S. HRG. 113–365

THE SURVEILLANCE TRANSPARENCY ACT OF 2013

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY,
TECHNOLOGY AND THE LAW

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

NOVEMBER 13, 2013

Serial No. J–113–40

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
89–466 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

DIANNE FEINSTEIN, California	CHUCK GRASSLEY, Iowa, *Ranking Member*
CHUCK SCHUMER, New York	ORRIN G. HATCH, Utah
DICK DURBIN, Illinois	JEFF SESSIONS, Alabama
SHELDON WHITEHOUSE, Rhode Island	LINDSEY GRAHAM, South Carolina
AMY KLOBUCHAR, Minnesota	JOHN CORNYN, Texas
AL FRANKEN, Minnesota	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	TED CRUZ, Texas
RICHARD BLUMENTHAL, Connecticut	JEFF FLAKE, Arizona
MAZIE HIRONO, Hawaii	

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

AL FRANKEN, Minnesota, *Chairman*

DIANNE FEINSTEIN, California	JEFF FLAKE, Arizona, *Ranking Member*
CHUCK SCHUMBER, New York	ORRIN G. HATCH, Utah
SHELDON WHITEHOUSE, Rhode Island	MICHAEL S. LEE, Utah
CHRISTOPHER A. COONS, Delaware	JOHN CORNYN, Texas
MAZIE HIRONO, Hawaii	LINDSEY GRAHAM, South Carolina

ALVARO BEDOYA, *Majority Chief Counsel*
ELIZABETH TAYLOR, *Minority Chief Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Franken, Hon. Al, a U.S. Senator from the State of Minnesota	1
prepared statement	34
Flake, Hon. Jeff, a U.S. Senator from the State of Arizona	3
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont, prepared statement	36

WITNESSES

Witness List	33
Heller, Hon. Dean, a United States Senator from the State of Nevada	3
Litt, Hon. Robert S., General Counsel, Office of the Director of National Intelligence, and J. Bradford Wiegmann, Deputy Assistant Attorney General, National Security Division, Department of Justice, Washington, DC	5
prepared statement	37
Bankston, Kevin S., Senior Counsel and Director, Free Expression Project, Center for Democracy & Technology, Washington, DC	18
prepared statement	43
Rosenzweig, Paul, Principal, Red Branch Consulting, PLLC, and Professorial Lecturer in Law, George Washington University, Washington, DC	20
prepared statement	58
Salgado, Richard, Director, Law Enforcement and Information Security Matters, Google, Inc., Mountain View, California	21
prepared statement	65

QUESTIONS

Questions submitted by Senator Leahy for Kevin Bankston	72
Questions submitted by Senator Flake for Paul Rosenzweig	73

QUESTIONS AND ANSWERS

Responses of Kevin Bankston to questions submitted by Senator Leahy	74
Responses of Paul Rosenzweig to questions submitted by Senator Flake	93

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

Alexander, Keith B., Director, NSA, statement	95
Felten, Edward W., Professor of Computer Science and Public Affairs, Princeton University, statement	102

THE SURVEILLANCE TRANSPARENCY ACT OF 2013

WEDNESDAY, NOVEMBER 13, 2013

U.S. SENATE,
SUBCOMMITTEE ON PRIVACY,
TECHNOLOGY, AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:03 a.m., in Room SD–226, Dirksen Senate Office Building, Hon. Al Franken, Chairman of the Subcommittee, presiding.

Present: Senators Franken, Leahy, Blumenthal, Flake, and Lee.

OPENING STATEMENT OF HON. AL FRANKEN, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Chairman FRANKEN. This hearing will come to order. Welcome to the Senate Judiciary Subcommittee on Privacy, Technology, and the Law. The subject of this hearing is my bill, the Surveillance Transparency Act of 2013. I am proud to say that 2 weeks ago I reintroduced this bill with the support of my friend and colleague, Senator Dean Heller of Nevada, who we will be hearing from in just a moment.

This bill is urgently necessary. Americans understand that we need to give due weight to privacy, on the one hand, and national security, on the other. But Americans are also naturally suspicious of executive power, and when the Government does things secretly, Americans tend to think that power is being abused. This is exactly the place where congressional oversight is useful and necessary.

For months now, there has been a steady stream of news stories about the NSA's surveillance programs. And yet right now, by law, Americans cannot get really the most basic information about what is going on with these programs. Consider this: It has been months since the PRISM program and the telephone call records program were revealed to the public. And yet to this day, Americans do not know the actual number of people whose information has been collected under those programs; they do not know how many of those people are American; and they have no way of knowing how many of these Americans have had their information actually seen by government officials—as opposed to just being held in a database.

The administration has taken good steps in good faith to address this problem. But I am afraid that these steps are too little and that they are not permanent.

And so Americans still have no way of knowing whether the Government is striking the right balance between privacy and security

or whether their privacy is being violated. I believe there needs to be more transparency.

I have written a bipartisan bill to address this. It will require that the NSA disclose to the public how many people are having their data collected under each key foreign intelligence authority. It would make the NSA estimate how many of those people are American citizens or green card holders and how many of those Americans have had their information actually looked at by government agents.

My bill would also lift the gag orders on Internet and phone companies so that those companies can tell Americans general information about the number of orders they are getting under each key authority and the number of users whose information has been produced in response to those orders.

Right now, as a result of those gags, many people think that American Internet companies are giving up far more information to the Government than they likely are. The Information Technology & Innovation Foundation estimates that American cloud computing companies could lose $22 to $35 billion in the next 3 years because of concerns about their involvement with surveillance programs. The analytics firm Forrester puts potential losses much higher, at around $180 billion.

A few companies have litigated and secured permission to publish limited statistics about the requests that they get. But again, this is too little, and it is not permanent.

My bill would permanently ensure that the American people have the information they need to reach an informed opinion about government surveillance. And it would protect American companies against losing business from misconceptions about their role in these programs.

I am pleased to say that this bill is the leading transparency proposal in the Senate, supported by a strong coalition of tech companies and civil liberties groups. The version as introduced gained the support of 12 senators, including the Chairman of the full Judiciary Committee, Patrick Leahy. I anticipate that we will soon be adding our original supporters onto the new bipartisan bill, hopefully with some additional support as well.

The purpose of this hearing is to make the case for this bill and to improve it by getting the feedback of top experts in the administration, privacy groups, and the private sector. I have specifically asked the Office of the Director of National Intelligence and the Department of Justice to provide candid comments on this bill, especially any concerns they have. I have already added provisions to the bill to protect national security, but I want to know of any further concerns that they have. I suspect that I will agree with them in some cases and disagree with them in others. In those cases, I want to have an open exchange about the disagreements.

That said, I want it to be clear at the outset that I have the utmost respect for the men and women of our intelligence community. I think they are patriots, and I think they have and do save lives.

I look forward to starting this conversation. With that, I will turn to our Ranking Member, Senator Flake.

Senator.

OPENING STATEMENT OF HON. JEFF FLAKE, A U.S. SENATOR FROM THE STATE OF ARIZONA

Senator FLAKE. Thank you, Senator Franken, and I appreciate those who will testify today. This is the first Subcommittee hearing we have had, and I suppose that given the rate at which technology develops, this will be an important Subcommittee as we go along to try to strike that balance that you talked about between privacy issues, between transparency, and national security. I look forward to this hearing to see if we have this legislation, if this bill before us actually strikes that balance. And I come to this hearing with an open mind and realize that this is really a struggle the Congress goes through continually.

I was around when the PATRIOT Act passed. There were issues with that, where we authorized it but then sunsetted a lot of the provisions that we needed to deal with later and then dealt with those later. We were continually with technology developing, continually trying to strike the right balance. The security leaks that we have had in the past couple of years and certainly in the past couple of months have undermined the confidence that the public has in what we are doing here, and that I think is damaging.

So I look forward to more transparency, whether in this legislation or some version of it or in some other way to make sure that people are confident that their public officials have transparency in mind and the best interests of the public in mind here.

So, with that, I look forward to hearing the testimony.

Chairman FRANKEN. Thank you, Senator Flake. This is the first hearing of this Subcommittee in this Congress, and I am happy to have you as the new Ranking Member of this Subcommittee.

It is now my pleasure to introduce your friend and colleague, the Senator from Nevada, Senator Heller. Two weeks ago, Senator Heller and I introduced an improved version of this bill. I think that Senator Heller's support for this bill and his presence here speaks to the fact that transparency is a bipartisan issue. Some of the best work in the Judiciary Committee on the issue of transparency has come from our Chairman and others on our side working with folks like the Ranking Member, Senator Grassley, and Senator Cornyn and many others. This bill is an effort to continue that tradition.

Senator Heller.

STATEMENT OF HON. DEAN HELLER, A UNITED STATES SENATOR FROM THE STATE OF NEVADA

Senator HELLER. Thank you, Mr. Chairman, and to Senator Flake, I am pleased to be here today. I would also like to thank you for inviting me to testify. I want to thank you for holding this hearing, and, Mr. Chairman, I want to thank you for your leadership that you have brought to the table on transparency to the bulk collection programs run by the NSA.

This is a strong bill rooted in the belief that Nevadans, Minnesotans, and all Americans should be provided access to reports that explain the personal communication records that the Government is collecting and how many Americans have had their information caught up in that collection.

By now most people are aware of the bulk collection practices by the Federal Government that are authorized by sections of the PATRIOT Act and sections of the FISA Amendments Act. I am confident the full Judiciary Committee will have a robust debate on the bulk collection practices and whether or not this program should continue. I believe that the bulk collection program mostly authorized under Section 215 of the PATRIOT Act should come to an end.

Subsequently I agreed to join with Judiciary Chairman Leahy as a principal sponsor with Senator Lee and Senator Durbin on the USA Freedom Act. While there is disagreement on whether this program should continue, I am confident all of us can agree that these programs deserve more transparency. This is why I joined Senator Franken to introduce the Surveillance Transparency Act of 2013.

This legislation would call for reports from the Attorney General detailing the requests for information authorized under the PATRIOT Act and the FISA Amendments Act. The reports would detail the total number of people whose information has been collected under these programs, how many Americans have had their information collected, and also how many Americans actually had their information looked at by the NSA.

Furthermore, this legislation would allow telephone and Internet companies to tell consumers basic information regarding the FISA Court orders they receive and the number of users whose information is turned over. The principles outlined in this bill to increase transparency for Americans and private companies would clear up a tremendous amount of confusion that exists with these programs. That is why transparency reform is included in multiple NSA reform proposals, including the Intelligence Oversight and Surveillance Reform Act introduced by Senator Wyden, the USA Freedom Act introduced by Chairman Leahy and myself, and the FISA Improvement Act introduced by Senator Feinstein.

Mr. Chairman, while positions on the bulk collection program may differ, many of us agree on the need for more transparency. That is why I urge support for the Franken-Heller legislation before this Subcommittee today. We are talking about millions of Americans' calls that are collected and stored by the NSA. Americans should have access to some basic information regarding the amount of data collected and what is actually being analyzed so that my constituents, your constituents, can determine for themselves whether they believe this program is worthy to continue or not.

And with that, again, thank you for the opportunity to have me testify, Mr. Chairman. I want to repeat thank you very much for your leadership on this issue.

Thank you.

Chairman FRANKEN. Thank you for yours, Senator Heller. I am looking forward to working together with you on this as we go through this process. You are excused, and your panel is adjourned.

Chairman FRANKEN. I would now like to introduce our second panel of witnesses.

Robert Litt is the General Counsel of the Office of the Director of National Intelligence. He was confirmed by the Senate by unani-

mous consent in 2009. Before joining the ODNI, Mr. Litt was a partner with the law firm of Arnold & Porter. From 1994 to 1999, Mr. Litt worked in the Department of Justice where he served as Deputy Assistant Attorney General in the Criminal Division and then as Principal Associate Deputy Attorney General.

Brad Wiegmann is a Deputy Assistant Attorney General for National Security at the Department of Justice. He has served as a career government attorney for the past 17 years, including positions at the State Department, the Department of Defense, and the National Security Council. His government service has focused on national security and international law, including counterterrorism, intelligence activities, and counterproliferation.

Welcome, gentlemen. ODNI and DOJ have submitted joint written testimony, which will be made part of the record. You each have 5 minutes for any opening remarks that you would like to make. Mr. Litt, would you begin?

STATEMENT OF HON. ROBERT S. LITT, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, AND J. BRADFORD WIEGMANN, DEPUTY ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION, DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. LITT. Thank you. Mr. Chairman, Ranking Member Flake, Senator Blumenthal, thank you for the opportunity to appear before you today to discuss this very important issue of how best to inform the public about sensitive intelligence activities consistent with the needs of national security. And I want to say that I appreciate the support that you have shown for the intelligence community over the last few months in their activities.

The recent unauthorized disclosures have led to a public dialogue about intelligence collection activities, particularly those conducted under the Foreign Intelligence Surveillance Act. But it is critical to ensure that that public dialogue is grounded in fact rather than in misconceptions. And, therefore, we agree that it is important to help the public understand how the intelligence community uses the legal authorities that Congress has provided it to gather foreign intelligence and the vigorous oversight of those activities to ensure that they comply with the law.

As you know, some months ago the President directed the intelligence community to make as much information as possible about certain intelligence programs that were the subject of those unauthorized disclosures available to the public, consistent with the need to protect national security and sensitive sources and methods. Since then, the Director of National Intelligence has declassified and released thousands of pages of documents about these programs, and we are continuing to review documents to release more of them.

These documents demonstrate that these programs are all authorized by law and subject to vigorous oversight by all three branches of government. And it is important to emphasize that this information was properly classified. It is being declassified now only because in the present circumstances the public interest in declassification outweighs the national security concerns that require

classification. But we still have to take those national security concerns into account.

In addition to declassifying documents, we have also taken significant steps to allow the public to know the extent to which we use the authorities under FISA, and I agree with both you and Senator Heller that it is appropriate to find ways to inform the public about this consistent with national security.

Specifically, as we set out in more detail in our written statement for the record, the Government is going to release on an annual basis the total number of orders issued under various FISA authorities and the total number of targets affected by those orders.

Moreover, recognizing that it is important for the companies to be able to reassure their customers about how often or, more precisely, how rarely the companies actually provide information about their customers to the Government, we have agreed to allow them to report the total number of law enforcement and national security legal demands they receive each year and the number of accounts affected by those orders.

We believe that this approach strikes the proper balance between providing the public information about the use of the legal authorities and protecting our important intelligence capabilities, and I would be glad to discuss that with you in more detail as we move ahead.

Turning to the Surveillance Transparency Act of 2013, which you and Senator Heller have cosponsored, we have reviewed the bill and we share the goal of providing the public greater insight into the Government's use of FISA authorities. And we appreciate the effort that you have made in this bill to try to accommodate transparency and national security. We have had good discussions with your staff about that bill.

Many of the bill's provisions are consistent with the steps we have taken so far, and we support them. But we do continue to have concerns that some of the provisions raise significant operational or practical problems. These concerns are set out in more detail in the written statement for the record, and I will just summarize now that they fall into two broad categories.

First, while we believe that it is possible and appropriate to reveal information about the number of targets of surveillance, counting the number of persons or of U.S. persons whose communications are actually collected, even if they are not the target, is operationally very difficult, at least without an extraordinary investment of resources, and maybe not even then.

For example, it is often not possible to determine whether a person who receives an e-mail is a U.S. person. The e-mail address says nothing about the citizenship or nationality of that person. And even in cases where we would be able to get the information that would allow us to make the determination of whether someone is a U.S. person, doing the research and collecting that information would perversely require a greater invasion of that person's privacy than would otherwise occur.

It is for these reasons that the Inspectors General of the National Security Agency and of the intelligence community have

stated in letters to the Congress that this kind of information simply cannot be reasonably obtained.

Second, we have significant concerns with allowing individual companies to report information about the number of orders to produce data that they receive under particular provisions of the law. Providing that information in that level of detail could provide our adversaries a detailed roadmap of which providers and which platforms to avoid in order to escape surveillance. We believe that the reporting we have already agreed to provides the right balance between transparency and national security.

Mr. Chairman, I want to emphasize our intention to work with the Congress and with this Committee to ensure the maximum possible transparency about our intelligence activities that is consistent with national security. The President is committed to this. The Director of National Intelligence is committed to this. The Attorney General is committed to this. General Alexander is committed to this. We are open to considering any proposals so long as they do not compromise our ability to collect the information we need to protect this Nation and our allies, and we look forward to working with you in this regard.

Thank you.

Chairman FRANKEN. Thank you, Mr. Litt.

Mr. Wiegmann.

Mr. WIEGMANN. Thank you, Mr. Chairman. Thank you for having me here today. I do not want to replicate what Bob Litt has just explained, so I do not want to waste the Committee's time, but we at the Department of Justice very much agree with what Bob has just explained. We very much support the transparency efforts that the intelligence community is engaged in now. We also, as Bob said, share the goals of the bill that you have prepared in terms of increasing transparency, but we have some technical concerns about how those proposals can be implemented that we are happy to discuss today.

I guess I would just say a couple of other things. One is that I think this is an area where the details very much matter. We are very much in support of transparency, but we want to do so in a way that is consistent with our national security needs. You have seen a number of documents declassified over the last several months, and I am sure from the outside it looks very slow and ad hoc, as you said earlier. That is because these documents involve a lot of detailed classified information, and it takes a lot of time to go through the documents and determine what can safely be revealed and what cannot, and there are a lot of equities of different components of the intelligence community that have a stake in the information in play. So our transparency efforts are a work in progress. We continue to work on them as we go forward, but we are trying to do so in a careful and deliberate way. But I do not doubt that to the outsider it looks as if it is slow and ad hoc, but that is because we are trying to protect national security while also promoting transparency goals.

So, with that, I guess I will just—the other thing I guess I would say in addition, though, is to contrast the U.S. response to these disclosures to those of some foreign governments. We have, in response to these unauthorized disclosures, tried to be more trans-

parent, and that has not always been the case with other governments that have experienced this, either in the past or more recently. So I do think we are working in good faith to try to be more open about our intelligence collection activities, and we are happy to work with the Committee to continue to promote that goal.

