will be reviewing these programs.

Second, regardless of where one comes down on the merits, the inevitability of full-throated judicial review of these programs should provide its own impetus for meaningful reform. It's obvious why those who question the government's interpretation (and underlying constitutionality) of these authorities desire change. But even those who *approve* of programs such as bulk telephony metadata collection and PRISM should also embrace reform—if only to increase the likelihood that these programs will *survive* such judicial review. On the statutory side, it should follow that the more precise the fit between the substantive authorities Congress has provided and the specific programs the government is undertaking, the more likely courts will uphold the Executive Branch's understandings. And with regard to constitutional considerations, the clearer it is that these authorities include meaningful checks and balances designed to minimize their impact on our constitutional rights and other privacy interests, the more likely courts will find them to be consistent with the Fourth Amendment.

Third, and perhaps most significantly, once we accept the urgency of FISA reform, we should also appreciate that there are any number of meaningful and responsible ways to get there from here—both with regard to reforming the substance of the government's surveillance authorities and the processes through which they are exercised. Thus, on the substantive front, even if we cannot all agree on whether the controversial collection authorities should be scaled back in the abstract, Congress could certainly move to *codify* baseline minimization requirements for each content-based surveillance program, rather than leaving them up to the discretion of the Executive Branch and FISA Court—to better limit how the government is allowed to *use* the information it is collecting. Congress might then also provide stiffer penalties for violations of these rules as a means of giving the minimization requirements teeth that, for now, they're quite demonstrably lacking.

With regard to process, I also believe that there is much to commend proposals for some kind of "special advocate" to participate in at least some proceedings before the FISA Court in order to present adversarial briefing and

4. *See* Am. Civil Liberties Union v. Clapper, No. 13-civ-3994 (S.D.N.Y. filed June 11, 2013).

5. *See In re* Elec. Privacy Info. Ctr., No. 13-58 (U.S. filed July 8, 2013).

argument—and then object in cases in which he believes the FISA Court has erred. There's also plenty of room for Congress to bolster the existing notice requirements for cases in which the government seeks to use FISA-derived evidence in criminal prosecutions, and to otherwise exert pressure on the FISA Court to publicize its decisions to the maximum extent practicable.

As significantly, such reforms should not just focus on responding to the controversies of the moment—*i.e.*, the 215 and 702 programs. If we've learned nothing else from this summer, hopefully we've learned the value and importance of meaningful public discourse and debate on these sets of issues—and, along with that, the costs to the government of having to defend these programs only after damaging disclosures concerning their scope and substance.

Ultimately, regardless of which specific path Congress chooses to take, the critical point for present purposes is that it's a false dichotomy to suggest, as some have, that the choice is between preserving the status quo and undermining the efficacy of these programs. Simply put, sufficiently careful and comprehensive FISA reform will only further our national security while better protecting our civil liberties.

I. LEGISLATING INTO GAPS: THE FOURTH AMENDMENT QUESTIONS

As is now well-known, FISA was enacted at least largely to provide legal underpinnings (and constraints) on government surveillance that had previously been conducted solely under the auspices of the Executive Branch.[6] Although the Supreme Court had held in the *Keith* case that there is no "domestic intelligence surveillance" exception to the Fourth Amendment's Warrant Clause,[7] the possible existence of a *foreign* intelligence surveillance exception, and the lower courts' varied and complex answers to that question,[8] underscored the need for a statute both authorizing and circumscribing such surveillance activities—in lieu of constitutional doctrine. In other words, FISA itself was meant to occupy an unsettled area of Fourth Amendment law.

6. *See generally* 1 DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS §§ 2:1 to 3:9, at 37–113 (2d ed. 2012).

7. *See* United States v. U.S. Dist. Ct., 407 U.S. 297 (1972).

8. *See, e.g.*, Steve Vladeck, *More on* Clapper *and the Foreign Intelligence Surveillance Exception*, LAWFARE, May 23, 2012 (3:32 p.m.), http://www.lawfareblog.com/2012/05/more-on-clapper/.

