STATEMENT

of

Paul Rosenzweig
Red Branch Consulting, PLLC
Professorial Lecturer in Law, George Washington University
Washington, D.C.

before the

Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
United States Senate

November 13, 2013

Surveillance and Transparency

Introduction

Chairman Franken, Ranking Member Flake, and Members of the Subcommittee, I thank you for your invitation to appear today and present testimony on increasing the transparency of NSA surveillance programs.

My name is Paul Rosenzweig and I am the Principal and founder of a small consulting company, Red Branch Consulting, PLLC, which specializes in, among other things, cybersecurity policy and legal advice. I am also a Professorial Lecturer in Law at George Washington University where I teach a course on Cybersecurity Law and Policy and a Senior Advisor to The Chertoff Group. In addition, I serve as an Adjunct Lecturer at Northwestern University, Medill School of Journalism; a member of the American Bar Association's Standing Committee on Law and National Security; a Distinguished Visiting Fellow at the Homeland Security Studies and Analysis Institute; a Visiting Fellow at The Heritage Foundation; and as a Contributing Editor at the blog, *Lawfare* (www.lawfareblog.com). From 2005 to January 2009 I served as the Deputy Assistant Secretary for Policy in the Department of Homeland Security.

Needless to say, my testimony today is in my individual capacity and does not reflect the views of any institution with which I am affiliated or any of my various clients. Much of my testimony today is derived

from prior academic work I have done in this field, most notably the book, *Cyber Warfare: How Conflict in Cyberspace is Challenging America and Changing the World* (Praeger Press 2013).[1]

Before I begin, two caveats are in order. First, as the current holder of an active Top Secret security clearance I am enjoined not to access classified materials that have been illegally disclosed. Naturally, that has caused a bit of a challenge in preparing testimony, since some of what is the subject of discussion today is public only because of such illegal disclosures. Fortunately, however, many of the most important underlying materials have been properly declassified by the Director of National Intelligence and may, therefore, be discussed in open session. Equally fortunately, I can confidently state that none of the programs we will be discussing today were within my purview when I was at the Department of Homeland Security. Hence everything I speak about today is based on the public record, as I understand it – without, by the way, necessarily assuming that everything in that record is an accurate reflection of what is actually happening within NSA and the Intelligence Community.

Second, in offering my thoughts to you today, I necessarily tread where others who are far smarter than I have already walked.[2] In particular, I have relied upon two truly magnificent legal analyses of the topic of NSA surveillance, one by Steve Bradbury, who served in the Office of Legal Counsel during the Bush Administration,[3] and the other by David Kris, who served as Assistant Attorney General for the National Security Division during the Obama Administration.[4]

In my testimony today, I want to make four basic points:

- First, transparency is good. But, too much transparency defeats the very purpose of democracy;
- Second, understanding the proper ground of transparency and its relationship to NSA surveillance and proposed enhancements leads me to conclude that requiring disclosure of aggregate (but not company specific) data about collection efforts will (if properly implemented) improve transparency;
- Third, the most effective reforms for achieving better transparency are likely structural rather than legislative; and

[1] I am, to a large degree, also relying on material I originally prepared as testimony for the House Permanent Select Committee on Intelligence. In the end, a scheduling conflict prevented me from appearing and I posted that draft testimony (portions of which are repeated here) on the *Lawfare* blog. *See* Reforming the NSA Surveillance Programs – The Testimony I Would Have Given (Oct. 24, 2013), http://www.lawfareblog.com/2013/10/reforming-the-nsa-surveillance-programs-the-testimony-i-would-have-given/.

[2] As Sir Isaac Newton said, if I see farther it is because I am "standing on the shoulders of giants." Letter to Robert Hooke (15 February 1676).

[3] Steven G. Bradbury, "Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702," 1 Lawfare Res. Paper Series No. 3 (Sept. 2013), http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf.

[4] David S. Kris, "On the Bulk Collection of Tangible Things," 1 Lawfare Res. Paper Series No. 4 (Sept. 2013), http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf.