That is all I have.

[The prepared statement of Messrs. Litt and Wiegmann appears as a submission for the record.]

Chairman FRANKEN. Thank you, Mr. Wiegmann, and thank you both. As I said, you submitted joint testimony, and, of course, that will be part of the record. I appreciate your not taking every minute of your time here.

I will say about the disclosures—that I have said that these have been, I think, in good faith. It is just that there is nothing in the law about them, so there is nothing permanent about what you are doing, and what we are trying to do is create a framework where people have a little bit more confidence or understanding or can decide for themselves whether they should have confidence.

Mr. Litt, you indicated that ODNI may lack the technical ability to estimate the number of U.S. citizens and permanent residents whose information has been collected under the different surveillance authorities. I find this kind of troubling, and here is why.

We give the intelligence community broad legal power to conduct surveillance precisely because that surveillance is supposed to be targeted at foreign adversaries, not at Americans. Many of the broadest laws we have written, like Section 702 of FISA, explicitly say that you can only use this law only to target foreign people. You cannot use it to target U.S. persons.

Mr. Litt, isn't it a bad thing that NSA does not even have a rough sense of how many Americans have had their information collected under a law, Section 702, that explicitly prohibits targeting Americans?

Mr. LITT. So I have to preface everything here by emphasizing that I am a lawyer, not an engineer or a computer scientist, and so everything I say here gets filtered through that prism. But——

Chairman FRANKEN. Well, if you were an engineer or a computer scientist, we would have you working on something else.

[Laughter.]

Mr. LITT. But I think it is important to differentiate here between the concept of who is targeted for collection and whose communications are incidentally collected.

Because of the legal requirement, for example, under Section 702 that NSA only target non-U.S. persons, NSA does the research necessary when they have a target to determine whether that person is or is not a U.S. person. They need to be able to make that determination.

That is a very, very different process from saying we are going to look at all of the communications that are collected, and we are going to evaluate every single party to every one of those communications to determine whether or not that is a U.S. person.

So they do have the ability to try to make the determination as to whether somebody is or is not a U.S. person for the purpose of targeting that person, but that is a different proposition.

Chairman FRANKEN. Okay. Well, I think an estimate, though, could be made through statistical sampling, a method that has been used in comparable circumstances before the FISA Court. I would like to add to the record two pieces of testimony that to me suggest that the NSA could be able to estimate how many Americans have had their information collected under foreign intelligence authorities. The first is from General Alexander. He testified in September that the NSA employs over a thousand mathematicians, more than any other employer in the United States, more than every university in Minnesota, more than MIT or CalTech.

The second piece of testimony is from Ed Felten, the Princeton professor and the former technologist for the Federal Trade Commission. He said, "Yes, the Government has the ability to give a rough estimate of the number of American citizens and permanent residents whose metadata and content has been collected."

[The statements appear as a submission for the record.]

Chairman FRANKEN. Let us move on to the disclosure by the companies. Mr. Litt, in your testimony you warn that, quoting from your testimony, "More detailed company-by-company disclosure threatens harm to national security by providing a roadmap for our adversaries on the Government's surveillance capabilities . . ." This concern makes sense. But I have difficulty reconciling your testimony with the Government's actions with respect to major companies like Google. The Government lets Google publish the number of national security letters it receives each year and the number of users affected. And 2 months ago, Michael Hayden, the former Director of NSA and of CIA, gave a speech in which he said, "Gmail is the preferred Internet service provider of terrorists worldwide." That is a verbatim quote, according to the *Washington Post*.

Mr. Litt, it seems to me that if the former head of the CIA and the NSA does not think it is a problem to let everyone know that terrorists just love Gmail, then why do you think that a company-by-company disclosure threatens national security? He evidently does not.

Mr. LITT. A couple of thoughts on that. To my knowledge, General Hayden did not talk to us before making those statements. I do not know that we would have authorized that statement to be made. I just do not know what was done there.

The point is that if we allow the companies on an annual basis to publish these statistics, it is going to simply provide additional information out there as new companies come online and pop up. You may have a company that, for example, for a period of years shows no orders and then all of a sudden starts showing orders, and that conveys a message that says we have got the capability to collect this now.

The more detail we provide out there and the more we break this down by authorities and companies, the easier it becomes for our adversaries to know where to talk and where not to talk.

What we have agreed to allow the companies to do is to report the aggregate number of times in which they provide information about their customers to the Government. And that, it seems to me, is an adequate way of providing the public the information they need to know about the minuscule proportion of times in

which that actually happens. And breaking it down further in our view crosses the line of the appropriate balance between transparency and national security.

Chairman FRANKEN. We are going to have testimony from some privacy people and from Google talk about that aggregation. I do not think that aggregation is all that helpful because you really are not giving people an idea of how much is—I mean, you are mixing apples and oranges, so you are having how many wiretaps there are on mobsters with—I mean, to me it does not create the kind of transparency that creates the kind of knowledge the American people—I have some time—gives the American people a way to judge the program.

Let me ask Mr. Wiegmann something. I am the Chairman. I guess I can go over my own times, but I have got 9 seconds, and I will try to ask a question. Mr. Wiegmann, I understand that you think that my bill would require too much detail in government reporting. I am going to weigh that feedback very carefully. But I do want to point out that when I drafted the government reporting requirements in the bill, I modeled them after the wiretap report that the Department of Justice releases every year.

If you look at last year's report, it breaks down the number of wiretaps not just nationally but by specific jurisdiction and then breaks down those numbers by the nature of the wiretap—a mobile phone, a home phone, a business phone. Last year's wiretap report shows that federal prosecutors in Manhattan secured wiretap orders for mobile phones 48 times in 2012, while their colleagues in Brooklyn only did this 5 times in the same period.

The wiretap report contains a wealth of information, yet nobody is arguing that criminals in Manhattan are reading the wiretap report and fleeing to Brooklyn because, you know, they are less likely to get their phone tapped there.

My bill would not even require anything near this level of reporting. It would require the Government to report national statistics, and any time the number of Americans affected was lower than 500, the report would just say "fewer than 500."

Mr. Wiegmann, why would the reporting requirements in my bill raise national security concerns if the far more detailed reporting requirements in DOJ's wiretap reports do not raise public safety concerns?

Mr. WIEGMANN. So that is a good question. The regular wiretaps under the Wiretap Act do not involve classified techniques, so there are platforms that we use in the intelligence context that it is unknown to the outsiders or anyone outside the executive branch as to whether we can collect on a particular communications technology. So the difference——

Chairman FRANKEN. But I am not having you——

Mr. WIEGMANN. What is that?

Chairman FRANKEN. The disclosure would not be talking about a technology other than it is on the Internet or phone.

Mr. WIEGMANN. Right.

Chairman FRANKEN. We know those technologies.

Mr. WIEGMANN. We think that our adversaries can surmise—let us say, for example, in year one we know that there is a company that has a particular number of surveillance requests and that

number is published. They then introduce a new capability, a new service that they provide, and then all of a sudden that number goes up dramatically in the following year. That is something that our adversaries could glean information from that and surmise as to whether we have the capability to collect on a new technology. So that is the type of thing that I am talking about that is different than in the wiretap context where everyone knows that a basic phone tap is something that you can do. So that is the difference there.

I would also like to address briefly your last question to Mr. Litt about NSLs. The reason why NSLs are different than other collection methods, is that it is just collecting business records. It is not an interception capability. You are not intercepting communications in real time. You are just collecting business records that the companies have, and so that is the distinction there that we do not have the same concerns about revealing those numbers in aggregate that we would with intercept capabilities.

Chairman FRANKEN. Well, thank you. I thank the Ranking Member for his indulgence. I have gone way over my time. I thank you too, but please continue.

Senator FLAKE. Well, thank you. They have been useful questions and some of the same questions that I had as well.

Mr. Litt, if you could kind of drill down a bit in terms of increased manpower and what it would take to actually make some determination of the percentage of individuals who are U.S. citizens who are surveilled, what would that look like, without revealing more than you need to reveal here? What would that take to actually go through and determine what percentage?

Mr. LITT. So I can offer actually an example in that regard. The Chairman made reference to the FISA Court opinion that we have released from 2011, which involved a compliance violation under the collection under Section 702. And in connection with that, NSA did do a statistical sample to try to determine how many wholly domestic communications may have been intercepted through one portion of this collection, and they did a statistical sample where they reviewed I think approximately 50,000 communications, which was a very small percentage of that.

My understanding is that it took a number of NSA analysts about 2 months to do that, and that even in that regard, there were a number of instances where they simply could not come up with the necessary information, that the actual information was in a wide—ended up with numbers in a wide range based on a lot of assumptions. And the last point I want to make on that is that that was actually an easier task than the one that is being asked here, because they were looking for wholly domestic communications, which means that anytime they found a communication where there was one non-U.S. person they could immediately throw it out and not look any further. So they never did actually go through and look at every single party to every single communication to determine whether or not it was a U.S. person.

So I think that that example gives a sense of the resource intensiveness that would be required and the difficulty, even if you apply all those resources, in coming up with reliable numbers at the end of the process.

Senator FLAKE. So you maintain that it would take—it would probably lead a lot of resources away from the main task just to comply with this provision?

Mr. LITT. Yes, I think those thousand mathematicians have other things that they can be doing in protecting the Nation rather than trying to go through and count U.S. persons.

Senator FLAKE. In your testimony you mention that it may have a greater impact on privacy to actually have to drill down and determine who is a U.S. person and who is not. What level of detail do you typically have to have? You have to run—I guess search what other communications have come to this person or whatever else, and those are the things that—can you kind of explain what you mean by saying that you impact more on people's privacy by drilling down and complying with this law than are currently out there?

Mr. LITT. Yes, that is exactly right. NSA's mission is to collect foreign intelligence. They are looking for the foreign side of the thing, and it is not what they ordinarily do to go out and try to find U.S. persons. And so if you impose upon them some sort of obligation to identify U.S. persons, they are going to take an e-mail address that may be, you know, Joe@hotmail.com, and they are going to have to dig down and say, "What else can we find out about Joe@hotmail.com?" And that is going to require learning more about that person than NSA otherwise would learn.

Senator FLAKE. Mr. Wiegmann, we allowed the companies out there, Google and others, to reveal more than they were able to reveal before. Google has procedures that they follow. What other companies have taken advantage of the opportunity they have to reveal more information about what is surveilled and what is not? Is it universal, all of them are taking advantage of this, or some of them, or what?

Mr. WIEGMANN. I would have to get back to you and give you the list of companies. I believe Microsoft has issued a Transparency Report with certain data, Facebook I believe. I would have to get you the complete list. I do not want to give you the wrong list of companies here, but I could get you the information about which ones have taken advantage of the Government's offer thus far.

Senator FLAKE. All right.

I am sure we will learn more in the next panel, but is it your understanding that all—how universal is the request for the ability to give broader information or more information about what is being surveilled and what is being collected, whatever else?

Mr. WIEGMANN. I think it is fair to say that a lot of the major Internet service providers do want to provide more information about how their users are affected by government surveillance. A number of them in the initial stages of this in the wake of the initial Snowden unauthorized disclosures came to us, and so we work with them on the proposal that Bob described, which was that we would release the aggregate number of law enforcement plus national security demands in the aggregate for those companies. I think they found that useful at the time because they put out press statements and so forth saying—you know, identifying those numbers and showing that that was a tiny fraction, I think in most cases less than one ten-thousandth or one one-hundred thou-

sandths of their user base was affected by not only the national security demands but also the law enforcement demands together. So whether you slice out the national security or whether you include the law enforcement, it is a tiny, tiny fraction of their total user accounts, and that is what they wanted to be able to show, as Senator Franken was saying, to debunk the idea that we are engaged in some kind of dragnet surveillance whereby we are getting access to all of their users. In fact, the opposite is true, that it is a tiny, tiny number. And they were able to do that with the disclosures that we authorized at that time.

Senator FLAKE. Thank you.

Mr. Litt, getting back to what we were talking about before, in order to comply with the provisions of this legislation, would you sometimes require more of the companies in terms of trying to follow down and drill down on how many U.S. persons were affected here? Might there be additional concerns from the private providers that were—I do not know. Might they be more uncomfortable with additional requests to try to determine—we already have minimization procedures that apply in order to exclude U.S. persons, but this would seem to be a lot more drilling down, as you mentioned before. What concerns do others have about this? And should they be concerned about more intrusiveness on the part of the Government to determine who is a U.S. person and who is not just for the purpose of complying with the Act?

Mr. LITT. Well, I do think that people should be concerned about the greater intrusiveness. I am not sure technically whether it would require any more of the companies or not. I think that more likely NSA would simply rely on its own internal resources rather than—because they would need some additional authority to go back to the companies to get subscriber information or whatever. So I am not sure that it would impose an additional burden on the companies, which does not in any way mitigate the intrusion on the individual.

Senator FLAKE. But you do not anticipate having to go back to the companies and say we would need additional information in order to determine—or to comply with the law?

Mr. LITT. I would not say that I do not anticipate it, but I am not sure that it would happen or that, frankly, there would be a way we could do it legally to get that information from the companies.

Senator FLAKE. Thank you, Mr. Chairman.

Chairman FRANKEN. Thank you. And I will say that we are going to have testimony from Google, and they have signed on to this, as have those companies. So we will hear from them.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman. Thank you for your leadership on this bill. Thank you to our Ranking Member and to Senator Heller. I am a cosponsor of this measure and really want to express my gratitude to you, Senator Franken, for spearheading this effort. But, of course, it really embodies the general truth that what you do not know can hurt you. And what the American people do not know about much of what you do, and it is important, indeed essential work to our national security, can create misinformation and deception and undermine the trust and

credibility in the entire program of surveillance and intelligence vital to national security. So what the American people do not know can hurt them if it becomes a source of mistrust and loss of credibility here and around the world.

So I think that this bill is very important, albeit only a first step, and I propose other measures such as a constitutional advocate that I think fits with the concept of this bill in terms of preserving an adversarial and accountability measure, as well as greater transparency and accountability in other ways.

I would like to focus on the technical issues that you have raised. Don't these pale compared to the importance of the objective? And aren't they surmountable with relatively few resources if we define narrowly what those technical problems are?

Mr. LITT. Well, taking—I mean, I guess I would say no and no. Taking your second point first, the judgment of people who have looked at this, not only people within NSA but, as I said, two Inspectors General who have also looked at it, is that this is not surmountable with a relatively modest application of resources, that it would be very resource intensive, and as I said, particularly with respect to U.S. persons, very—require additional intrusions on privacy.

Our judgment is that this is not the best way to try to strike the balance between privacy and national security. I understand the view that there is important information out there. But one of the necessities of conducting intelligence operations is that not all the information that might be of use to the public is going to come out in the public.

So I think that our view is that the steps that we have taken are appropriate ones, and we are prepared to work with the Committee and the Congress on additional steps that might be taken. But——

Senator BLUMENTHAL. But I do not understand—and forgive me for interrupting, but my time is limited. I do not understand what resource intensive—you know, that is a code word. It is a term of art maybe that is used to say it looks pretty difficult to do. It looks like it is going to cost a lot. How resource intensive really is it to accomplish these purposes?

Mr. LITT. I do not know that we have done an actual cost estimate. The only yardstick I can give you is what was required to do the smaller and easier task that was done in connection with the FISA Court opinion that required, I believe, a half dozen analysts 2 months to do and still come up with an estimate that had wide ranges in it. And so that——

Senator BLUMENTHAL. Maybe you can give us some idea of what those ranges are.

Mr. LITT. If you give me a second.

Chairman FRANKEN. This will not come out of the Senator's time.

Mr. LITT. It is a long opinion, and it is going to take me a second to find the right place.

[Pause.]

Mr. LITT. I am sorry. I should have marked this in advance.

So as I said, the issue was to determine what were wholly domestic communications, which I said is a different task, and as a result of this review, they determined that there were between 996—essentially between 1,000 and 5,000 communications that met

that test. So you have a fivefold range there, and there are other estimates in here, for example, that say, well, it would not be any greater than this number. But they are all based on assumptions and estimates, and I do not know that there is any comfort that we could accomplish this with any degree of reliability.

Senator BLUMENTHAL. But you have given me a number for the communications but not a number for the dollars. To put it perhaps oversimplistically, how do you measure resource intensive?

Mr. LITT. I mean, you have to look at the number of people who would be required and the amount of time that would be required.

Senator BLUMENTHAL. And can you give us some idea of what they would be?

Mr. LITT. As I said, the only metric that I have is what was required to get this number, and my understanding is that that was, I believe, six analysts for a 2-month period. You would have to multiply that across a much larger sample, a much more difficult task, and additional FISA authorities. So you are talking, you know, some number of man-years that would be required to do this.

Senator BLUMENTHAL. Thank you. Let me just move on. In the interest of perhaps anticipating the testimony we are going to receive from the next panel, I do not know whether you have had a chance to review that testimony, but, for example, a lot of it concerns the impact on communications internationally, and I wonder if you could comment in particular on the testimony, very compelling testimony, from Mr. Salgado about the need for transparency to enable the trust and credibility that is important for communications worldwide?

Mr. LITT. So I have not had a chance to review the other testimony. I am generally familiar with the companies' position. I think we have a lot of sympathy for their position. The unauthorized disclosures that have come out here have put them in a difficult position. It is one of the many things that we regret about these disclosures.

Having said that, as Brad mentioned earlier, we are authorizing—we are prepared to authorize the companies to release the total number of orders they get and to disclose customer information and the total number of accounts affected by those orders. That is going to be a minuscule number. As Brad said, it is something like—you know, it is a fraction of 1 percent, and that covers all authorities. And it seems to me that that minuscule number is sufficient to meet the company's needs, and it really does not advance things anyway—when they are allowed to disclose that 0.0001 percent of their customer accounts are affected by orders to provide information to the Government, it does not really advance their needs to say, well, 0.000001 percent of those were pursuant to this authority and 0.000003 percent were pursuant to that authority. The relevant statistic is that any customer of Google or of any other company, there is only an infinitesimal likelihood that that person's information is ever going to be asked for by the Government.

Senator BLUMENTHAL. Thank you. My time has expired. Thank you very much.