The same can be said of section 215 of the USA PATRIOT Act and section 702 of FISA. Section 215, which authorizes the government to obtain—without a warrant—certain "tangible things" held by businesses deemed to be "relevant" to an ongoing terrorism investigation,[9] capitalizes upon the so-called "third-party" doctrine. That doctrine, which traces its origins in principal part to the Supreme Court's 1979 decision in *Smith* v. *Maryland*,[10] holds that individuals do not have an expectation of privacy in personal information that they voluntarily provide to a third party where the third party uses such information as part of its ordinary course of business—and so the government does not violate the Fourth Amendment when they obtain such information *from* such third-parties without the individuals' consent.[11] At least thus far, the FISA Court opinions that have analyzed the Fourth Amendment questions raised by the bulk telephony metadata program have held them to be squarely settled by *Smith*—because the metadata is all being collected from telecom providers who use the information for business purposes, and is therefore information in which individuals are said to have no legitimate expectation of privacy.[12]

Likewise with regard to section 702 (along with surveillance carried out pursuant to Executive Order 12,333): Insofar as these authorities contemplate sweeping, warrantless interceptions of communications where the targets are reasonably believed to be non-citizens outside the territorial United States,[13] the provision thereby occupies territory left open after the Supreme Court's 1990 decision in *United States* v. *Verdugo-Urquidez*, which suggested that non-citizens outside the territorial United States categorically lack Fourth Amendment rights.[14] And insofar as surveillance conducted pursuant to these authorities might incidentally result in the interception of communications by individuals *with* Fourth Amendment rights, for which the government would usually need a warrant, the "incidental overhears" doctrine suggests that there's no Fourth Amendment

9. 50 U.S.C. § 1861(a)(1).

10. 442 U.S. 735 (1979).

11. *See id.* at 742–45.

12. *See, e.g.*, *In re* Application of the FBI for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR-13-109, slip op. at 6–9 (FISA Ct. Aug. 29, 2013) [hereinafter Eagan Opinion].

13. *See, e.g.*, 50 U.S.C. § 1881a(a)(1).

14. 494 U.S. 259 (1990).

violation so long as the government was not specifically *targeting* such communications.[15]

But even if it *appears* that these programs are therefore free of constitutional defects, the doctrines are not as settled as many may like to believe, potentially leaving these surveillance programs, in their current form, vulnerable to judicial intervention. For example, five different Justices expressed varying degrees of skepticism with the continuing scope of the third-party doctrine in the Supreme Court's January 2012 decision in *United States* v. *Jones*,[16] and even on its own terms, one could argue that there's a difference between information *obtained* by a third-party and information *aggregated* by the government in a manner that is necessarily unavailable to any private entity.[17]

One might also quibble with the extent to which *Verdugo-Urquidez* settled the inapplicability of the Fourth Amendment to non-citizens overseas, especially since Justice Kennedy (whose vote was necessary to the result) appeared uncomfortable with such a categorical rejection of constitutional protections—as opposed to a case-by-case analysis.[18] To similar effect, there is also reason to question the FISA Court of Review's 2008 endorsement of a categorical "foreign intelligence surveillance" exception to the Fourth Amendment's Warrant Clause.[19] But far more significantly, there are strong arguments against application of the "incidental overhears" doctrine to communications by U.S. persons obtained under section 702, both because (1) such communications are obtained on a massive scale;

---

15. *See, e.g.*, United States v. Bin Laden, 126 F. Supp. 2d 264, 280–81 (S.D.N.Y. 2000).

16. *See* 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring); *id.* at 957–64 (Alito, J., concurring in the judgment).

17. That is to say, although individuals may not retain an expectation of privacy in specific data streams they provide to individual third parties (*e.g.*, phone companies; financial institutions; etc.), individuals *may* retain an expectation of privacy in the aggregation of those streams, which, at least in theory, is a capability possessed solely by the government. *Cf.* Kyllo v. United States, 533 U.S. 27 (2001) (holding that individuals retain an expectation of privacy from "plain-view" technologies that can only be deployed by the government, as opposed to other private parties).