- Fourth, our current system of intelligence oversight generally works. It is incumbent on this Subcommittee and those in Congress with knowledge of how our intelligence apparatus operates to defend that system as effective and appropriate.

Cyberspace is the natural battleground for enhanced analytical tools that are enabled by the technology of data collection. If our goal is to combat terrorists or insurgents (or even other nations) then the cyber domain offers us the capacity not just to steal secret information through espionage, but to take observable public behavior and information and use sophisticated analytic tools to develop a more nuanced and robust understanding of their tactics and intentions. Likewise, it can be used by our opponents to uncover our own secrets.

In considering this new capability we can't have it both ways. We can't with one breath condemn government access to vast quantities of data about individuals, as a return of "Big Brother"[5] and at the same time criticize the government for its failure to "connect the dots" (as we did, for example, during the Christmas 2009 bomb plot attempted by Umar Farouk Abdulmutallab).[6]

More to the point —these analytical tools are of such great utility that governments will expand their use, as will the private sector. Old rules about collection and use limitations are no longer technologically relevant. If we value privacy at all, these ineffective protections must be replaced with new constructs – likely including greater transparency. The goal then is the identification of a suitable legal and policy regime to regulate and manage the use of mass quantities of personal data.

Transparency[7]

Let me begin the analysis by noting the significance of transparency and oversight, generally, but also their contingent value. Transparency is a fundamental and vital aspect of democracy. Those who advance transparency concerns often, rightly, have recourse to the wisdom of James Madison, who observed that democracy without information is "but prologue to a farce or a tragedy."[8]

---

[5] *E.g.* William Safire, "You Are a Suspect," *The New York Times*, Nov. 14, 2002, at A35. This criticism led directly to the termination of one program and the creation of the Technology and Privacy Advisory Committee, http://www.defense.gov/news/Jan2006/d20060208tapac.pdf.

[6] *See*, *e.g.*, Scott Shane & Eric Lipton, "Passengers' Actions Thwart a Plan to Down a Jet," *The New York Times,* Dec. 27, 2009, at A1.

[7] I first wrote about the thoughts in this section in Paul Rosenzweig, Calibrated Openness, Harv. Int'l Rev. (Summer 2004).

[8] Madison to W.T. Barry (Aug. 4, 1822), *The Founders' Constitution* Ch. 18, Doc. 35, http://press-pubs.uchicago.edu/founders/documents/v1ch18s35.html. As with many aphorisms from the Founders, Madison was probably talking about something else other than transparency when he wrote these words. *See* Michael Doyle, "Misquoting Madison," Legal Affairs (July-August 2002) ("what Madison was talking about was not government information, but the Three Rs," *i.e.* education), http://www.legalaffairs.org/issues/July-August-2002/scene_doyle_julaug2002.msp. Nevertheless, the words have come to serve as a symbol for those who favor greater government transparency.

Yet Madison understood that transparency was not a supreme value that trumped all other concerns. He also participated in the U.S. Constitutional Convention of 1787, the secrecy of whose proceedings was the key to its success. While governments may hide behind closed doors, U.S. democracy was also born behind them. It is not enough, then, to reflexively call for more transparency in all circumstances. The right amount is debatable, even for those, like Madison, who understand its utility.

What we need is to develop an heuristic for assessing the proper balance between opacity and transparency. To do so we must ask, why do we seek transparency in the first instance? Not for its own sake. Without need, transparency is little more than voyeurism. Rather, its ground is oversight--it enables us to limit and review the exercise of authority.

In the domain of NSA surveillance, the form of oversight should vary depending upon the extent to which transparency and opacity are necessary to the new capabilities and their impact on the public. Allowing some form of surveillance is vital to assure the protection of American interests. Conversely, allowing full public disclosure of our sources and methods is dangerous – identifying publicly how we conduct surveillance risks use of that information by terrorists and, in turn, draws a roadmap of which threats are not known. Thus, complete transparency will defeat the very purpose of disclosure and may even make us less secure.