Thanks, Mr. Chairman.

Chairman FRANKEN. Thank you, Senator Blumenthal, and I am a cosponsor of your constitutional advocate bill.

Senator BLUMENTHAL. Right. Thank you.

Chairman FRANKEN. Senator Lee.

Senator LEE. Thank you, Mr. Chairman. Thanks to you for being here with us today.

Much of the testimony that we have received today highlights the consequences of unchecked government intrusion into the private lives of citizens and their interactions with private businesses.

Senator Franken's bill would take important steps to increase the transparency of government requests for information, and I very much applaud those efforts. In fact, Senator Leahy and I have incorporated the vast majority of Senator Franken's provisions into our bill, S. 1215, the FISA Accountability, Privacy, and Protection Act, which makes broader reforms to the privacy protections within the FISA program.

Our bill would tighten statutory authorities governing surveillance, would increase oversight and accountability, and would ensure that Americans' constitutional rights under the Fourth Amendment are protected.

The reporting provisions in these bills guarantee that we have an accurate understanding of the scope of these information collection activities and allow businesses to regain the trust of the public through the reasonable disclosure of their interactions with government agencies as they provide information. It is time we started requiring a little more sunlight in this fairly shadowy space.

Mr. Litt, in your written testimony, you expressed support for the majority of the disclosure requirements in this bill. I was wondering, is your support a direct result of formerly covert collection programs having become public? Or do you think that nationwide aggregate disclosures are inherently beneficial and should be sought out?

Mr. LITT. I think the answer to that is that aggregate disclosures are a good thing, provided they do not compromise our ability to collect important information. I think in the situation we are in right now, whatever the appropriate result might have been 6 months ago, in the situation we are in right now where the Director of National Intelligence has already declassified the fact of certain programs and how they operate, that it is entirely appropriate to have aggregate disclosures of these activities going forward.

For other important intelligence activities, I am not sure that we would reach the same balance, but to the extent that we are talking about these particular disclosures, we believe that they do strike the right balance now.

If I could just for one thing—I know this is perhaps not considered a discreet thing to do. I do want to take issue with your suggestion that we are talking about unchecked intrusions into the privacy of Americans, because, in fact, they are very checked. We operate within the laws authorized by Congress. We operate with extensive oversight from all three branches of government, and they are highly regulated and highly checked. Whether or not they are appropriate or not I think is a valid question, but nobody should be under the illusion that we are operating without any checks on what we do.

Senator LEE. That is a fair point, and I understand your position there. One of the concerns is always, of course, that what might well be handled by responsible people today, tomorrow might not be. We do not know whether that might happen a week from now or a year from now or 10 years from now, but in a sense, we have seen this movie before and we know how it ends. If you give too much power to the Government with regard to domestic surveillance, eventually it will be abused, and we need to put in place whatever procedures might be necessary.

If I understand your answer to my question correctly, part of what you are saying is that prior to the declassification that occurred recently, this might have run afoul of—this might have triggered your concerns, this kind of legislation might have triggered your concerns in the sense that it might have compromised ongoing activities. But since those have now been declassified, there is no reason not to do this. Am I understanding you correctly?

Mr. LITT. Yes, I think that is right.

Senator LEE. Okay. Thank you, sir, and thank you, Mr. Chairman.

Chairman FRANKEN. Thank you, Senator.

I want to thank you gentlemen not just for your testimony but for your service. You made a good point there about there are checks to what you do, and this is part of it. And you made a comment that there are checks on what you do, but that does not mean what you do is always appropriate. And that is what we are trying to get to here.

You have made some disclosures that I think have been in good faith, but they are not permanent. They are not a part of the law. And so that is what we are discussing here. And, again, I want to thank both of you for your testimony, and now I want to call our third panel. So thank you both, gentlemen.

Mr. LITT. Thank you, Mr. Chairman.

Mr. WIEGMANN. Thank you.

Chairman FRANKEN. Kevin Bankston is senior counsel and director of the Free Expression Project at the Center for Democracy and Technology. Mr. Bankston is a long-time advocate and litigator on privacy, civil liberties, and Internet policy matters. Mr. Bankston and the Center for Democracy and Technology organized and led the coalition of companies and civil liberties groups that called for greater transparency and that now is advocating the passage of this bill.

Paul Rosenzweig is the founder of Red Branch Consulting, a national security consulting company, and a senior adviser to the Chertoff Group. From 2005 to 2009, he served as Deputy Assistant Secretary for Policy in the Department of Homeland Security. He also teaches at George Washington University Law School.

Richard Salgado is Google's director for information security and law enforcement matters. He served as a federal prosecutor in the Computer Crime and Intellectual Property Section of the Department of Justice, where he specialized in technology-related privacy crimes. He has taught at Stanford Law School, Georgetown University Law Center, and George Mason University Law School.

Thank you all for joining us. Your complete written testimony will be made part of the record. You each have 5 minutes, about 5 minutes, for any opening remarks that you would like to make.

Mr. Bankston, please go ahead.

STATEMENT OF KEVIN S. BANKSTON, SENIOR COUNSEL AND DIRECTOR, FREE EXPRESSION PROJECT, CENTER FOR DEMOCRACY & TECHNOLOGY, WASHINGTON, DC

Mr. BANKSTON. Chairman Franken, Ranking Member Flake, and members of the Subcommittee, thank you for the opportunity to testify on behalf of the Center for Democracy & Technology, a nonprofit, public interest organization dedicated to keeping the Internet open, innovative, and free.

I and the broad coalition of Internet companies and advocates that CDT brought together this summer to press for greater surveillance transparency are grateful to Chairman Franken and Senator Heller for introducing the Surveillance Transparency Act, a bill that would allow companies and require the Government to publish basic statistics about how the Government is using its national security surveillance authorities.

Particularly in the wake of recent revelations about the NSA's surveillance programs, we believe this level of transparency about what companies do—and don't do—in response to government demands is critically important for three reasons.

First, the American people and policymakers have a clear right and need to know this information so that they may have a more informed public debate about the appropriateness of the Government's use of its authorities and to better ensure that those authorities are not misused or abused.

Second, the companies have a clear First Amendment right to tell us this information, and the Government's attempt to gag them from sharing even this most basic data or even to admit that they have received foreign intelligence demands at all is clearly unconstitutional. Indeed, you will see this prior restraint at work today in the room. Even though everyone in this room knows and understands that Google has received Foreign Intelligence Surveillance Act process, Google's representative is the one person in the room who cannot admit it.

Third, greater transparency is urgently necessary to restore the international community's trust in the U.S. Government and in our U.S. Internet industry, which is projected to lose tens, if not hundreds, of billions of dollars in the face of widespread concern from foreign governments and international users.

We must take this opportunity to demonstrate that our surveillance practices are necessary and proportionate and respectful of constitutional and human rights. And if the numbers show otherwise, we must take this opportunity to reform our surveillance laws to better protect our rights as well as our national security.

Speaking of national security, there are two basic arguments why publishing these numbers would threaten it, but neither is persuasive.

First, there is concern that such reporting will reveal which services have not been targeted by the U.S. Government such that our enemies will seek them out. However, it has always been the case

that companies that have not yet received secret national security demands can say that they have not received secret national security demands, as was most recently demonstrated just last week when Apple revealed that it has never received an order under Section 215 of the PATRIOT Act.

The second argument is that reporting will reveal which services have been targeted such that their enemies will avoid them. However, this concern rings somewhat hollow when top intelligence officials such as current NSA Director Keith Alexander have repeatedly and publicly announced the names of various services, such as Google, Facebook, Twitter, and Yahoo!, that they believe terrorists are using. Senator Franken also mentioned a comment by former NSA Director Michael Hayden.

Put simply, and as these generals recognized, saying that someone on a service is being surveilled is very different from identifying who on that service is being surveilled, and only the latter is dangerous to national security. Therefore, the less transparent alternatives to the bill that the Government has suggested are unnecessary to protect national security. More than that, they would actually be worse than the current transparency status quo.

On the Government reporting side, the DNI has announced he will voluntarily publish new statistics reflecting how many people have been "targeted" under various surveillance authorities. But such limited reporting would actually be misleading.

For example, the DNI's reporting for 2012 would only have indicated that around 300 people had their telephony metadata targeted under Section 215 of the PATRIOT Act, yet we now know that the Government has used Section 215 to obtain the phone records of every single person in the country. Such falsely reassuring reporting would do more harm than good.

On the company reporting side, the government advocates for a lot of what I will call "fuzzing" and "lumping." They want to lump together into a single number all the different foreign intelligence authorities as well as all State, local, and federal law enforcement requests and then fuzz that number up by putting it into a range of a thousand. That kind of fuzzing and lumping would be a step back for transparency, obscuring more than it reveals, especially considering that companies are already engaged in detailed reporting about the law enforcement process they receive and in some cases have also been allowed to publish separate rounded numbers about the national security letters they receive.

No one has ever suggested that either that reporting or the detailed reporting that the Government has done for decades about its law enforcement wiretapping has ever disrupted an investigation. Neither would the reporting required and allowed for under this bill or that provided by the transparency provisions of the USA Freedom Act, another bill that CDT strongly supports.

Greater transparency is no replacement for substantive reform of our surveillance laws, but it can serve as a key stepping stone toward that broader reform by allowing the public and policymakers to better understand how the Government is using its powers.

So I thank you for your consideration, and I look forward to your questions.

[The prepared statement of Mr. Bankston appears as a submission for the record.]

Chairman FRANKEN. Thank you, Mr. Bankston.

Mr. Rosenzweig.

STATEMENT OF PAUL ROSENZWEIG, PRINCIPAL, RED BRANCH CONSULTING, PLLC, AND PROFESSORIAL LECTURER IN LAW, GEORGE WASHINGTON UNIVERSITY, WASHINGTON, DC

Mr. ROSENZWEIG. Senator Franken, Senator Flake, members of the Subcommittee, I thank you very much for the invitation to appear today. It is always an honor to be asked to provide one's views to the Senate of the United States, and I thank you for affording me that opportunity.

I should begin by saying that, as a current holder of a top secret clearance for some of the work I continue to do for DHS, I have limited what I have read to what has been lawfully declassified by the DNI, as have most of the people in my position, which somewhat constrains how I can speak to the issues today. That having been said, I would make four basic points.

The first is that transparency is a good thing, but unlimited transparency cannot be our end goal. Secrecy itself has its virtues in any number of circumstances. One can think of everything ranging from the attorney-client privilege to the identity of an undercover officer in a gang in Los Angeles to any number of reasons why governments legitimately keep secrets that are subject to oversight in a classified manner, either through the oversight of the executive branch or the legislative branch or in some cases the judicial branch.

Thus, while I fully support the overarching sentiment that underlies much of the bill that is before you, that is, the idea that we can and should seek to increase transparency with respect to the NSA surveillance programs, I think that we have to do so in a calibrated way, one that takes into account what the end goal of transparency in this circumstance is.

Now, I would submit that the end goal here is greater oversight, greater audit, greater assurance that the NSA and other intelligence community activities are acting in conformance with the laws as we have set them out and not in ways that are in violation of those laws. So to my mind, the right answer to many of the questions that you are asking is how will the transparency that you are advocating advance that goal.

With that in mind, my second point is that I think that the proper reflection on what we should be learning more about with respect to the NSA surveillance is to require a lot of disclosure of aggregate information, a lot of disclosure with respect to existing programs, but that we should take very seriously the protestations of government officials who are, frankly, in a better position to know than I am at least, given what little I know about the classified nature of these programs, that further disclosures will disclose sources, methods, capabilities that have not yet publicly been disclosed.

Indeed, my single greatest constructive criticism that I would offer with respect to the bill before you is the idea that the disclosure requirements are keyed to statutory programs themselves like

Section 215 or Section 702 and seems to operate from the unstated assumption that we have already learned all of the classified programs that are operating under those statutes.

If that is the case, then the transparency that is key to those sections is to be welcomed indeed. I suspect, without knowing, that there are other programs involved, other covert programs that have not yet been disclosed, either lawfully or unlawfully, and it is at least plausible to me that further disclosures of particularized numbers would lead to the disclosure of programs that have not yet made it into the public record. If that were the case, I would think that that would be an unfortunate result.

My third point would simply be that the most effective reforms, I think, are not just enhanced transparency for the American public but more structural reforms, things that you can do that are not part of this bill, that are part of, I think, what Congress can do, things like making the NSA Inspector General a Presidential appointment, expanding the jurisdiction of the Privacy and Civil Liberties Oversight Board. Those sorts of things do not sound as sexy as greater transparency, but I tend to think that in the end they will actually prove more effective than even the most detailed disclosure of individuated numbers within various programs.

With that, I will conclude, and I look forward to your questions.

[The prepared statement of Mr. Rosenzweig appears as a submission for the record.]

Chairman FRANKEN. Thank you, Mr. Rosenzweig.

Mr. Salgado.

STATEMENT OF RICHARD SALGADO, DIRECTOR, LAW ENFORCEMENT AND INFORMATION SECURITY MATTERS, GOOGLE, INC., MOUNTAIN VIEW, CALIFORNIA

Mr. SALGADO. Chairman Franken, Ranking Member Flake, Senator Blumenthal, and Senator Lee, thank you for the opportunity to appear before you this morning to talk about the Surveillance Transparency Act of 2013. My name is Richard Salgado. I am the director for law enforcement and information security at Google. In that capacity I oversee the company's response to government requests for user information under various authorities. I am also responsible for working with teams across Google to protect the security of our networks and our user data.

Mr. Chairman, we commend you for introducing the Surveillance Transparency Act of 2013. Simply stated, we believe that service providers should be able to disclose basic statistics about national security demands that we may receive.

The revelations about the U.S. Government's and other governments' surveillance practices over the past few months have sparked a serious debate about the laws governing surveillance of private communications by the intelligence community. Google recognizes the very real threats that the U.S. and other countries face today, and of course, governments have a duty to protect their citizens. But the current lack of transparency about the nature of government surveillance in democratic countries undermines the freedom and the trust most citizens cherish. It also has a negative impact on our economic growth and security and on the promise of the Internet as a platform for openness and free expression.

In the wake of press reports about the so-called PRISM program, governments around the world have been considering proposals that would limit the free flow of information. This could have severe unintended consequences, such as a reduction in data security, increased costs, decreased competitiveness, and harms to consumers.

Proposals like data localization pose a significant threat to the free and open Internet. If they are adopted, then what we will face is the effective creation of a "splinternet" broken up into smaller national and regional pieces with barriers around it to replace the global Internet that we know today. Enacting the Surveillance Transparency Act would allow the U.S. to take a first step toward rebuilding the trust that is necessary.

Transparency and national security are not mutually exclusive. Since 2010, we have published a Transparency Report where we share information about the law enforcement requests for user data we receive from governments around the world. Earlier this year, after some discussions with the Department of Justice, we began providing more information about the volume and scope of national security letters that we receive, although in broad ranges. There has been no intimation from the Department of Justice that publishing statistics concerning NSLs has damaged national security.

We approached the DOJ about expanding our reporting to include aggregated statistics about FISA requests that we may receive. We were disappointed that the Justice Department refused. In June, we filed a motion for declaratory judgment before the Foreign Intelligence Surveillance Court asserting a First Amendment right to publish this type of information. The DOJ repeated that it would allow companies to add the number of domestic law enforcement and national security requests together and report the sum as falling within some broad range. But this would be a significant step backward for Google's users and the broader public. Rather than promote transparency, this proposal would actually obscure important information about the volume and type of all government demands that Google may receive, not just national security demands.

As I mentioned, Google already discloses aggregate statistics about domestic law enforcement demands and has done so since 2010. Publishing future reports, where we could only release this type of information in ranges rather than actual numbers and type, would provide less transparency than we have now.

In addition, there would be no discernible benefit for transparency around national security demands that we may receive. Indeed, Google would continue to be prohibited from even acknowledging their receipt, which would only invite continued speculation about the import of the range that we are able to report. We would also lose the benefit of providing information specifically about national security letters that we currently enjoy. In short, the DOJ proposal would not provide the type of transparency that is reflected in the Transparency Surveillance Act of 2013.

Transparency is critical in informing the public debate on these issues, but it is only one step among many that are needed. Two weeks ago, Google, along with AOL, Apple, Facebook, LinkedIn, Microsoft, and Yahoo!, voiced support for broader FISA reform that

would include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms. We strongly believe that governments throughout the world must revisit laws and practices governing state surveillance of individuals and access to private communications. This activity must be rule-bound, narrowly tailored, transparent, and subject to oversight.

We look forward to working with the Congress on the Surveillance Transparency Act of 2013 and other reform measures. Thank you for your time and consideration.

[The prepared statement of Mr. Salgado appears as a submission for the record.]

Chairman FRANKEN. Thank you, gentlemen, for your testimony.

Mr. Bankston and Mr. Salgado, you heard witnesses from ODNI and DOJ say that it would be very difficult for the Government to provide an estimate of the number of U.S. persons caught up in surveillance. Do you agree with them?

Mr. BANKSTON. I prefer to talk about what the NSA should be able to do rather than getting into a debate over what they technically could do, although I have some opinions about that as well.

The authorities we are discussing today are foreign intelligence authorities. They are predominantly intended to and are sometimes limited to acquiring the communications of foreign persons or persons outside of the United States and have special protections for U.S. persons. Therefore, knowing how many U.S. persons have been surveilled, have been swept up intentionally or unintentionally under these powers is critical to understanding whether they are being used correctly, proportionately, and in line with constitutional and statutory limits. And the fact that the NSA is claiming that it does not have the ability to provide even a rough estimate as to how many U.S. persons have been swept up in their surveillance is, quite frankly, shocking and I think points to perhaps a need to recalibrate what we are authorizing them to do if they cannot even judge how their activities are impacting the American people.

More importantly, I am also disappointed to hear the implication that the NSA has more important things to do than to ensure that it is not inappropriately impacting the privacy of U.S. persons. That should be a core priority of the NSA, one that it can and should dedicate a reasonable amount of resources to. We think that with a reasonable amount of resources it can, as demonstrated in the FISA Court case of 2011, take measures to make reasonable estimates about how their authorities are impacting the American——

Chairman FRANKEN. Indeed, in the Bates FISA Court decision in 2011, NSA had been violating its authority, right? And they were able to discover that partly by doing the kind of estimation that they did.