18. *See, e.g.*, *Verdugo-Urquidez*, 494 U.S. at 275–78 (Kennedy, J., concurring); *see also* Michael Bahar, *As Necessity Creates the Rule:* Eisentrager*,* Boumediene*, and the Enemy—How Strategic Realities Can Constitutionally Require Greater Rights for Detainees in the Wars of the Twenty-First Century*, 11 U. PA. J. CONST. L. 277, 315 (2009) (observing that Justice Kennedy's concurrence in *Verdugo-Urquidez* is widely viewed as the controlling opinion on the issue of extraterritoriality application of the Fourth Amendment).

19. *See In re* Directives [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008). *But see* Vladeck, *supra* note 8.

and (2) the government is well aware that such communications are likely to be intercepted.[20]

To be clear, my point is not that the 215 and 702 programs, in their current forms, *violate* the Fourth Amendment. I mean only to underscore the open constitutional questions *surrounding* these programs—questions that, in my view, are not nearly as well settled by existing doctrine as the some may believe.

II. THE INEVITABILITY OF FULL-SCALE JUDICIAL REVIEW

The fact that these Fourth Amendment questions are not fully settled is also reinforced *by* those opinions of the FISA Court to which the public has now become privy. Even though we now have the benefit of a series of decisions by the FISA Court explaining why these programs are both consistent with their underlying statutes and the Fourth Amendment,[21] those opinions leave a lot to be desired. Indeed, not only have criticisms of the FISA Court's analyses come from all sides,[22] but the Justice Department's defense of the legality of the metadata program, at least, has focused on arguments largely *distinct* from those endorsed by the FISA Court.[23]

I don't mean to criticize the FISA judges themselves, for in many respects, they've been handed a loaded deck.[24] Virtually all of the proceedings before the FISA Court thus far have been *ex parte*, without the benefit of adversarial briefing or argument. It is true that there is a robust *internal* review process within the FISC, and that the NSA appears to have *self-reported* its errors; but that may not be enough, especially when dealing with such complex and massive programs. We now know, for example, that there have been a series of instances in which the

20. *See, e.g.*, United States v. Bin Laden, 126 F. Supp. 2d 264, 280–82 (S.D.N.Y. 2000); *see also* [REDACTED], 2011 WL 10945618, at *26–27 & n.67 (FISA Ct. Oct. 3, 2011) [hereinafter Bates Opinion].

21. *See, e.g.*, Eagan Opinion, *supra* note 12.

22. *See, e.g.*, Orin Kerr, *My (Mostly Critical) Thoughts on the August 2013 FISC Opinion on Section 215*, THE VOLOKH CONSPIRACY, Sept. 17, 2013 (7:39 p.m.), http://www.volokh.com/2013/09/17/thoughts-august-2013-fisc-opinion-section-215/.

23. *See, e.g.*, Defendants' Memorandum of Law in Support of Motion To Dismiss the Complaint at 19–31, ACLU v. Clapper, No. 13-3994 (S.D.N.Y. filed Aug. 26, 2013), *available at* https://www.aclu.org/files/assets/govt_motion_to_dismiss.pdf.

24. *See* James G. Carr, *A Better Secret Court*, N.Y. TIMES, July 23, 2013, at A21.

government, according to the FISA Court, *misled* the court about the nature of its surveillance programs and/or its interpretation of the relevant statutory authorities.[25]

The upshot of these points is the conclusion that the open questions I've described above will not receive a full judicial airing before the FISA Court itself. And that fact has a lot to say about why I believe it's likely that these programs will receive more sweeping judicial review sooner or later. Indeed, the U.S. District Court for the Southern District of New York will hear oral argument late next month on the ACLU's lawsuit challenging the bulk metadata program on statutory and constitutional grounds,[26] and the Supreme Court is also soon set to consider an application for extraordinary relief from the Electronic Privacy and Information Center (EPIC) raising analogous challenges to the FISA Court's orders at the heart of the bulk metadata program.[27] We also learned late Friday that the government has also now notified a federal criminal defendant in Colorado of its intent to introduce evidence obtained under section 702 against him in his criminal trial,[28] which will undoubtedly spawn litigation over the constitutional question there.