What is required is a measured, flexible, adaptable transparency suited to the needs of oversight without frustrating the legitimate interests in limiting disclosure. Here, public disclosure through widespread debate in Congress and the public should be limited, in favor of a model of delegated transparency -- Congressional and Executive Branch review (for example, random administrative and legislative auditing of how the government is using the information provided) that will guard against any potential for abuse while vindicating the manifest value of limited disclosure.

In short, Madison was not a hypocrite. Rather, opacity and transparency each have their place, in different measures as circumstances call for. The wisdom of Madison's insight--that both are necessary--remains as true today as it was 226 years ago.

Assessing Transparency at the NSA

With these principles in mind, let me now turn to an assessment of the Surveillance Transparency Act of 2013, S. 1621.[9] As you will gather, I tend to favor those aspects of the bill that create delegated or calibrated transparency and respond to the new paradigm of data analytics and privacy, while disfavoring those that don't. I also note some things that might be better solutions to the transparency question that you might consider adding to the bill.

[9] I refer in this testimony to the version of S. 1621 introduced on October 30, 2013 by Senator Franken with Senator Heller as a co-sponsor.

Many have suggested that the NSA be obliged to be more transparent in revealing the nature and frequency of certain types of data collection activities, or alternatively, the frequency of data collection requests to Internet Service Providers (ISPs). This is one of those situations where the virtues of transparency, which are very real, need to be carefully calibrated to avoid unnecessary harm.

Here, we might ask what the ground of transparency is? Presumably it is to enhance the confidence that Americans have in the operation of their security agencies. If that is the case, which I think it is, then the virtues of public oversight are served by the disclosure of aggregate numbers of requests and generic descriptions of type. More details risk compromising sources and methods, but at a reasonable level of detail we can get much of the oversight we want without too grave a damage to our capabilities.

Section 2: To that end, I find myself reasonably supportive of Section 2 of the bill. To the extent that existing bulk data programs have already been unlawfully disclosed there is little value in continuing to maintain a veil of secrecy surrounding the number of FISA orders issued or an estimated number of how many individuals are subject to surveillance. I do, however, have two constructive suggestions for modification to the bill's requirement that I offer for your consideration:

First, though the text of the bill does ask that the Administration report on the number of FISA applications that are "modified" by the FISC, I think that this does not quite capture the nature of FISC oversight and, to some degree, tends to understand the nature of the interaction between the Court and the Executive Branch. As Chief Judge Walton recently advised this Committee,[10] fully 24% of the applications made to the FISC are modified in significant and substantive ways. While the phrase "modified" might be read to encompass both technical and conforming amendment to applications, as well as significant changes in scope and content, the oversight debate is really only advanced by transparency about the later, more substantive, modifications. I suggest that you consider clarifying this provision to make it clear that only "real" modifications are to be reported.

Second, the bill seems to assume that all of the disclosures to be made will relate to formerly-covert programs that have already been illegally disclosed. In other words, in calling for disclosures about the types of data collected and the frequency of computer-assisted queries, it appears to me that the bill operates from the unstated presumption that the only programs to which these might apply are the phone metadata; internet metadata; and PRISM/internet content programs already disclosed.

I am concerned that implicit assumption may unwarranted. I don't pretend to know the full scope and extent of covert collection programs currently being run under those legal authorities. Indeed, to the extent they have not yet been illegally disclosed they are, by definition, outside my knowledge. Perhaps none exists – but I don't know that either. And, perhaps (though I am skeptical) disclosures about numbers of applications and numbers of interceptees, as well as a break down based on the type of communication at issue, can be made without disclosing information that would allow one to infer the

[10] Chief Judge Walton to Sen. Patrick Leahy (Oct. 11, 2013), http://www.uscourts.gov/uscourts/courts/fisc/chairman-leahy-letter-131011.pdf

existence of a program that remains (and properly ought to remain) covert. But I think it more likely that such disclosures might reveal heretofore classified programs, to the detriment of our nation's security.

I am sure that is not the intent of this bill. As the sponsors have made clear they seek to foster debate about national security matters while not degrading our nation's capabilities – a goal I'm sure we all share. It is essential, therefore, that the bill's text be modified to permit the Executive Branch to decline to provide a complete data set in the called-for report when doing so would publicly disclose sources and methods that are properly classified and have not been disclosed. In practice, this would mean a report with data relating to disclosed programs only; or a report where the estimates of data were such that in the Executive Branch's judgment a full report could be made without disclosing the existence of classified programs.