Mr. BANKSTON. Indeed. And if such estimates had been required——

Chairman FRANKEN. Which was important to do.

Mr. BANKSTON. If those had been required earlier, we would have found out 3 years earlier that Americans were unconstitutionally being surveilled and presumably would have put a stop to it.

Chairman FRANKEN. Mr. Salgado?

Mr. SALGADO. I think it certainly makes sense to explore all the various ways that we can increase transparency around these programs whose data is being collected and what data. We want to be able to do that, of course, in a way that is a practical, reliable way. So I think it makes good sense to explore the different ways that that kind of an obligation could be satisfied by the Government and to take into account the costs that may be necessary to incur. But certainly the value of that sort of detail is significant.

Chairman FRANKEN. Thank you.

Mr. Bankston, you organized an impressive coalition of dozens of technology companies and civil society groups all calling for greater transparency and endorsing my bill specifically. It is a broad coalition of the Nation's leading technology and Internet companies, including Google and Apple and Microsoft and Facebook, as well as many of the leading civil liberties groups.

But, Mr. Salgado, could you just speak to why Google and Apple and Microsoft and Facebook—companies that normally compete with each other—are working together on this and what this means in terms of your business?

Mr. SALGADO. Yes, thank you, Chairman. The disclosures that we have seen coming out in June, and since then, have the great potential for doing serious damage to the competitiveness of these American companies. There is a potential for great damage to the Internet as a whole, but certainly what I think these companies and Google recognize is that the trust, which is threatened, is essential to these businesses. It is very important that the users of our services understand that we are stewards of their data, we hold it responsibly, we treat it with respect, and that there is not any sort of confusion around the rules where we may be compelled to disclose the data to the Government; and when there are rules around that, that it is clear what they are and the interaction between the Government and Google and the other companies as well.

This is essential to make sure that the users have confidence in their ability to place and trust their data with us. The impact of the disclosures in June are manifest. We can see as an academic matter—rather, as an anecdotal matter that customers who may be considering using the rich services available in the cloud are nervous to do so now as a result of those disclosures. This means that companies, some abroad and some in the United States, may not be taking advantages of the efficiencies and security benefits and all the other advantages of the cloud as a result of this. It is a terrible result and one that we need to address. Transparency, among other steps, would help restore the confidence in the cloud and American companies.

Chairman FRANKEN. Thank you.

The Ranking Member.

Senator FLAKE. Thank you. I appreciate the testimony.

Mr. Salgado, you heard the testimony previously and my question as to whether or not some of the companies would be concerned, would share the concern that there would be increased privacy concerns were this additional information to be gathered. Tell me why that does not make sense or tell me why you disagree.

Mr. SALGADO. Senator, I assume you are referring to the U.S. persons step within the government disclosure portion.

Senator FLAKE. Yes.

Mr. SALGADO. I think I share Mr. Litt's view that it is unlikely that this would result in any more disclosures by companies to be able to make the evaluation that would be required of the——

Senator FLAKE. So they have the data, they could simply drill down on their own data without asking you for additional information?

Mr. SALGADO. That is what I would anticipate, sir.

Senator FLAKE. But revealing more information about drilling down on U.S. persons does not concern you as a company to have that additional information out there as required in this legislation.

Mr. SALGADO. I think that as we look at the methods by which the intelligence community may address the U.S. persons estimation, it makes sense to look at that. How do you minimize those additional steps? And do they, in fact, require intrusions where there were not any before absent that obligation?

Senator FLAKE. Mr. Bankston, did you have any thoughts on that, the general privacy concerns that they raised, additional concerns about privacy that would be raised by drilling down on this information?

Mr. BANKSTON. I think it is important to note that, to some extent, privacy is invaded and has been invaded when the Government collects the data itself. And to say that we cannot make a meaningful estimate of how many people's data we have collected and how many U.S. persons' data we have collected, because to look at some small selection of it, to make that estimate would harm privacy, it just does not make sense to me. Privacy to some great extent has already been violated. We are just trying now to get a gauge of how many people's privacy has been violated.

Senator FLAKE. Mr. Salgado, you mentioned the prospect of different countries walling off their data or making an attempt to. How real of a concern and how timely of a concern is that? Have we seen such moves being taken by certain countries? Can you explain a little about that?

Mr. SALGADO. Yes, Senator, we have, so it is a very real threat. We have seen proposed legislation in jurisdictions to do just this.

We see it in several flavors. There is the possibility of requiring data location; so requiring companies to exclusively store data within a jurisdiction. You see affirmative laws that are often referred to as blocking statutes which would say companies that operate in this jurisdiction are not allowed to cooperate with U.S. authorities around data disclosure. So you see different flavors of these things. They all tend to start to create a network structure, an Internet structure that is based on political boundaries, and the idea of a global Internet quickly breaks down.

Senator FLAKE. Well, thank you. That is a concern that I think a lot of us have. This free flow across borders that has been so healthy and been necessary for the growth of this kind of communication would be disrupted.

Mr. Rosenzweig, let me just get a general answer from you on this. Is the value of legislation like this—I can see the value in a lot of companies to be able to explain more to their users and give

greater comfort there. Is there as much value in this being an additional check on Government not to go too far because they have to reveal this information? What is the greater value in legislation like this? Or is it shared that way?

Mr. ROSENZWEIG. I think the first principle of value of the legislation is the one that Senator Franken expressed, which would be to statutorily mandate that which is now merely voluntary and an act of grace by the executive branch. So I think that that is—regularizing that, institutionalizing that is a positive value.

I think that in general, legislation that requires the Government to explain itself is a positive value as well, everything from FOIA to Inspectors General statutes.

My concern in particular would be to ensure that the disclosure requirements do not wind up disrupting the existence of heretofore undisclosed programs that are of value to us, and that I think I cannot answer in a generalized manner. I think it is a very case-by-case specific matter. I think that it is probably not a decision best left to the executive branch alone. I think it is a decision left to the executive branch in a classified discussion with this body and with the House of Representatives. It by its nature cannot be a discussion that, at least at the first instance, involves the American people, because that by its nature terminates the discussion itself.

Senator FLAKE. Thank you. This has been very helpful.

Chairman FRANKEN. Thank you, Senator Flake.

Chairman Leahy has graced us and has arrived. I would like to add this statement from the Chairman to the record.

[The prepared statement of Chairman Leahy appears as a submission for the record.]

Chairman FRANKEN. I would like to ask him to ask his questions.

Chairman LEAHY. Thank you, and I also thank the courtesy of my friend from Connecticut, Senator Blumenthal.

I think more and more people agree or should agree that we need additional transparency about our government surveillance activities. Without greater transparency, we are not going to restore public confidence. And I think Senator Franken's work to build a consensus around transparency legislation deserves praise, and I am glad that Google and other tech companies are lending their support to that bill.

I think that the tech industry realizes we need more than just transparency. We need some substantive reform. Seven of the major tech companies, and I am going to read them to make sure I got them all right—Google, Microsoft, Yahoo!, Apple, Facebook, AOL, and LinkedIn—signed a letter to me supporting greater transparency. They want substantial enhancement to privacy protection, appropriate oversight, and accountability matters, and I know Mr. Salgado knows that letter. I recently introduced a comprehensive surveillance reform bill—it is bipartisan—the USA Freedom Act, and I appreciate these companies supporting stronger FISA reform.

Mr. Salgado, let me ask you, just enhancing transparency, is that going to be enough to bring back global confidence in American technology companies? Do we need to do more? And if we do not do more, is this going to affect U.S. businesses?

Mr. SALGADO. Thank you, Mr. Chairman. I think it is an important step to have increased transparency, but I do agree that more is needed than that. And as you noted, we have expressed our support for the legislation that you have offered. I think we need some reform that allows users and others to know that the intelligence community and its collection of data is done under law, that it is rule-bound, that it is narrowly tailored, that there is oversight, there is accountability for it; and, of course, as we have been discussing today, that there is some transparency around it that can help bring some of the trust that all this is happening.

Chairman LEAHY. And aside from affecting the reputation of the United States, if we do not enact meaningful reforms, it is going to affect businesses, too, is it not?

Mr. SALGADO. Absolutely, Mr. Chairman. And, in fact, we have already seen impacts on the businesses. I think Chairman Franken cited a couple studies in the opening statement that reflected some serious financial consequences. I think there are real concerns around the entire structure of the Internet over these revelations if this is not addressed correctly.

Chairman LEAHY. Well, let me go a little bit on that. One of my biggest concerns about Section 215 phone records is that the legal rationale underpinning it has no limiting principle. If all of our phone records are relevant to intelligence investigations, then why wouldn't everything be considered relevant? And if that is the case, are companies like yours concerned that consumers will not trust that their data is safe from unwarranted government intrusion? Does Google think about what that might do as far as cloud technology is concerned?

Mr. SALGADO. That is right, Mr. Chairman. The confusion that came out as a result of the June revelations and since then and additional stories I think have led to a real concern, both inside the United States and outside of the United States, about what it is that is happening and what are the rules that govern it, what is the role of the FISA Court, what are the decisions that are coming out of that Court. All of those have played a role in the confusion and the need for some clarity.

Chairman LEAHY. Well, especially when NSA handles things so carelessly that they let a 29-year-old contractor walk off with all their secrets, and so far as I know, nobody has even been reprimanded for that.

Mr. Bankston, what do you think?

Mr. BANKSTON. Speaking generally, we think that transparency is critical to restoring trust in the U.S. Internet economy and in the U.S. Government itself, but that it alone is not sufficient and that indeed substantive reform is necessary. CDT supports the bill that you have introduced, the USA Freedom Act, and we thank you for it. We look forward to working with you and the Committee as it moves forward.

Chairman LEAHY. I am worried about overclassification. I find oftentimes—and every administration has been guilty of this—it is easier to classify a mistake rather than trying to explain it.

Let me ask, Mr. Salgado, are you permitted to tell us whether Google has received any FISA Court orders?

Mr. SALGADO. I am sorry, Mr. Chairman. I would have to decline that answer until the bill that we are discussing today has passed.

Chairman LEAHY. Is our country safer because you cannot answer the question?

Mr. SALGADO. I cannot imagine the country is safer as a result of that.

Chairman LEAHY. Thank you. That answers my question.

Mr. Bankston, concerns have been raised that company-by-company reporting of FISA might tip off those we are trying to track, but there is a lot of reporting available on criminal surveillance. Are national security related investigations sufficiently different from criminal investigations so that we have to have this kind of secrecy?

Mr. BANKSTON. I do not believe so, Chairman, no. In the criminal context, we are often investigating sophisticated organized criminals and, in fact, sometimes investigating terrorists. And yet we have been able to publish and the U.S. Government has been able to publish very detailed statistics about how the Government is using its authorities, both the Government as a whole and company by company, without any suggestion that that has harmed national security.

And I just want to take the moment to address this issue of lumping all of those authorities together. I think that combining numbers for targeted FISA intercepts with FISA pen registers, with FISA orders for records, with FISA warrants for stored communications, with all the range of national security letters, and then combining that with all federal, State, and local law enforcement warrants, wiretaps, pen registers, subpoenas and other court orders leads to such a useless number as to be actually detrimental. It is like asking a doctor to attempt to diagnose a patient by looking at his shadow. Only the grossest, most obvious abuse, if even that, would be evident.

Chairman LEAHY. And I apologize to Professor Rosenzweig. I have not had time. I will submit a question for the record, Mr. Bankston, on your argument that companies' First Amendment rights have been violated, the question of prior restraint, the Second Circuit case. Please take a look at the question. I really would like your answer for the record. It is important to me.

Mr. BANKSTON. Thank you, Senator.

[The question from Chairman Leahy appears as a submission for the record.]

Chairman LEAHY. Thank you.

Chairman FRANKEN. Thank you, Mr. Chairman.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you. Thank you, Mr. Chairman and Mr. Chairman. Thank you to both Chairmen. And thank you all for being here today.

I was interested in a number of your points, particularly Mr. Salgado, that additional measures are necessary, especially in response to Chairman Leahy's questions, to not only provide additional transparency but also assure that individual rights are protected. As you know, I have proposed that there be a constitutional advocate to, in effect, provide some adversarial process within the FISA Court. You know as lawyers courts make better decisions

when more than one side is presented. Very few judges would permit a proceeding before them in which only one side is presented because they know that the core principle of our judicial system is that it is adversarial and that the truth emerges as differing points of view, factual perspectives, and evidence are presented. And so that is one area where I think that the system can be made more accountable, if not more transparent, and as well, disclosure of some of the rulings and opinions of the Court. Right now it is a secret court that operates in secret making secret decisions and secret law—one of the few, if only, courts in the United States where there is any secret proceedings of this kind making secret law.

So let me elicit your comments on those kinds of additional protections to our constitutional rights from the perspective that you all have raised about our need for credibility and trust internationally in this system. After all, the means of communication, the Internet, depend on international trust and credibility. Otherwise, it falls apart. So let me ask that somewhat open-ended question.

Mr. SALGADO. Well, thank you, Senator. I am happy to take the first swipe at that. There are a number of proposals right now that are being considered, and that is a very good thing. And the general principles that there needs to be accountability and transparency with some oversight and the rules are clear are addressed by the various bills.

Certainly as an example, making sure that a court that is reviewing applications for surveillance has an opportunity to hear different ideas, different sides, that makes perfect sense. And it is certainly at the heart of most of the judicial proceedings we have in the United States. So that is something that I think makes a good deal of sense as far as a structural change to the current arrangement under FISA and the obtaining of FISA authorities.

The same, of course, is true with understanding the interpretations of the law that the Court applies to the different applications that come in. I think those are two good examples of the sorts of ideas that can help restore confidence that the system works.

Mr. ROSENZWEIG. I am actually a fan of the idea of an advocate, but for slightly different reasons, I think, than Mr. Salgado just said. The reason that we do not have an advocate in the search warrant application situation, for example, which is an ex parte application, or in a grand jury situation is because those decisions are ultimately subject to ex ante review in a criminal proceeding where there is a defense attorney who presents an adversarial view on whether or not the issuance of the warrant was with probable cause or the grand jury subpoena was overbroad or things like that. We lack that systematic check in the intelligence context because, of course, the intelligence surveillance rarely, if ever, results in a criminal prosecution in which that kind of adversarial process comes forward.

So to my mind, I would want to distinguish in allowing an advocate between those situations in which the FISA Court were making some broad new systematic determination and interpretation of law like the interpretation that gave us the relevance decision in the Section 215 law, I would like to distinguish that from what I would characterize—and I admit the line is hard to draw—"routinized applications of a settled law," where the value of an adver-

sarial advocate would be much diminished, and the procedural difficulties that would arise from it, the costs involved, the time delay, might very well be adverse to national security. So cabined in that way, I think that would be a perfectly fine idea.

And as for the public disclosure, I would offer the exact same answer I gave Senator Flake in the other context, which is provided that we make sure that it does not wind up with the adverse effect of disclosing heretofore undisclosed programs that are properly classified, that would be as well as advancement in our understanding. Again, I admit that is a hard line to draw, and probably in both instances the best answer would be to let the FISA Court make that decision itself, to authorize the appointment of the advocate in the situations where it wants to, and to authorize them affirmatively or direct them affirmatively to make public disclosures when they think the disclosure of an opinion would not adversely affect national security interests.

Mr. BANKSTON. Thank you. The FISA Court's job used to be pretty straightforward. It was a pretty straightforward statute based on some pretty straightforward Fourth Amendment jurisprudence addressing some pretty straightforward technologies.

Now we have the FISA Court addressing an incredibly complex and broad statute in the form of the FISA Amendments Act; we have a rapidly complexifying technological landscape; and we have the FISA Court, rather than simply making magisterial decisions, creating a body of common law on some of the hardest and most important Fourth Amendment questions of our time, sometimes in the face of what the Court has described as misleading conduct by the lawyers in front of it.

In that context, I do believe that it is critically important not only to have great transparency regarding the decisions made by the Court, but also to have an advocate in front of the Court who is there to protect the people. And as such, CDT does support your legislation, Senator Blumenthal, and is working with your staff and with Chairman Leahy's staff on the issues that that might bring to bear.

Senator BLUMENTHAL. Thank you all.

Thank you, Mr. Chairman.

Chairman FRANKEN. Thank you, Senator Blumenthal. Not to speak for you, but I think that the way that Mr. Rosenzweig described the role of a constitutional advocate is very in line with what you envision.

Senator BLUMENTHAL. Very much so. Thank you.

Chairman FRANKEN. Well, thank you. I want to thank all three of you for your testimony, and in closing I want to also thank the Ranking Member, Senator Flake, along with Senator Heller and Chairman Leahy who lent this legislation critical support. And, of course, I want to thank all the witnesses, each and every one of them who appeared today. We have heard a lot of valuable testimony. There was a lot that I agreed with. There are some things that I did not agree with, but I want to leave everyone with this thought:

There is no question that the American people need more information about these programs. Just no question about that. For democracy to work, its citizens need to have at least a basic amount

of information about the surveillance their own Government conducts over their affairs. I think that my bill will give the American people that transparency, and I am looking forward to continuing to work with the administration and my colleagues to make sure that we are getting it right.

We will hold the record open for 1 week for submission of questions for the witnesses and other materials. This hearing is adjourned.

[Whereupon, at 11:43 a.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

UPDATED Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

On

"The Surveillance Transparency Act of 2013"

Wednesday, November 13, 2013
Dirksen Senate Office Building, Room 226
10:00 a.m.