Thus, regardless of *which* of these judicial proceedings gets there first, it is only a matter of time before the federal courts are asked to provide full-fledged answers to the statutory and constitutional questions surrounding the 215 and 702 programs. And it stands to reason that, if and when that time comes, meaningful statutory reforms will go a long way toward insulating the programs from judicial invalidation.

Take the metadata program as an example: Whether or not the program in its current form *is* consistent with Congress's intent when it enacted and amended section 215—and when it enacted another law expressly *prohibiting* telephony service providers from turning over customer records except pursuant to authorities

25. *See* Bates Opinion, *supra* note 20, at *5 n.14.

26. *See supra* note 4.

27. *See supra* note 5.

28. *See* Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES, Oct. 27, 2013, at A21; *see also* Second Notice of Intent To Use Foreign Intelligence Surveillance Act Information, United States v. Muhtorov, No. 12-cr-00033 (D. Colo. filed Oct. 25, 2013), *available at* https://www.documentcloud.org/documents/810241-faa-notice.html.

other than section 215[29]—is a question on which reasonable minds have vigorously disagreed.[30] But what seems beyond dispute is that the program today is operated on terms far broader than what some Members of Congress who initially drafted section 215 contemplated.[31] And so, as between judicial review of a program that seems increasingly divorced from its statutory underpinnings, and judicial review of a surveillance scheme that hews fairly closely to statutory text, it seems clear which is more likely to survive. And the more Congress is specifically trying to prevent the government from misusing or otherwise abusing its authorities to obtain information and/or communications for which it lacks a legal basis, the more likely that the programs will withstand *constitutional* scrutiny, as well.

My point is fairly straightforward, to be sure; but insofar as the government's surveillance authorities under FISA operate in a constitutional shadow, the longer that shadow becomes, the more likely these authorities will be carefully scrutinized by the federal courts—scrutiny that meaningful statutory reform could go a long way toward satisfying.

Finally, and perhaps most significantly, it bears emphasizing that this discussion should hardly be limited to those issues currently on the front lines of American discourse. Although the 215 and 702 programs have excited the most public opinion in recent months, Congress should also ask whether similar reforms might be appropriate for *other* surveillance programs—including those programs the existence and/or scope of which are still classified. For as much as we have learned this summer about bulk metadata collection and PRISM, it only seems fair to assume that there are a number of additional programs to which the American public is *not* privy—and yet which may be in at least as much need of the same kinds of reforms. Put another way, reforms should be structural, and not just at the visible margins.

---

29. *See, e.g.*, 18 U.S.C. § 2702(b)(2) (not including section 215 among the authorities listed as "exceptions" to statutory bar on disclosure of records by electronic communications service providers).

30. *See, e.g.*, sources cited *supra* note 3.

31. *See, e.g.*, Letter from Hon. F. James Sensenbrenner, Jr., to Hon. Eric H. Holder, Jr. (Sept. 6, 2013), *available at* http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf.

III. SOME THOUGHTS ON REFORMS

Of course, not all reforms are equal—and no one reform is a magic bullet. Thus, I don't mean to take sides as between the various proposals for FISA reform currently percolating in Congress. I must also confess that I am profoundly ambivalent about whether reform should prohibit the bulk *collection* of information on a mass, suspicionless scale—not because I don't have strong views on the matter, but because I fear that too many of the arguments *justifying* such government surveillance are based on considerations that cannot adequately be publicized.[32]

Instead, I think it would be far more productive to briefly outline a few potential reforms that strike me as especially attractive even (if not especially) in the absence of new, front-end collection restrictions:

On the substantive side, Congress might start by clarifying which collections are permitted on such a wholesale, suspicionless scale, and which aren't. For example, is there a meaningful distinction between telephony metadata and, *e.g.*, internet metadata? Is PRISM consistent with what Congress meant when it initially enacted section 702? Are there other specific collection authorities that are being used to conduct surveillance that Congress never intended to—and still would not—authorize? Regardless of what one thinks the scope of the government's surveillance authorities *should* be, greater public transparency concerning what they *are* (and are *not*) seems an important starting point for any serious reform discussion.