As I said, without knowledge of the existence (or non-existence) of other classified programs, I cannot be certain that my theoretical concern is grounded in a realistic fear. But I am sufficiently worried about the prospect that I consider such a modification essential to the bill.

Section 3: The considerations of transparency that I adduced earlier lead me to conclude that Section 3 of the bill, which would allow individual companies to disclose aggregate requests made of them, individually, is generally less well-founded. That degree of specificity is certainly in the ISPs interests – it responds, I am sure, to their own corporate needs and would serve as a palliative to public pressure. But that type of disclosure it isn't in our collective national interest. Too much detail risks telling malicious actors which providers the government is focusing on (and, thus, which they should avoid) . If we begin with the premise that NSA is a *spy* agency, we need it to operate effectively. We should avoid systematically giving our opponents too much information that allows them to develop alternate strategies for avoiding surveillance.

Structural Changes: Finally, given my views, you will not be surprised that I think that most of the more effective possible changes lie not in significant legislative tinkering and transparency requirements, but rather in interstitial structural and operational reforms that improve the audit and oversight process without fundamentally altering the capabilities of NSA or the IC organizations. Here are a few (listed just in bullet point form) that might be worth thinking about:

- Make the NSA Inspector General a presidential appointment, with Senate confirmation;
- Require statutorily, the appointment of an NSA Civil Liberties & Privacy Officer;
- Change the jurisdiction of the Privacy and Civil Liberties Oversight Board to include all intelligence activities, not just those with a counter-terrorism focus;
- Create panels of cleared external reviewers for consultation by the DNI regarding new programs;
- Institutionalize privacy and civil liberties concerns by making it a factor in performance reviews; and

- Have the DNI annually report in a public forum on privacy and civil liberties matters.

Congressional Responsibility

I will conclude with one final point, more about Congress and this Subcommittee than the NSA. Madison's fundamental insight about transparency is that it is not an absolute value, but rather a relative one. Since the mid-1970s, with the reforms prompted by the Church and Pike Committee investigations, we in America have been engaged in an experiment – an experiment to see whether Madison's insight can be converted to reality. The question we have been asking is whether it is possible for a country like America to have covert operations under law – or, to coin a phrase, whether we can have intelligence collections within the bounds of democracy.

To my mind the system of delegated transparency, where Congress stands in for the general public, has worked reasonably well – allowing us to use intelligence capabilities while minimizing the risks of abuse of law. Today, however, thanks to recent disclosures, that system is under assault. Most who challenge the system do so from the best of motives. But I have little doubt that there are some whose calls for transparency mask the intention of diminishing American capabilities.

And that, I think, means that in this post-Snowden era, this Subcommittee (and its other Congressional counterparts)[11] bear a great responsibility. To you falls the task of defending the integrity of our current system of intelligence oversight. While I have spoken in my testimony of possible reforms to the NSA's programs, both legislative and structural, the critical insight for me is that, despite the hue and cry, the system is not badly broken. It can be improved, but in the main it has produced a reasonably effective system of oversight that, if the public record is an accurate reflection, resulted in precious little abuse of the sort we ought to fear.

You should be proud of that record and of your role in creating it. Can the Senate, perhaps, do a better job of oversight? I have no doubt. But in the end, perhaps I have greater confidence in you than you do in yourselves. Notwithstanding the calls for reform and the many plausible reforms you might consider, this Congress should defend the essential structure of our current system. And that, in the end, means rejecting most calls for wholesale reform and complete transparency, and, instead, defending the role of graduated or delegated oversight.

[11] I am not alone in making this point. My colleague Ben Wittes said something very similar to the Senate Select Committee on Intelligence last month. Statement of Benjamin Wittes before the Select Committee on Intelligence, United States Senate (Sept. 26, 2013), www.intelligence.senate.gov/130926/wittes.pdf.