Panel I

The Honorable Dean Heller
United States Senator (R-NV)
Washington, DC

Panel II

The Honorable Robert Litt
General Counsel
Office of the Director of National Intelligence
Washington, DC

Brad Wiegmann
Deputy Assistant Attorney General, National Security Division
Department of Justice
Washington, DC

Panel III

Kevin Bankston
Director, Free Expression Project
Center for Democracy and Technology
Washington, DC

Paul Rosenzweig
Principal, Red Branch Consulting
Professorial Lecturer in Law, George Washington University
Washington, DC

Richard Salgado
Director, Law Enforcement and Information Security Matters
Google, Inc.
Mountain View, CA

PREPARED STATEMENT OF HON. AL FRANKEN

Opening Statement of Chairman Franken on "The Surveillance Transparency Act of 2013"

This hearing will come to order. Welcome to the Senate Judiciary Subcommittee on Privacy, Technology and the Law. The subject of this hearing is my bill, the Surveillance Transparency Act of 2013. I'm proud to say that two weeks ago I re-introduced this bill with the support of my friend and colleague, Senator Dean Heller of Nevada, who we'll be hearing from shortly.

This bill is urgently necessary. Americans understand that we need to give due weight to privacy, on the one hand, and national security, on the other. But Americans are also naturally suspicious of executive power. And when the government does things secretly, Americans tend to think that power is being abused. This is exactly the place where congressional oversight is useful and necessary.

For months now, there has been a steady stream of news stories about the NSA's surveillance programs. And yet right now, by law, Americans cannot get really the most basic information about what's going on with those programs. Consider this: it's been months since the PRISM program and the telephone call records program were revealed to the public. And yet to this day:

- Americans don't know the actual number of people whose information has been collected under those programs.
- They don't know how many of those people are American.
- And they have no way of knowing how many of these Americans have had their information actually seen by government officials – as opposed to just being held in a database.

The Administration has taken good steps in good faith to address this problem. But I'm afraid that these steps are too little, and they're not permanent.

And so, Americans still have no way of knowing whether the government is striking the right balance between privacy and security – or whether their privacy is being violated. There needs to be more transparency.

I've written a bipartisan bill to address this. It will require the NSA to disclose to the public how many people are having their data collected under each key foreign intelligence authority. It would make the NSA estimate how many of those people are American citizens or green card holders – and how many of those Americans have had their information actually looked at by government agents.

My bill would also lift the gag orders on Internet and phone companies so that those companies can tell Americans general information about the number of orders they're getting under each key authority and the number of users whose information has been produced in response to those orders.

Right now, as a result of those gags, many people think that American Internet companies are giving up far more information to the government than they likely are. The Information Technology & Innovation Foundation estimates that American cloud computing companies could lose $22 to $35 billion in the next 3 years because of concerns about their involvement with surveillance programs. The analytics firm Forrester puts potential losses much higher, at $180 billion.

A few companies have litigated and secured permission to publish limited statistics about the requests that they get. But again, this is too little – and it's not permanent.

My bill would permanently ensure that the American people have the information they need to reach an informed opinion about government surveillance. And it would protect American companies against losing business from misconceptions about their role in these programs.

I'm pleased to say that this bill is the leading transparency proposal in the Senate, supported by a strong coalition of tech companies and civil liberties groups. The version as introduced gained the support of 12 Senators, including the Chairman of the full Judiciary Committee, Patrick Leahy. I anticipate that we'll soon be adding our original supporters onto the new bipartisan bill, hopefully with some additional support as well.

The purpose of this hearing is to make the case for this bill and to improve it by getting the feedback of top experts in the Administration, privacy groups, and the private sector. I've specifically asked the Office of the Director of National Intelligence and the Department of Justice to provide candid comments on this bill – especially any concerns they have. I've already added provisions to the bill to protect national security, but I want to know of any further concerns they have. I suspect that I'll agree with them in some cases and disagree with them on others. In those cases, I want to have an open exchange about those disagreements.

That said, I want it to be clear at the outset that I have the utmost respect for the men and women of our Intelligence Community. I think they are patriots, and I think they save lives.

I look forward to starting this conversation. With that I'll turn to our Ranking Member, Senator Flake.

PREPARED STATEMENT OF HON. PATRICK J. LEAHY

Statement of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
Hearing On
"The Surveillance Transparency Act of 2013"
November 13, 2013

Revelations about the National Security Agency's dragnet collection of Americans' telephone records has led to an important national conversation about the scope of our government's intelligence-gathering authorities. Today, the Subcommittee on Privacy, Technology, and the Law will consider legislative changes to increase the transparency of the government's surveillance activities. As a cosponsor of the Surveillance Transparency Act, I thank Senator Franken for his leadership on these issues and for holding this hearing.

While I appreciate recent efforts by the administration to release documents and be more forthcoming about its surveillance activities, we must codify expanded reporting requirements to ensure accountability. The Surveillance Transparency Act would require enhanced government reporting about requests for information from private companies under the Foreign Intelligence Surveillance Act and the USA PATRIOT Act. The legislation would require the government to report annually to the public on the number of surveillance orders issued to private companies and the types of information sought. Additionally, the bill would compel the government to produce public reports on the number of Americans whose information was collected and reviewed by government officials.

The bill also would permit companies to disclose voluntarily more information about the types of requests for user information they receive from the government. Under the legislation, companies would be allowed to reveal the number of orders they received and complied with; the general types of information that were furnished; and the number of users whose information was provided to the government for each type of surveillance request. I strongly believe that this enhanced transparency will help to inform the public debate about the breadth of the government's surveillance authorities.

The intelligence community faces a serious trust deficit. More transparency is one important step toward rebuilding that trust. But transparency alone is not enough. To completely restore faith in the intelligence community and global confidence in America's technology companies, we must make significant substantive reforms to our surveillance laws – to stop the dragnet collection of innocent Americans' phone records and place appropriate safeguards on a whole range of surveillance authorities.

That is why last month, I introduced the bipartisan, bicameral USA FREEDOM Act. I was pleased to incorporate important transparency provisions derived from the Surveillance Transparency Act into that legislation. I look forward to hearing from the witnesses today and appreciate the letter from more than 60 Internet companies and advocacy groups supporting expanded transparency and accountability reforms in the Surveillance Transparency Act.

#####

PREPARED STATEMENT OF HON. ROBERT S. LITT AND J. BRADFORD WIEGMANN

JOINT TESTIMONY OF THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE AND THE DEPARTMENT OF JUSTICE

Robert S. Litt, General Counsel, Office of the Director of National Intelligence

J. Bradford Wiegmann, Deputy Assistant Attorney General, National Security Division, United States Department of Justice

Senate Committee on the Judiciary

Subcommittee on Privacy, Technology and the Law

November 13, 2013

Good afternoon Chairman Franken, Ranking Member Flake, and distinguished members of the Subcommittee. We appreciate this opportunity to appear before you today to discuss the Intelligence Community's efforts to increase transparency concerning certain intelligence collection activities under the Foreign Intelligence Surveillance Act (FISA). We will also offer some initial views on S.1621, the Surveillance Transparency Act of 2013.

The Administration's Efforts To Increase Transparency of FISA Activities

Recent unauthorized disclosures have sparked an ongoing public dialogue about intelligence collection activities, particularly those conducted under FISA. Increasing transparency regarding how some of these activities are conducted is important to ensuring that this dialogue is grounded in facts. As we have publicly explained over the last several months, bulk collection of telephony metadata under the business records provision of FISA (known as Section 215), and other collection activities targeting non-U.S. persons overseas under Section 702 of FISA, are authorized by law, have been approved by the FISA Court, and have been overseen by all three branches of our government. The extensive information we have released to the public about these activities over the last several months demonstrates the rigorous oversight under which these programs operate.

We recognize the public interest in understanding how the Intelligence Community uses the legal authorities provided by Congress to conduct surveillance and gather foreign intelligence. It is appropriate for Congress to examine whether these legal authorities, as implemented by the Executive Branch, strike the appropriate balance between privacy and national security. We welcome the opportunity to discuss ways to make more information about intelligence activities conducted under FISA available to the public in a responsible way. At the same time, we are mindful of the need not to disclose information that our adversaries could exploit to evade surveillance and harm our national security. There is no doubt that the recent unauthorized

disclosures about our surveillance capabilities risk causing substantial damage to our national security, and it is essential that we not take steps that will increase that damage.

In keeping with this balance, in June the President directed the Intelligence Community to make as much information about the Section 215 and Section 702 programs available to the public as possible, consistent with the need to protect national security and sensitive sources and methods. Since then, the Director of National Intelligence has declassified and publicly released substantial information in order to facilitate informed public debate about these programs. Among other things, the Government has declassified and disclosed the primary and secondary orders from the FISA Court that describe in detail how the bulk telephony metadata collection program operates and the important restrictions on how the data collected under the program are accessed, retained, and disseminated. We have also declassified and released to the public numerous FISA Court opinions and orders concerning the two programs, including detailed discussions of compliance issues that have arisen during the programs' history and the Government's responses to these incidents. We have also released extensive materials that were provided to the Congress in conjunction with its oversight and reauthorization of these authorities.

Our efforts to promote greater transparency through declassification and public release of relevant documents are not yet complete. We will continue to declassify and release more information, while carefully protecting information that we cannot responsibly release because of national security concerns. These ongoing declassification efforts are an important means of enhancing public confidence that the Intelligence Community is using its legal authorities appropriately, which has unfortunately become increasingly necessary in the wake of confusion, concerns, and misunderstandings caused by the recent and continuing unauthorized disclosures of classified information.

As part of our ongoing efforts to increase transparency, the Director of National Intelligence has also committed to providing annual public reports that include nationwide statistical data on the Intelligence Community's use of certain FISA authorities. Specifically, for each of the following categories of FISA and related authorities, the Intelligence Community will release to the public the total number of orders issued during the prior twelve-month period and the number of targets affected by these orders:

- FISA orders based on probable cause (Titles I and III and Sections 703 and 704 of FISA).
- Directives under Section 702 of FISA.
- FISA Business Records orders (Title V of FISA).
- FISA Pen Register/Trap and Trace orders (Title IV of FISA).
- National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. § 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709.

This information will enable the public to understand how often the Intelligence Community uses these authorities nationwide, how many persons or entities are targeted by these efforts, and how these figures change over time. The Director of National Intelligence has concluded that providing this information on a nationwide basis is an acceptable course in light of the goal of public transparency, without unduly risking national security.

We also understand the concerns that specific companies have expressed as to their ability to inform their customers of how often data is provided to the Government in response to legal process. In light of those concerns, we have authorized companies to report within certain ranges the total number of federal, state, and local law enforcement and national security legal demands they receive on a nationwide basis, and the number of user accounts affected by such orders. This allows companies to illustrate that such process affects only a tiny percentage of their users, even taking all of that process together, and thus to refute inaccurate reports that companies cooperate with the Government in dragnet surveillance of all of their customers. At the same time, this approach avoids the disclosure of information to our adversaries regarding the extent or existence of FISA coverage of services or communications platforms provided by particular companies.

The scope of the voluntary disclosures by the Executive Branch concerning sensitive intelligence collection activities carried out under FISA is unprecedented. We hope that the information we have released, and will continue to release, will allow the American public to understand better how our intelligence collection authorities are used. We also hope the public will see the rigorous oversight conducted by all three branches of government over our intelligence activities, which helps to ensure that those activities protect national security, balance important privacy considerations, and operate lawfully.

Preliminary Views on S.1621, the Surveillance Transparency Act of 2013

Turning to S.1621, we have reviewed the bill with both transparency and national security concerns in mind, and we share the goal of the legislation of providing the public with greater insight into the Government's use of FISA authorities. Many of the bill's provisions are consistent with the steps we have taken to report more information to the public while protecting intelligence sources and methods. Other provisions, however, raise significant practical or operational concerns, as we shall explain. We hope that we can work with you to find common ground on this bill, and we would be happy to provide technical assistance to address the concerns we have identified.

Section 2

Section 2 of the bill includes enhanced reporting requirements for the use of FISA authorities pertaining to electronic surveillance, pen register and trap and trace devices, business records, and Title VII. Some of these reporting requirements we fully support, but others would be difficult if not impossible for the Government to implement.

We support the provisions requiring reporting of the total number of applications made for orders pursuant to Titles I, IV, and V of FISA, including reporting on the total number of such orders granted, modified, or denied. Likewise, we support the provisions requiring reporting of the total number of directives issued under Section 702 and orders granted under Sections 703 and 704. And for each of these authorities, we would support provisions requiring the Government to report the number of targets affected by such orders, information we have already committed to provide.

We have significant concerns, however, about provisions that would require reporting exact numbers or estimates of the number of individuals and of U.S. persons whose information is acquired from surveillance conducted pursuant to these authorities but who are not themselves targets of the surveillance. We can compile and report statistics concerning the *targets* of FISA collection activities, but it would be difficult if not impossible to do so for individuals whose communications or information may be incidentally collected.

Identifying the number of persons who are "subject to surveillance" under FISA would require reviewing, in detail, all of the information we collect and then manually determining every unique person who is party to an intercepted communication. That is, we would have to review all of the communications collected concerning a foreign intelligence target and attempt to determine who else is involved in each communication and whether each such individual is someone who has already been counted or, instead, is a new individual communicating with the target, which will often be an impossible task. Moreover, doing so would run contrary to the culture and mission of the Intelligence Community, which is to discover among the communications acquired those of foreign intelligence value and disregard those that hold no such promise. What's more, we would then have to determine which of those individuals are U.S. persons—although often there is no reliable way to determine that and attemping to do so would further detract from the privacy of the person incidentally collected.

Many communications acquired under FISA are never reviewed by analysts or at least do not become the focus of any attention. When analysts do review them, they focus on identifying material that is of foreign intelligence value. It would be difficult if not impossible to count the number of persons whose communications may have been incidentally obtained in this context, let alone attempt to identify which of those individuals were U.S. persons, as the bill would require. The same is true of collection via the FISA-authorized pen register/trap and trace program, which collects metadata associated with telephone calls or electronic communications of a target .

Moreover, attempting to identify the numbers of persons or U.S. persons whose communications or information may be incidentally collected would, in practice, have a privacy-diminishing effect directly contrary to the aims of this bill. Attempting to make this determination would require the Intelligence Community to research and review personally identifying information solely for the purpose of complying with the reporting requirements, even if the information has

not been determined to contain foreign intelligence. Such an effort would conflict with our efforts to protect privacy.

In sum, reporting on numbers of targets is feasible; it is consistent with our efforts to protect privacy; and it provides information that is valuable and relevant to the public, i.e., the numbers of individuals whom the Government has purposefully sought to monitor. Reporting on numbers of individuals affected by incidental collection is operationally difficult, if not impossible, and attempting to do so would require otherwise unnecessary intrusions on personal privacy. We therefore strongly urge that the bill's disclosure requirements only apply to the number of individuals who are targets of intelligence collection, and not to the number of individuals whose communications may have been incidentally collected.

Section 3

Section 3 of the bill would amend FISA to allow a person (including a company) who received a FISA order to disclose to the public every six months, among other things, the total number of orders or directives received under each specific FISA authority, the percentage or total number of orders or directives complied with, in whole or in part, and the total number of individuals, users, or accounts whose information of any kind was produced to the Government, or was obtained or collected by the Government, under an order or directive received under that specific authority.

We recognize the importance of allowing companies to provide transparency to their customers, and we have taken steps to allow them to do so. The Government has agreed to permit companies to report, in certain ranges, the aggregate number of criminal and national security-related orders they receive from federal, state, and local government entities combined. We have also agreed to permit companies to report the number of user accounts affected by such orders. We believe that those measures will serve the overriding interest of the public: these measures will show that the sum total of all such process affects only a tiny fraction of the companies' user accounts. At the same time, the aggregated nature of such disclosures minimizes the potential harm to national security. We could support legislation that would mandate such disclosures as a matter of law.

We do have significant operational and national security concerns with the detailed, company-by-company disclosures that the bill, as currently written, would authorize regarding legal demands for interception of communications. More detailed company-by-company disclosure threatens harm to national security by providing a roadmap for our adversaries on the Government's surveillance capabilities relating to services or communications platforms offered by any particular company. This information would be valuable to our adversaries, who could derive a clear picture of where the Government's surveillance efforts are directed and how its surveillance activities change over time, including when the Government initiates or expands surveillance efforts involving specific providers or services that adversaries may have previously

considered "safe." There is a limit to how much we can say about this in an open hearing, and we would be happy to provide more detailed information in a classified setting. But the basic point is straightforward: disclosing information in a manner that would permit our adversaries to deduce our specific collection capabilities and shortcomings would harm national security by allowing those adversaries to switch providers and services in order to avoid our surveillance. .

Already, our Intelligence Community knows that our adversaries purposely gather such information to assess our capabilities and evade surveillance. Providing them the information on our collection capabilities that they are working so hard to gather could significantly and irreparably harm our intelligence collection efforts. So, while we fully support nationwide, aggregate disclosure in the interests of transparency, as well as certain generic company-level reporting, we are concerned that the bill's provisions requiring more detailed company-specific disclosure would pose a risk to national security.

As we have explained, the Intelligence Community has carefully considered how to disclose FISA statistics in a way that will educate the public while protecting sources and methods associated with FISA collection activities. We believe that the nationwide statistics the Government has committed to provide, and the more general data the Government has authorized companies to disclose, strike the right balance. This level of reporting would demonstrate how various FISA authorities are used by the Government in the aggregate and also allow the public to see, in general, the number of subscriber accounts that are accessed through all forms of legal process, without compromising our national security authorities.

Again, thank you for the opportunity to appear before you today. As we said at the outset, we are entirely supportive of the goal of the Surveillance Transparency Act, to increase public understanding of the ways in which we use our legal authorities to conduct surveillance and oversee that use to ensure that it complies with the law. While we have concerns about some of the specific provisions, we look forward to continuing to work with the Subcommittee on improving this important transparency legislation. We would be pleased to answer any questions.

PREPARED STATEMENT OF KEVIN S. BANKSTON

Statement of Kevin S. Bankston

Senior Counsel & Director of the Free Expression Project at
The Center for Democracy & Technology

Before the Senate Committee on the Judiciary,
Subcommittee on Privacy, Technology and the Law
on
The Surveillance Transparency Act of 2013

November 13, 2013

Chairman Franken, Ranking Member Flake and Members of the Subcommittee:

Thank you for the opportunity to testify this morning on behalf of the Center for Democracy & Technology, a non-profit, public interest advocacy organization dedicated to keeping the Internet open, innovative and free. Although I speak only for CDT, as the Director of its Free Expression Project, I am also here today in the service of a broad coalition brought together by CDT this summer to advocate for greater transparency around the government's surveillance activities.