Additionally, two obvious places for non-collection reforms involve the minimization requirements that apply to content-based surveillance programs. Although the *existence* of minimization requirements is mandated by statute,[33] the statutes have very little to say about the *substance* of those requirements. And although it may not be ideal for Congress to provide comprehensive requirements by statute on a program-by-program basis, it does seem to me to be obvious that Congress should prescribe a much more detailed statutory minimization *baseline*—

32. Without a full appreciation of the government's technological capabilities, it is difficult to assess the efficacy of alternatives to those surveillance methods that have been disclosed, and, as such, difficult to assess whether such bulk collection is truly "necessary" as compared to less-restrictive alternatives such as a query-based approach. Of course, this Committee is not saddled with the same lack of information.

33. *See, e.g.*, 50 U.S.C. § 1881a(e); *see also id.* § 1801(h) (providing minimal definition of "minimization procedures").

basic use restrictions that are a matter of statutory command, and not just Executive Branch or FISA Court discretion. To that end, it is certainly worth considering whether any and all post-collection querying of information involving U.S. persons must always be based upon reasonable, articulable suspicion ("RAS"). Congress might also consider clearer and harsher *penalties* for minimization violations—both when the violation appears to be authorized (as in the circumstances in which the FISA Court noted that government had misled it), or when it arises from the *ultra vires* conduct of individual government employees. Even without scaling back the government's substantive collection reforms, such amendments could dramatically help to improve checks and balances *within* these programs.

On the process side, it does seem like an especially good idea to allow for greater adversarial engagement before the FISA Court—especially in those cases raising new questions of legal interpretation. Whether called a "special advocate" who nominally represents the public, or a security-cleared counsel specifically representing the putative targets of government surveillance, it seems to me obvious (as it did to two of the court's former judges)[34] that the FISA Court would better be able to discharge its duties with the assistance of able counsel from more than just the government's perspective.[35]

Congress might also consider ramping up the FISA Court's transparency—not by requiring publication of all of its work, but by at least creating a default (albeit *rebuttable*) presumption in favor of publication,[36] along with more rigorous

34. *See, e.g.*, Carr, *supra* note 24.

35. To be sure, a complex series of Article III standing issues might arise if and when the special advocate were empowered to *appeal* an adverse decision by the FISA Court to the FISA Court of Review. *See, e.g.*, Hollingsworth v. Perry, 133 S. Ct. 2652 (2013) (holding that defenders of state ballot proposition—as opposed to state itself—had no standing to appeal its invalidation by a district court because they had no "direct stake" in the outcome of their appeal). But however his responsibilities are defined, the participation of a "special advocate" before the FISA Court *itself* raises no such concerns since the only party that needs standing before that tribunal is the plaintiff—*i.e.,* the government. Thus, so long as proceedings before the FISA Court *presently* satisfy Article III's adversity requirement, *see, e.g.*, *In re* Sealed Case, 310 F.3d 717, 732 & n.19 (FISA Ct. Rev. 2002), no *new* Article III problems would be created by the participation of an additional party, on almost any terms, in the FISA Court.

36. There is no present statutory rule regarding publication of FISA Court opinions. That court's own rules leave publication to the discretion of the individual judge. *See* U.S. For. Intel. Surv. Ct. Rules of Proc. R. 62(a) (2010). And although mandatory publication might raise constitutional concerns, it should follow that a rebuttable publication presumption would not interfere with any indefeasible constitutional authority that it might be argued the President possesses in this field.

reporting requirements both to Congress (and not just the intelligence committees), and, in some cases, to the public as well. After all, for as much as we now know about the 215 and 702 programs, there is also the prospect of additional current or future secret government surveillance programs to which we have not been, or otherwise will not become, privy. And if we've learned nothing else from the past few months, hopefully we now appreciate the significance of meaningful public understanding, awareness, and opportunity to engage on the substance of those activities the government carries out in our name—especially those that end up directly affecting United States persons.

* * *

Thank you again for the opportunity to testify before the Committee today. I look forward to your questions.