Our coalition includes dozens of Internet companies large and small, such as Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Yahoo, and Twitter, as well as over fifty nonprofit organizations and trade associations from across the political spectrum. The members of that coalition all signed a letter this July asking Congress to ensure that Internet companies who are entrusted with privacy and security of their users data are allowed to regularly issue transparency reports that reflect the specific number of requests that they receive under particular surveillance authorities such as those in the Foreign Intelligence Surveillance Act (FISA), as well as the specific number of individuals affected by those requests, and the basic categories of information sought.[1] The coalition further asked that Congress require the government to issue its own regular report with the same details.

In addition to seeking redress from Congress, a number of these companies have sought a remedy from the Foreign Intelligence Surveillance Court, an effort that CDT and an alliance of free speech organizations have supported as a friend of the court.[2] However, we do not believe that individual companies should have to seek permission from the FISA Court, nor be forced to individually negotiate agreements with the Department of Justice on an ad hoc basis, in order to publish data that they have a First Amendment right to share and that we, the people, have a right to know.

---

[1] That coalition letter is available at https://www.cdt.org/weneedtoknow.
[2] *See Center for Democracy & Technology*, "Civil Liberties Groups Support Google and Microsoft in Demanding Transparency from Secret Surveillance Court", September 9, 2013, at https://www.cdt.org/pr_statement/civil-liberties-groups-support-companies-demanding-transparency-fisc.

Rather, we believe that the best and most permanent solution is for Congress to act, now.

Therefore, CDT and the coalition are grateful to Senator Franken and to the cosponsors of the Surveillance Transparency Act for so quickly introducing legislation that would allow companies, and require the government, to publish basic statistics about the scope and nature of the government's surveillance activities. As we made clear in our second joint letter this September,[3] the coalition strongly supports this effort and we look forward to working together to achieve passage of legislation that will ensure the level of transparency necessary to appropriately inform the American public and preserve the trust of Internet users here and around the world.

Particularly in the wake of recent revelations about the nature of the National Security Agency's surveillance programs, we believe that this level of transparency about what the companies do—and don't do—when the government demands their users' data is critically important for three reasons I'll discuss today:

First, the American people have a clear right and need to know this information, so that they may have a more informed public debate about the appropriateness of the government's use of its surveillance authorities, and so as to better ensure that those authorities are not misused or abused.

Second, the companies have a clear First Amendment right to share this information, and the government's attempt to gag them and prevent them from sharing even this most basic data is clearly unconstitutional.

Third, greater transparency is urgently necessary to restore the international community's trust in the US Internet industry and the US government, in the face of widespread concern from foreign governments and Internet users about the privacy and security of data that is transmitted to or through the United States. We must take this opportunity to demonstrate that Americans' constitutional rights and everyone's human rights are being respected. And if the numbers show otherwise, we must take this opportunity to reform our surveillance laws to better protect our rights as well as our national security.

The level of transparency provided for in the Surveillance Transparency Act would serve all of these interests. As I will discuss, such transparency would not threaten national security, but would help to ensure that our surveillance programs are narrowly tailored, effectively overseen, and consistent with statutory, constitutional, and human rights. CDT supports these transparency efforts as a key part of any broader surveillance reform agenda, and we are pleased to see similar transparency

---

[3] The second coalition letter is available at https://www.cdt.org/files/pdfs/weneedtoknow-transparency-bills-support-letter.pdf.

provisions in the USA FREEDOM Act, a bill that CDT strongly endorses.[4] Greater transparency is no replacement for substantive reform of our surveillance laws, but can serve as a key stepping stone toward that broader reform by allowing the public and policymakers to better understand how the government is using its power.

I. The Public Has a Right to Know.

Democracy requires accountability, and accountability requires transparency. As Congress recognized when it imposed detailed reporting requirements regarding law enforcement wiretaps,[5] public understanding of how the government uses its surveillance powers is a critical check on abuse. The need for such a check is even greater in the context of national security investigations, where the vagueness and breadth the government's mandate, the greater level of secrecy, and the lack of traditional checks and balances like individualized and particularized probable cause-based warrants and adversarial proceedings in open courts, all heighten the risk of overreach and abuse.[6]

Detailed government reporting on how national security surveillance authorities are being used is critical to maintaining accountability. However, neither the rudimentary reporting that is currently required by law, which is basically a tally of the number of different types of orders issued,[7] nor the additional annual reporting promised in August by the Director of National Intelligence, is sufficient.[8] That is

---

[4] *See Center for Democracy & Technology*, "CDT Endorses FISA Reform Bill, USA FREEDOM Act", October 29, 2013, at https://www.cdt.org/pr_statement/cdt-endorses-fisa-reform-bill-usa-freedom-act.

[5] *See* 18 U.S.C. § 2519.

[6] *See, e.g.*, United States v. U.S. District Court, 407 U.S. 297, 314 (1972) ("The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.") (holding that the Fourth Amendment's safeguards apply to national security-related wiretapping).

[7] *Compare, e.g.*, the 2-page letter from the Department of Justice recounting the number of FISA orders and National Security Letters issued in 2012 (at https://www.fas.org/irp/agency/doj/fisa/2012rept.pdf) to the massively detailed annual wiretap report issued by the Administrative Office of the United States Courts in the same year (at http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx).

[8] *See Center for Democracy & Technology*, "Administration Continues to Disappoint on Transparency Around NSA Surveillance", August 29, 2013, at https://www.cdt.org/pr_statement/administration-continues-disappoint-transparency-around-nsa-surveillance, commenting on DNI Clapper's announcement on the same date, at http://icontherecord.tumblr.com/post/59719173750/dni-clapper-directs-annual-release-of-information.

because neither the statutorily required reporting nor the DNI's voluntary reporting give any indication of how many people are actually having their data provided to or obtained by the government under any particular legal authority. Indeed, the limited additional reporting proposed by the DNI—which would only indicate how many individuals have had their data "targeted" by the government—would be affirmatively misleading. For example, the DNI's proposed reporting for 2012 would only have indicated that around 300 individuals had their data "targeted" under Section 215 of the PATRIOT Act.[9] Yet we now know that the government has used Section 215 of the PATRIOT Act to obtain the phone records of *everyone in the country*. Such falsely reassuring reporting would do more harm than good.

This is why not only more detailed government reporting, but also reporting by individual companies, is an absolutely necessary additional check. Reporting by individual companies puts the government's numbers into context, allowing companies themselves to define their terms and thereby ensure that the government is npt able to cabin its disclosures in a misleading way. Company reporting also allows a comparison of the government's numbers and the companies numbers, such that any significant discrepancy can be detected, and an explanation for that discrepancy can be demanded. The American people should be able to trust their government—but must also be able to verify what they are being told. Trust, but verify.

Company reporting better ensures that the American people have a clearer picture of the basic scope and nature of the government's surveillance activities. It also allows Internet users both here and abroad to compare the compliance rates between companies, and judge which companies are more or less conscientious about pushing back on improper or overbroad requests. Such reporting fosters a greater understanding of and appreciation for companies' specific privacy practices, and encourages companies to compete on privacy and to strengthen their practices in order to build user trust.

The public has a right to know what these companies do, and don't do, when the government demands their data. Not only that: the companies themselves have a right, and a pressing business need, to tell us.

---

[9] *See* "Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act Reauthorization", August 9, 2013, at p.4, at https://www.eff.org/sites/default/files/filenode/section215.pdf ("Although the number of unique identifiers has varied substantially over the years, in 2012, fewer than 300 met the "reasonable, articulable suspicion" standard and were used as seeds to query the [telephony]data [obtained under Section 215] after meeting the standard.").

II. The Companies Have a Right to Tell Us.

As several of the companies have recounted at length in their briefs to the FISA court, the FISA statutes does not prohibit them from disclosing basic aggregate data about the electronic surveillance orders they receive, and if the statutes did so broadly restrict their speech, those statutes would be unconstitutional under the First Amendment.[10] The Department of Justice disagrees, and has been individually negotiating with companies about what they can and cannot say about the government demands they receive, leveraging statutory language that was intended to prohibit tipping off a target into what amounts to a *de facto* speech licensing scheme.

The Surveillance Transparency Act would put an end to this piecemeal system of prior restraint, clarifying what CDT and the companies believe to be the case already: that the general secrecy provisions of the FISA statute do not prohibit the disclosure of basic statistical information by companies that receive FISA process. Meanwhile, the Act's amendments would not change the fact that companies are prohibited from disclosing that they have received any particular surveillance demand regarding any particular person, or otherwise disclosing the identity of a target or the specifics of the targeted data to anyone, be it the suspect, a journalist, or the general public.

Such a restriction against tipping off a target is narrowly tailored to protect national security and prevent the disruption of particular investigations, at least while those investigations are ongoing. However, a general ban on any disclosure by a company that they have received any process under particular national security statutes is not so tailored, nor does it serve any legitimate—much less, compelling—national security interest, as I'll discuss more in a following section. Therefore, and as discussed at length in the amicus brief submitted to the FISA court by CDT and its allies, the secrecy provisions of the FISA are unconstitutional to the extent they impose such a broad gag.

---

[10] *See, e.g.*, the briefs of the movants, Google (http://www.uscourts.gov/uscourts/courts/fisc/misc-13-03-motion-130909.pdf), Microsoft (http://www.uscourts.gov/uscourts/courts/fisc/misc-13-04-microsoft-corporation-130909.pdf), Facebook (http://www.uscourts.gov/uscourts/courts/fisc/misc-13-06-motion-130909.pdf), Yahoo (http://www.uscourts.gov/uscourts/courts/fisc/misc-13-05-motion-130909.pdf), and LinkedIn (http://www.uscourts.gov/uscourts/courts/fisc/misc-13-07-motion-for-declaratory-judgement-LinkedIn-130917.pdf), and the briefs of *amici*, Dropbox (http://www.uscourts.gov/uscourts/courts/fisc/13-03-04-05-06-motion-dropbox-leave-130923.pdf) and Apple, Inc. (http://www.uscourts.gov/uscourts/courts/fisc/Misc-13-03-04-05-06-07-131105.pdf).

But again, neither we nor the companies petitioning the FISA court believe that the FISA statute's provisions actually require such a needlessly and unconstitutionally broad level of secrecy. Looking at similar language in the law enforcement surveillance statutes bolsters this conclusion. The secrecy provisions in FISA and in the federal wiretapping and pen register surveillance statutes used by law enforcement use essentially the same language.[11] Therefore, if the FISA statute prohibits the publication of aggregate surveillance data, so too do those law enforcement statutes. Yet a number of companies have been publishing such law enforcement data for years now, without the Justice Department or anyone else ever suggesting that they were not allowed to do so. And if they are allowed publish that data, then they are allowed to publish this data.

Importantly, and as the Reporters Committee for Freedom of the Press discusses in detail in its own amicus brief to the FISA court,[12] the fact that the government itself is now disclosing more information about its surveillance activities actually strengthens the companies' right to share their own perspective, rather than weakening it. The government choosing to speak on an issue does not and cannot preclude a private actor from speaking on the same issue. Rather, it is yet another demonstration of the fact that the companies' own accounts of what the government is describing constitute core political speech that goes to the heart of the First Amendment.

III. Greater Transparency is Necessary to Restore Trust in the US Internet Industry and the US Government.

In addition to the companies having a First Amendment right to speak, and we the people having a right to hear what those willing speakers have to say, we also all have a shared interest in restoring the trust in the US Internet industry that has been lost as a result of the NSA's surveillance programs, the secrecy surrounding

---

[11] *Compare, e.g.*, 50 U.S.C. § 1805(c)(2)(B) of FISA (in response to a FISA electronic surveillance order, the specified communications provider shall "furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier...is providing that target of electronic surveillance") and 18 U.S.C. § 2518(4) of the federal wiretap statute (in response to a wiretap order, the specified communications provider "shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider... is according the person whose communications are to be intercepted.").

[12] RCFP's amicus brief is available at http://www.uscourts.gov/uscourts/courts/fisc/misc-13-02-04-brief-of-amici-curiae-130715.pdf.

them, and the reporting (and in some cases misreporting) of the nature and scope of those programs.

The international outcry over the NSA's activities is substantial, and has doubtlessly impacted the competiveness of US Internet companies that serve international users. A study by the Information Technology & Innovation Foundation in the beginning of August—when much about the NSA's activities was still unreported—predicted that the US cloud computing industry stands to lose $22 to $35 billion over the next three years in response to the NSA scandal.[13] Forrester Research, building on the work of ITIF, concluded that the damage could be much greater, as high as $180 billion, or a quarter of all information technology service provider revenues in the same timeframe.[14] Internet industry leaders like Mark Zuckerberg of Facebook are warning that international users of US services are losing trust in US Internet companies,[15] and US telecommunications providers like AT&T are already seeing the NSA scandal interfere with their international business dealings.[16] Meanwhile, some European policymakers are threatening to revoke the "safe harbor" agreement that allows US companies to process the personal data of European users,[17] while a number of international leaders are discussing how to avoid the use of American services and to provide for—or require—the localization of Internet data and services.[18]

Congress needs to act quickly to remedy this growing trust gap that threatens the future of our Internet economy, and to allow the affected companies themselves to

---

[13] *See* Daniel Castro, *The Information Technology & Innovation Foundation*, "How Much Will PRISM Cost the US Cloud Computing Industry", August 5, 2013, at http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry.

[14] *See* James Staten, *Forrester Research Inc.*, "The Cost of PRISM Will Be Larger Than ITIF Projects", August 14, 2013, at http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

[15] *See* Alina Selyukh, *Reuters*, "Facebook's Zuckerberg Says US Spying Hurt Users' Trust", September 18, 2013, at http://mobile.reuters.com/article/technologyNews/idUSBRE98H19P20130918.

[16] See Anton Troianovski, Thomas Gryta and Sam Schechner, *Wall Street Journal*, "NSA Fallout Thwarts AT&T", at http://online.wsj.com/news/articles/SB10001424052702304073204579167873091999730 (describing how AT&T is facing intense scrutiny of its proposed acquisition of European wireless carrier Vodaphone in response to AT&T's collaboration with the NSA).

[17] Alex Byers, *Politico Morning Tech*, "Tech 'Safe Harbor' Under Fire in Europe", November 6, 2013, at http://www.politico.com/morningtech/1113/morningtech12137.html.

[18] See Leslie Harris, *Center for Democracy & Technology*, "Don't Gerrymander the Internet", November 4, 2013, at https://www.cdt.org/commentary/don%E2%80%99t-gerrymander-internet.

directly speak to and rebuild trust with their users about how they respond to the US government's demands for user data. Such transparency, in addition to serving the economic interest of the United States and helping to protect the constitutional rights of American companies and the American people, also and importantly helps to promote and preserve the human rights of all people who use the Internet.[19] As an international leader in the promotion of "Internet Freedom" as a human rights imperative, the US must also be a leader when it comes to transparency around Internet surveillance—and, to the extent that transparency reveals abuse, a leader in surveillance reform.

IV. The Level of Transparency Provided By The Surveillance Transparency Act Will Not Harm National Security.

The level of transparency that the Surveillance Transparency Act requires of the government and allows for the recipients of national security-related legal process will serve all of the purposes outlined above. What it will not do is harm national security. Basic statistics about the number of requests issued under particular legal authorities and the number of people affected, published once every six months in aggregate, do not provide nearly enough information to our adversaries to tip off any particular targets that they are being surveilled.

This conclusion is borne out by looking at the surveillance reporting that is done in the law enforcement context. The statutorily required reports on law enforcement wiretapping that have been issued every year for decades are incredibly detailed, and include:

- the specific number of wiretap orders issued in each federal court district and in each county of each state;
- the particular types of crimes being investigated;
- whether the surveillance targeted oral, telephonic, or electronic communications, or some combination;
- whether the wiretap targeted a business, a residence, or a mobile device,
- the length of the wiretaps;
- the cost of the wiretaps;
- the number of persons and communications intercepted by the wiretaps, and how many of those communications were incriminating;
- how often those wiretaps led to arrests or convictions;
- and more.

---

[19] *See, e.g.*, Open Society Foundations, "The Global Principles on National Security and the Right to Information (The Tshwane Principles)", June 12, 2013, pp. 25-26, at http://www.opensocietyfoundations.org/briefing-papers/understanding-tshwane-principles (describing international human rights-based principles on the public's right to information on national security matters, including the principle that "The public should also have access to information about entities authorized to conduct surveillance, and statistics about the use of such surveillance.").

Meanwhile, since Google first began issuing transparency reports in 2010, a growing number of Internet companies have been publishing detailed statistics on the law enforcement process they receive, including how many of each type of order they receive, how many of those they comply with, how many users are affected, and how many of those requests seek communications content or non-content records.[20]

Yet no one has ever suggested, much less demonstrated, that this wealth of information about law enforcement wiretapping has ever harmed any criminal investigation, tipped off a target, or given organized crime a leg up when trying to evade the law. Nor has anyone explained why the result would be any different when discussing national security surveillance. Knowing that the government is surveilling someone, and knowing that the government is surveilling someone in particular, are two very different things. And just as the law enforcement reports aren't enough to alert even a sophisticated criminal organization that it has been successfully targeted, the reporting proposed by the Surveillance Transparency Act—which is much less granular than what exists in the law enforcement context—would not alert even a sophisticated terrorist cell or spying ring that it has been targeted. Indeed, because there are even more targets of federal national security wiretaps than there are federal law enforcement wiretaps, the identity of any particular national security target is that much more indeterminate.[21]

Based on the US government's brief to the FISA court in response to the companies' motions seeking permission to publish meaningful FISA statistics,[22] the Intelligence Community's security concerns about enhanced transparency reporting by companies fall into two basic categories. First, there is the concern that allowing more detailed reporting will reveal which services are not currently being surveilled by the US government. However, it has always been the case that companies that have not received secret national security demands can say that they have not received secret national security demands; no matter how broad the secrecy requirements in the statutes may be, they don't reach parties who have not received a demand under those statutes. This simple fact was most recently demonstrated just last week, when Apple revealed in its first transparency report that is has never received an order to produce records under Section 215 of the USA PATRIOT Act.[23]

---

[20] *See* http://www.google.com/transparencyreport/ for Google's transparency reports as well as links to the reports of other companies including Apple, Dropbox, Facebook, LinkedIn, Microsoft, Twitter, and Yahoo.

[21] For example, the federal courts authorized 1,354 wiretap orders in 2012, compared to the 1,788 FISA court orders for electronic surveillance authorized under 50 U.S.C. § 1807. *See supra* n. 7 for links to the relevant reports.

[22] The government's brief is available at http://www.uscourts.gov/uscourts/courts/fisc/motion-declaratory-judgement-131002.pdf.

[23] *See* Apple Inc.'s "Report on Government Information Requests", November 5, 2013, at http://www.apple.com/pr/pdf/131105reportongovinforequests3.pdf

The second concern voiced by the government is that company reporting will reveal when the government is investigating users of particular services. However, this concern rings hollow when top intelligence officials repeatedly announce in public the names of various services that they believe terrorists are using. For example, current NSA Director Keith Alexander stated in written testimony to the Senate Judiciary Committee just last month that "[t]errorists...take advantage of familiar services: Gmail, Facebook, Twitter, etc.",[24] and in response to news reports has admitted that NSA obtains information from Google and Yahoo in terrorism investigations using court orders, as opposed to accessing those companies' servers directly.[25] Meanwhile, former NSA Director Michael Hayden recently proclaimed that Google's email service Gmail "is the preferred Internet service provider of terrorists worldwide."[26]

NSA directors past and present are rightly unconcerned about tipping off the terrorists that purportedly use Gmail, Facebook, Twitter, and Yahoo with their general statements. First, because any bad guys presumably already assume that each Internet service is being surveilled to some extent; second, because no bad guys can tell whether they in particular have been targeted yet—even if they already know from the companies' law enforcement reporting, or from Generals Alexander and Keith themselves, that the government routinely seeks information from a wide range of Internet services. Basic information about how the government is using its various surveillance authorities isn't of use to terrorists. It is, however, of great use to the American people and users of American Internet services who are trying to evaluate whether or not the US government's surveillance powers are being used in a reasonable and proportionate manner.

Put another way, if the government is using its authorities in a targeted way—even if the number of targets is large—being transparent about those numbers will not

---

("Apple has never received an order under Section 215 of the USA Patriot Act. We would expect to challenge such an order if served on us.").

[24] Opening Statement of Gen. Keith B. Alexander before the Senate Committee on the Judiciary (October 2, 2013), at http://www.judiciary.senate.gov/pdf/10-2-13AlexanderTestimony.pdf.

[25] Said Alexander, "We do not have access to Google servers, Yahoo servers. We go through a court order. We issue that court order to them through the FBI. And it's not millions. It's thousands of those that are done, and it's almost all against terrorism and other things like that." Denver Nicks, *TIME*, "NSA Chief Denies Agency Taps Google And Yahoo", October 30, 2013, at http://swampland.time.com/2013/10/30/nsa-chief-denies-agency-taps-google-and-yahoo/.

[26] Andrea Peterson, *The Washington Post*, "Former NSA and CIA director says terrorists love using Gmail", September 15, 2013, at http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/15/former-nsa-and-cia-director-says-terrorists-love-using-gmail/.

harm national security by tipping off any particular target. However, if those authorities are being used in an untargeted way to engage in bulk collection of data that implicates the privacy of most or all users of a service, then transparency about those numbers is all the more important because the people deserve to know.

This conclusion highlights a key purpose of transparency reporting about national security surveillance: it will not only reveal, but also help to prevent, improper use of surveillance authorities. For example, if the NSA knows that a demand for the records about millions of Google or Facebook users will be reflected in the company's next transparency report, it will likely only make such a demand if it is certain that Congress and the courts approve, that the demand is legal and constitutional, and that the demand is truly critical to protecting national security.

Transparency reporting isn't just an early warning system for detecting abuse; it is in itself an abuse prevention measure.

V. Transparency Reports Should Include Specific Numbers for Specific Authorities: No "Fuzzing" or "Lumping" of the Numbers is Necessary or Desirable.

Based on the Intelligence Community's individually negotiated agreements with specific companies such as Facebook and Microsoft,[27] and its arguments in front of the FISA Court,[28] we anticipate that the government's position will be that the new level of transparency promised by the DNI in August, in combination with piecemeal allowances for companies to publish a combined number for all law enforcement and national security surveillance requests rounded to the nearest thousand, is transparency enough.

First and foremost, such measures are insufficient because they are purely at the Executive Branch's discretion, and the Executive should not be the sole judge of how transparent it must be. Nor should transparency be the right only of those companies with the political clout necessary to successfully negotiate with the Justice Department or the legal budget necessary to mount a court challenge. We need a single, legislated solution, and as discussed earlier, one that respects both the companies' right to speak for themselves and the people's right to hear what they have to say.

Therefore, CDT—standing by what we and the coalition sought in our previous letters—opposes any "fuzzing" of the numbers, *i.e.*, requiring that numbers be rounded to the nearest hundred or thousand, or that they only be identified as a

---

[27] *See, e.g., Center for Democracy & Technology*, "CDT Applauds New Transparency from Microsoft and Facebook as Important Step, Calls for More Data", June 15, 2013, at https://www.cdt.org/pr_statement/cdt-applauds-new-transparency-microsoft-and-facebook-important-step-calls-more-data.

[28] *See supra* n. 22 for the government's brief to the FISA court.

range of numbers like 0 to 1000 or under 500. Similarly, we also oppose any "lumping "of those numbers, *i.e.*, requiring that the numbers regarding different surveillance authorities be combined into one.

As for the idea of lumping *all* of the various types of national security demands into one rounded number—or, even worse, lumping all of those demands in with all law enforcement demands—we believe that such a number would be essentially meaningless as a measure of how the government is using its surveillance authorities, and would be a substantial step back from what companies are already allowed to report.

Companies have a right to publish, and in some cases have already been publishing for years, detailed information about law enforcement demands. Several companies, with the permission of the Justice Department, have also already been publishing a rounded estimate of the number of National Security Letters that they receive.[29] And, as we and the companies have argued to the FISA court, those companies also have a right—that they are now seeking to vindicate—to publish statistics about the FISA process that they receive. Neither they nor the American people should have to trade away those strides in transparency that have already been made, in order to obtain the most basic, rudimentary information possible about the scope of government surveillance, especially when—as already discussed—the disclosure of more meaningful statistics would not harm national security.

Lumping all national security demands into a single number—mixing together targeted electronic surveillance of communications content under FISA, FISA pen register and trap and trace surveillance of non-content, year-long programmatic acquisition of foreign intelligence information under the FISA Amendments Act, FISA demands for records under USA PATRIOT Section 215, all the various types of National Security Letters, and even warrants for physical searches for FISA—serves no purpose but to obscure how specific authorities are being used.

Allowing only a single number—encompassing demands issued under different statutes that use different standards and procedures to authorize the acquisition of different types of data using different modes of surveillance—misses the entire point of such reporting, which is to allow the people to determine if and when a particular authority is incorrectly being used to obtain too much data, or to obtain the wrong kind of data, or to engage in the wrong type of surveillance. Adding all law enforcement requests into the mix makes the number even more useless, while also representing a significant step back from the level of transparency that companies have already achieved.

---

[29] For example, in 2012, Google received 0-999 National Security Letters seeking data regarding 1000-1999 users or accounts. *See* http://www.google.com/transparencyreport/userdatarequests/US/.

Put simply, asking the public and policymakers to judge the appropriateness of the government's surveillance practices based on a single, combined, rounded number is like asking a doctor to diagnose a patient's shadow. Only the grossest, most obvious problem—if even that—will ever be evident. Such deliberately obscured disclosures will also do little to restore the user trust that has been lost, as we've already seen. In June, with the permission of the Justice Department, the companies Apple, Facebook, Microsoft, and Yahoo all published single, combined numbers reflecting all national security and law enforcement requests.[30] Despite those months-old disclosures, the trust gap remains, and grows wider, with every new revelation about the NSA programs.

CDT therefore stands by and reiterates the request made in the coalition letter we signed: we strongly believe that Congress should authorize companies and require the government to publish statistics about the specific number of requests, and the specific number of persons affected, under each specific legal authority, along with a breakdown of how many requests sought communications content or non-content records.

CDT does not believe that any lumping or fuzzing of numbers is required to protect national security. However, if Congress ultimately disagrees, we would like to make clear that allowing for separate, rounded or ranged numbers for specific surveillance authorities—rounding within reason, and the smaller the range, the better—is far preferable to the forced combination of numbers for different surveillance authorities. We do not think, though, that forced fuzzing of large numbers, or forced fuzzing of numbers reported by service providers with a large number of users, serves any purpose. There is no meaningful difference from a national security perspective between saying—for example and hypothetically—that Dropbox received FISA orders requesting 153 customers' data and saying that it received requests for less than 500 customers' data. Nor is national security put at greater risk by saying that Microsoft received 1,433 National Security Letters instead of rounding that number to 1,400 or putting it in a range of 1,000 to 2,000. Either way, no suspect could ever conclude with any level of confidence that they had or had not been targeted.

Therefore we hope that any legislation, if it requires rounding or ranging of numbers at all, only imposes that requirement where the number of requests, or the number of users of the relevant service, or both, are very small. The First Amendment requires that we start with the presumption that the companies can speak. Any limitation on that right must be narrowly tailored to serve a compelling government purpose, and should not be based on vague intimations of potential danger or the automatic assumption that any meaningful level of transparency will harm national security.

---

[30] See Sam Gustin, *TIME*, "Tech Titans Press Feds in Battle Over NSA Transparency", September 10, 2013, at http://business.time.com/2013/09/10/tech-titans-press-feds-in-battle-over-nsa-transparency/.

VI. Suggested Improvements to the Bill

CDT strongly supports the Surveillance Transparency Act. However, in the spirit of making a good bill better, we offer a few suggestions on how it might be improved.

First, and consistent with our joint letter, we would prefer to see the bills reporting requirements and allowances include not only FISA authorities but National Security Letter authorities as well, powerful authorities that operate under a similar veil of secrecy. Notably, National Security Letter reporting is allowed in the transparency provisions of the USA Freedom Act sponsored by Chairman Leahy, who also was a cosponsor of this bill as originally introduced.

Also consistent with our joint letter and the positions stated above, CDT would prefer to see removed the provision in the Surveillance Transparency Act that would obscure the number of persons affected by a particular category of surveillance request when that number is less than five hundred. Barring that, we would prefer to see that number substantially reduced. Similarly, although it is not the subject of this hearing, we would prefer that the USA Freedom Act not require that the numbers it authorizes companies to publish be rounded to the nearest hundred. We do not think such fuzzing of the numbers is necessary to protect national security.

We also believe, consistent with our joint letter, that the government reporting required by the bill, and the company reporting authorized by the bill, should include reporting of the type of data sought—content or non-content—regardless of which authority is at issue or whether that data pertained to a US or non-US person. We do not think that limiting such reporting to certain categories of authorities or categories of persons is necessary to protect national security; we do think that such reporting is critical to ensuring that each authority is being used appropriately.

Similarly, CDT does not think that government reporting about how many US persons' data was obtained or reviewed should turn on which authority is at issue; it too should be required for each authority. Notably, the government is already required to provide such US-person numbers in its National Security Letter reporting;[31] it can and should do so for each of its surveillance powers, particularly where many of those powers depend on—or were justified based on—the distinction in treatment between US persons and non-US persons.

Speaking of the bill's requirement that the government report a good faith estimate of how many US persons' data were obtained or reviewed pursuant to particular authorities, we anticipate that the government will claim that it lacks the capacity to do so. We are very skeptical of this claim. The bill does not ask for an exact number but only a good faith estimate, and leading technical experts such as Princeton

[31] See the Justice Department letter reporting on 2012's FISA and National Security Letter numbers, *supra* n. 7.

professor Ed Felten, the former chief technologist for the Federal Trade Commission, have explained how such estimates are possible.[32] Just as the government relied on random sampling in litigation before the FISA court to determine a rough estimate of how many US person communications it obtained under Section 702 of the FISA Amendments Act,[33] and just as it uses a wide variety of presumptions in the targeting and minimization guidelines that govern its use of that authority in order to determine which communications likely belong to non-US persons outside of the country,[34] so too can it estimate how much of the information it collects belongs or pertains to US persons inside of the country. Although those guidelines are imperfect to say the least,[35] having demonstrably led to the overcollection of US person communications, they at the very least can provide a rough estimate that would be of use to the American people and policymakers.

We are certain that the NSA, the largest employer of mathematicians on the planet, can solve this problem. But if the NSA truly lacks the ability to distinguish in a meaningful way between the data and communications of US persons and those of non-US persons, then Congress' grant of broad surveillance powers that are justified by or depend on such ability must be revisited.

VII. Conclusion

Although we do recommend some changes, CDT and the coalition that signed our joint letter strongly support the Surveillance Transparency Act of 2013. We look forward to working with this Subcommittee, the full Judiciary Committee, and Congress as a whole to achieve passage not only of transparency reform measures such as the Surveillance Transparency Act but also of broader, substantive surveillance reforms such as those contained in the USA Freedom Act, to better ensure our nation's surveillance activities are fully consistent with constitutional principles and human rights. Thank you for your time and consideration.

---

[32] *See* Edward W. Felten's Responses to Questions for the Record, submitted on October 29, 2013 to the United States Senate Committee on the Judiciary, at http://www.judiciary.senate.gov/resources/documents/113thCongressDocuments/upload/100213QFRs-Felten.pdf.

[33] *See* the recently declassified FISA Court memorandum opinion of October 3, 2011 at pp. 32-35, at https://www.eff.org/document/october-3-2011-fisc-opinion-holding-nsa-surveillance-unconstitutional.

[34] *See* Glenn Greenwald and Tim Ball, *The Guardian*, "The Top Secret Rules That Allow The NSA to Use US Data Without a Warrant", June 20, 2013, at http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant (publishing the FAA targeting and minimization guidelines).

[35] *See* Kurt Opsahl and Trevor Timm, *Electronic Frontier Foundation*, "In Depth Review: New NSA Documents Expose How Americans Can Be Spied on Without A Warrant", June 21, 2013, at https://www.eff.org/deeplinks/2013/06/depth-review-new-nsa-documents-expose-how-americans-can-be-spied-without-warrant.

PREPARED STATEMENT OF PAUL ROSENZWEIG

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.

PREPARED STATEMENT OF RICHARD SALGADO

Google

Written Testimony of Richard Salgado
Director, Law Enforcement and Information Security, Google, Inc.
Senate Judiciary Subcommittee on Privacy, Technology and the Law
Hearing on "The Surveillance Transparency Act of 2013"
November 13, 2013

Chairman Franken, Ranking Member Flake, and members of the Subcommittee, thank you for the opportunity to appear before you this morning to discuss the Surveillance Transparency Act of 2013.

As the Director for Law Enforcement and Information Security at Google, I oversee the company's response to government requests for user information under various authorities. I am also responsible for working with teams across Google to protect the security of our networks and user data. I have served as a Senior Counsel in the Computer Crime and Intellectual Property Section in the Department of Justice, and have taught and lectured on these issues at Georgetown University Law Center, George Mason University Law School, and Stanford Law School.

In September, Google joined a diverse array of companies, trade associations, and civil society organizations to express strong support for the Surveillance Transparency Act of 2013. The signatories to this letter include AOL, Apple, Facebook, LinkedIn, Microsoft, Twitter, and Yahoo! — all of whom, like Google, believe that service providers should be permitted to disclose basic statistics about Foreign Intelligence Surveillance Act demands that they may receive.

We commend Chairman Franken for introducing, with Senator Heller, the Surveillance Transparency Act of 2013 and for the leadership he has shown on this important issue. Transparency can and should play a critical role in the broader debate around substantive reforms that would address concerns raised by the government's use of existing surveillance authorities.

In my testimony today, I will make four principal points:

- **First**, recent disclosures concerning the extent of government surveillance undermine confidence in Internet services reliant on user trust, create significant risks for economic security and growth, and threaten to jeopardize the current global Internet governance

structure. These disclosures, however, provide a unique opportunity to revisit existing surveillance laws.

- **Second,** Google has long been committed to increasing transparency around government demands for user data. Lumping domestic and national security requests together in ranges in our Transparency Report, as the DOJ has proposed, would be a significant step backward for our users and the general public, who would receive less information than we disclose in our current Transparency Report.

- **Third**, companies' right to publish aggregate statistics about the nature and scope of government surveillance programs promotes a more open dialogue about reform without jeopardizing national security. Transparency is an essential component to inform the debate over broader reforms to our surveillance laws, and efforts to prevent companies from publishing statistics about national security demands hinder the debate.

- **Fourth,** transparency is only one step among many needed. It can and should be a critical part of broader reforms with the goal of ensuring that government surveillance programs are rule-bound, narrowly tailored, transparent, and subject to oversight.

Transparency Can Help Restore Trust with Users and Governments and Inform the Broader Debate Around Comprehensive Reform

The revelations about the U.S. government's and other governments' surveillance practices over the past few months have sparked a serious debate about the need to revisit the laws governing surveillance of private communications by the intelligence community. Google recognizes the very real threats that the U.S. and other countries face today, and of course governments have a duty to protect their citizens. The current lack of transparency about the nature of government surveillance in democratic countries, however, undermines the freedoms most citizens cherish. It also has a negative impact on our economic growth and security and on the ultimate promise of the Internet as a platform for openness and free expression.

In the wake of press reports about the so-called "PRISM" program, governments around the world have been considering ways to limit the impact of the U.S. government's and other governments' surveillance on their citizens. One way that some governments are seeking to achieve this goal is by limiting the flow of information over the Internet between their country and the U.S. However, the free flow of data globally is critical to ever-expanding amounts of economic activity throughout the world, and limitations on that flow could have severe unintended consequences, such as a reduction in data security, increased costs, decreased competitiveness, and harms to consumers. And the impact on U.S. companies, and the broader U.S. economy, could be significant. Two

reports, for example, estimate that the effect on U.S. companies may be in the tens of billions or even hundreds of billions of dollars.

One concrete example that Google, other companies in numerous industries, and civil society are grappling with is the movement towards so-called "data localization," which has gained considerable traction since the revelation of the PRISM program. As we speak, the Brazilian Congress, for example, is considering legislation that would require data relating to the Brazilian operations of both domestic and international companies — as well as Brazilian citizens — to be stored in Brazil. Companies like Google that do not comply with such a requirement could be barred from doing business in one of the world's most significant markets or be obligated to pay hundreds of millions of dollars in fines.

The impact of the revelations goes beyond the economic losses cited. They come at a time when many governments and other stakeholders are increasingly critical of the role the U.S. has played in safeguarding the free and open Internet through its support of the multi-stakeholder governance model, a model where the Internet is not governed only by states, but through institutions comprised of civil society, business, government and users. Today, calls for the Internet to be regulated by the U.N.-chartered International Telecommunications Union or other United Nations institutions and put solely under government control are louder than ever. At last month's Internet Governance Forum, a gathering of key Internet stakeholders in Bali, calls for limiting the role of the U.S. were significant and accompanied by proposals now under consideration.

These trends, both within individual countries and in broader international forums, pose a significant threat to the free and open Internet that we benefit from today. If data localization and other efforts are successful, then what we will face is the effective Balkanization of the Internet and the creation of a "splinternet" broken up into smaller national and regional pieces with barriers around each of the splintered Internets to replace the global Internet we know today.

Committing to more transparency by enacting the Surveillance Transparency Act would allow the U.S. to take a first step towards rebuilding trust. It would do so by clarifying for all stakeholders the number and nature of national security-related orders that companies like Google may receive, if any. If Google, for example, could publish those numbers as Google and other service providers have proposed — and as Chairman Franken's bill would allow — our users and the broader public would have a better understanding of our posture in response to any national security demands that we may receive, as well as the volume, scope, and type of such demands that we may receive.

Publishing the number of demands by legal authority and the number of users or accounts impacted would go a long way to putting the relationship between U.S.-based companies and the U.S. government into a more accurate perspective. And as I note later on in my testimony, we

believe that transparency is a critical part of the broader set of reforms that are needed in order to address the issue of government surveillance of the world's communications networks.

Google Has Long Been Committed to the Principle of Transparency as Part of Broader Efforts to Reform Surveillance Laws

Our interest in providing more transparency around government requests for user data long preceded the recent revelations about the government's use of its surveillance authorities. In 2010 we issued our first Transparency Report regarding requests for user data going back to 2009. The goal was to provide useful information to our users and the general public about such requests that we receive from governmental entities throughout the world. We were the first company to publish such data, and we applaud other companies that have released transparency reports.

We release our Transparency Report on a biannual basis, and we strive to surface new and useful information and data with each iteration. For example, for the second half of 2012, we broke down legal requests in the U.S. by type *(i.e.*, subpoena, search warrant, and other requests) for the first time, shedding more light on the nature of the information sought by governmental entities in the U.S. And, earlier this year, after long negotiations with the DOJ, we began providing more information about the volume and scope — albeit in broad ranges — of National Security Letters that we receive.

Transparency helps our users understand our practices, and it allows us to correct inaccurate characterizations of our posture in response to national security demands that we may receive. For instance, contrary to some initial media accounts, Google has not given the U.S. government or any other government access to Google's servers. Google refuses to participate in any program that requires it to provide the U.S. government or any other government with access to its systems or to install their equipment on Google's networks.

Transparency Reports Promote Reform Without Jeopardizing Security

Earlier this year, Google approached the DOJ about including aggregated statistics reflecting requests Google may receive under FISA as part of its normal transparency reporting cycle. Unfortunately, the DOJ refused, and has taken the position that providers cannot even acknowledge receipt of FISA orders, let alone publish aggregate statistics around national security demands that they may receive.

There are important First Amendment principles at stake. The DOJ's position that service providers can't publish data concerning national security demands is a prior restraint on speech.

Prior restraints, as the Supreme Court has held, carry a heavy presumption against constitutional validity under the First Amendment. Moreover, any blanket prohibition on the ability of providers to speak about national security demands that they may receive is a content-based restriction on speech. Like prior restraints, content-based restrictions are heavily disfavored. The government has to show that the prohibition on speech is narrowly tailored to support a compelling governmental interest; that is, that there are no less restrictive alternatives that would be at least as effective in achieving the government's objectives.

Accordingly, Google filed a Motion for Declaratory Judgment before the Foreign Intelligence Surveillance Court in June asserting a First Amendment right to publish statistics regarding Google's receipt of various national security demands, if any. We subsequently amended our Motion, seeking permission to publish the total number of compulsory requests we may receive under various national security authorities and the total number of users or accounts that may be impacted by each category of request.

In its heavily redacted Response and accompanying Declaration to our Motion for Declaratory Judgement before the FISC, the DOJ reiterated that it would only allow companies to combine domestic law enforcement and national security demands together. Lumping domestic law enforcement and national security demands together, however, would be a significant step backward for Google's users and the broader public.

The DOJ's proposal would limit Google to reporting law enforcement and national security demands, if any, in a single range. Rather than promote transparency, this proposal would obscure important information about the volume and type of *all* government requests that Google may receive, not just national security demands. Google already discloses aggregate statistics about domestic law enforcement demands that we receive. As noted above, we have done so since 2010. Publishing future Transparency Reports where we could release this information only in ranges (rather than disclosing actual numbers) would provide less transparency.

In addition to masking information about domestic law enforcement demands that Google receives, there would be no discernible benefit for transparency around national security demands that we may receive. Reporting domestic law enforcement and national security demands together would only invite speculation about the import of the range reported and would yield no information whatsoever about any national security demands that we may receive. Indeed, Google would be prohibited from even acknowledging receipt of national security demands, if any, including NSLs, which we currently disclose in our Transparency Report.

Transparency and national security are not mutually exclusive. There has been no intimation from law enforcement that the data we've published so far has tipped off organized crime or caused

other individuals suspected of criminal activity to gravitate to other services. The Department of Justice has likewise given no signs that the publication of ranges of NSLs we receive has had such effects for terrorists. Indeed, the number of government requests that we receive in the U.S. as reflected in the Transparency Report has increased substantially since we first published our Transparency Report, suggesting that there is no correlation between transparency and hinderance of investigations. Google is not seeking to disclose the targets or substance of any national security demands that we may receive. Nor are we seeking to acknowledge national security demands contemporaneous with their receipt or to disclose sources and methods.

In light of these facts, publishing aggregated statistics around other foreign intelligence demands that we may receive would not damage national security investigations. We believe Google and other companies have a First Amendment right to publish basic, aggregate statistics about the volume, scope, and type of national security demands that we may receive. In a democratic society, the government simply cannot be the sole arbiter of who gets to speak and what they may say on issues of paramount national importance. The right to speak about such weighty matters of public interest is not and should not be the exclusive province of the intelligence community.

In Addition to Transparency, Congress Should Consider Broader Reforms to Surveillance Laws

Transparency is a critical step in informing the broader public about the extent to which covered entities are compelled to provide user data in response to national security demands. It is clear, however, that governments, both in the U.S. and abroad, must examine broader reforms to government surveillance programs that threaten to erode confidence in the privacy and security of data that is entrusted to covered entities.

We can start with fixing our domestic surveillance laws. Google strongly supports legislation that would update the Electronic Communications Privacy Act to require a warrant in all instances where governmental entities want to obtain the content of users' communications. This is the core goal of both S. 607, the Electronic Communications Privacy Act Amendments Act of 2013, bipartisan legislation sponsored in the Senate by Senators Leahy and Lee, and H.R. 1852, the Email Privacy Act, sponsored by Representative Yoder and cosponsored on a strongly bipartisan basis by over 140 members of the House. Each of the bills would update ECPA by creating a bright line, warrant-for-content standard. We urge Congress to pass ECPA reform as soon as possible, and to resist efforts to include carve-outs and exceptions that would whittle away at this bright line, warrant-for-content standard and contravene users' reasonable expectations of privacy.

Also, agreements like Mutual Legal Assistance Treaties guarantee that standards for due process are met and offer a consistent framework for expedient mutual assistance in investigations that

cross borders. Where countries other than the country in which a company is headquartered require user data and it is legally justified, MLAT can provide the right framework for law enforcement cooperation. More can and should be done to significantly improve efficiency and ease of use of the MLAT process.

With respect to broader reform of surveillance laws and practices, Google, AOL, Apple, Facebook, LinkedIn, Microsoft, and Yahoo! recently voiced support for broader FISA reforms that would include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for FISA surveillance.

In the letter we stated:

> As companies whose services are used by hundreds of millions of people around the world, we welcome the debate about how to protect both national security and privacy interests and we applaud the sponsors of the USA Freedom Act for making an important contribution to this discussion… Transparency is a critical first step to an informed public debate, but it is clear that more needs to be done. Our companies believe that government surveillance practices should also be reformed to include substantial enhancements to privacy protections and appropriate oversight and accountability mechanisms for those programs.

We also strongly believe that governments throughout the world must revisit laws and practices governing surveillance of individuals and access to their information.

* * * * *

Google looks forward to working with this Subcommittee, the full Judiciary Committee, and Congress as a whole on the Surveillance Transparency Act of 2013 and other reform measures that ensure national security authorities are utilized in a way that is rule-bound, narrowly tailored, transparent, and subject to oversight.

Thank you for your time and consideration.

QUESTIONS SUBMITTED BY SENATOR LEAHY FOR KEVIN BANKSTON

QUESTIONS FOR THE RECORD – Chairman Leahy
11/13/13 – Surveillance Transparency Act Hearing

Questions for Kevin Bankston

1. Your written testimony argues that companies' First Amendment rights are violated when they are not permitted to speak publicly about the numbers of surveillance orders they have received and complied with. Is this a prior restraint? Does that argument have support from the Second Circuit precedent striking down the nondisclosure order provisions governing National Security Letters?

QUESTIONS SUBMITTED BY SENATOR FLAKE FOR PAUL ROSENZWEIG

Written Questions of Senator Jeff Flake
"The Surveillance Transparency Act of 2013"
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
November 20, 2013

Professor Paul Rosenzweig

1. In your testimony before the subcommittee, you stated you supported having an advocate appear before the Foreign Intelligence Surveillance Courts, but only if it would not cause procedural difficulties, be adverse to national security, or result in time delays. Do you have any concern that S. 1467, one of the proposals to create a special advocate, could cause procedural difficulties, be adverse to national security, or result in time delays?

RESPONSES OF KEVIN BANKSTON TO QUESTIONS SUBMITTED BY SENATOR LEAHY

RESPONSE TO QUESTION FOR THE RECORD
KEVIN BANKSTON, POLICY DIRECTOR
NEW AMERICA FOUNDATION'S OPEN TECHNOLOGY INSTITUTE
11/13/13 – SURVEILLANCE TRANSPARENCY ACT HEARING[1]

Response to question for the record from Chairman Leahy to Kevin Bankston:

1. **Your written testimony argues that companies' First Amendment rights are violated when they are not permitted to speak publicly about the numbers of surveillance orders they have received and complied with. Is this a prior restraint? Does that argument have support from the Second Circuit precedent striking down the nondisclosure order provisions governing National Security Letters?**

Yes, companies' First Amendment rights are violated when they are not permitted to speak publicly about the numbers of surveillance orders they have received and complied with, and yes, this is a prior restraint, and yes, that argument has support from the Second Circuit precedent striking down the nondisclosure order provisions governing National Security Letters (NSLs). In that case, *Doe v. Mukasey*, 549 F.3d 861 (2nd Cir. 2008), the court treated as a prior restraint the NSL statute's ban on any disclosure by NSL recipients about the fact that they have received NSLs, by finding that the statute failed to satisfy the procedural requirements for prior restraints established by the Supreme Court in *Freedman v. Maryland*, 380 U.S. 51 (1965).

Indeed, the same concerns about Executive discretion to censor without adequate procedural safeguards that animated the *Freedman* decision apply to the Justice Department's *ad hoc* negotiated agreements with Internet companies regarding secret surveillance requests, whereby *some* companies are allowed to publish *some* statistics about *some* national security-related requests under the Foreign Intelligence Surveillance Act (FISA) or NSL statutes. For example, the Justice Department has allowed Google and Twitter to publish the annual number of NSLs that they receive—but not the number of FISA requests they receive—rounded to the nearest thousand, while allowing Microsoft and Facebook to publish the annual number of all requests that they receive (regular law enforcement, plus all FISA process, plus NSLs), but only if combined into a single number that is also rounded to the nearest thousand. These Executive decisions, about which companies are allowed to report which numbers and whether and how those numbers must be combined or rounded, essentially amount to a *de facto* speech licensing scheme that occurs without any procedural safeguards at all, much less a prior court review weighing the companies' First Amendment interests: a classic prior restraint.

In my capacity as the Free Expression Director at the Center for the Democracy & Technology, I was one of several lawyers representing a number of free speech organizations as *amici* before

[1] At the time of the hearing on 11/13/13, Bankston was testifying in his previous capacity as the Free Expression Director and Senior Counsel of the Center for Democracy & Technology.

the FISA court, writing in support of the companies' motion for declaratory judgment that they have a First Amendment right to engage in basic transparency reporting about the numbers and kinds of FISA court requests that they receive. That brief, attached and also available at http://www.uscourts.gov/uscourts/courts/fisc/misc-13-03-misc-13-04-brief-130708.pdf, addresses the relevant First Amendment issues at greater length, concluding at pp. 8-9 that "the nature of the [FISA disclosure] restrictions is that of a prior restraint" and reiterating how such a restraint is "the most serious and least tolerable infringement on First Amendment rights." The brief also discusses at p. 11 how the *Doe v. Mukasey* decision and other case law regarding the NSL statute's gag provisions support that conclusion.

UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT
WASHINGTON, D.C.

IN RE MOTION FOR DECLARATORY JUDGMENT OF GOOGLE INC.'S FIRST AMENDMENT RIGHT TO PUBLISH AGGREGATE INFORMATION ABOUT FISA ORDERS.	Docket No. Misc. 13-03
IN RE MOTION TO DISCLOSE AGGREGATE DATA REGARDING FISA ORDERS	Docket No. Misc. 13-04

BRIEF OF FIRST AMENDMENT COALITION, AMERICAN CIVIL LIBERTIES UNION, CENTER FOR DEMOCRACY AND TECHNOLOGY, ELECTRONIC FRONTIER FOUNDATION, AND TECHFREEDOM AS *AMICI CURIAE* IN SUPPORT OF THE MOTIONS FOR DECLARATORY JUDGMENT

Floyd Abrams
Dean Ringel
Philip V. Tisne
CAHILL GORDON & REINDEL LLP
80 Pine Street
New York, New York 10005-1772
(212) 701-3000
Attorneys for Amici Curiae

July 8, 2013

TABLE OF CONTENTS

page(s)

TABLE OF AUTHORITIES ii

STATEMENT OF AMICI 1

DESCRIPTION OF THE AMICI 1

ARGUMENT 2

A. *The First Amendment Imposes a Heavy Burden on Any Effort To Bar Disclosure Here* 2

B. *First Amendment Principles Have Barred Overbroad Non-disclosure Rules in the Context of National Security* 11

TABLE OF AUTHORITIES

Cases *page(s)*

Alexander v. *United States*,
509 U.S. 544 (1993) 9

Bartnicki v. *Vopper*,
532 U.S. 514 (2001) 7

Butterworth v. *Smith*,
494 U.S. 624 (1990) 8

Citizens United v. *Federal Election Commission*,
558 U.S. 310 (2010) 5

Consolidated Edison Co. of New York, Inc. v. *Public Service Commission of New York*, 447 U.S. 530 (1980) 6

First National Bank of Boston v. *Bellotti*,
435 U.S. 765 (1978) 6

The Florida Star v. *B.J.F.*,
491 U.S. 524 (1989) 7

Garrison v. *State of Louisiana*,
379 U.S. 64 (1964) 6

In re Grand Jury Proceedings,
814 F.2d 6 (1st Cir. 1987) 8

In re Grand Jury Subpoena,
574 F. Supp. 85 (S.D.N.Y. 1983) 8

Hamdi v. *Rumsfeld*,
542 U.S. 507 (2004) 10

Holder v. *Humanitarian Law Project*,
130 S. Ct. 2705 (2010) 10

Home Building & Loan Ass'n v. *Blaisdell*,
290 U.S. 398 (1934) 10

John Doe, Inc. v. *Mukasey*,
549 F.3d 861 (2d Cir. 2008) 11

Ex parte Milligan,
71 U.S. 2 (1803).....10

Mills v. *Alabama*,
384 U.S. 214 (1971).....6

In re National Security Letter,
No. C 11-02173 (SI), 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013).....11

Nebraska Press Ass'n v. *Stuart*,
427 U.S. 539 (1976).....9

New York Times Co. v. *Sullivan*,
376 U.S. 254 (1964).....5

New York Times Co. v. *United States*,
403 U.S. 713 (1971).....9

Police Department of City of Chicago v. *Mosley*,
408 U.S. 92 (1972).....7

Procunier v. *Martinez*,
416 U.S. 396 (1974).....7

Richmond Newspapers, Inc. v. *Virginia*,
448 U.S. 555 (1980).....9, 10

Roth v. *United States*,
354 U.S. 476 (1957).....5, 6

Seattle Times Co. v. *Rhinehart*,
467 U.S. 20 (1984).....7

Snepp v. *United States*,
444 U.S. 507 (1980).....7

Snyder v. *Phelps*,
131 S. Ct. 1207 (2011).....6

United States v. *Aguilar*,
515 U.S. 593 (1995).....7

United States v. *Morison*,
844 F.2d 1057 (4th Cir. 1988).....5

United States v. *New York Times Co.*,
328 F. Supp. 324 (S.D.N.Y. 1971) 5

United States v. *Playboy Entertainment Group, Inc.*,
529 U.S. 803 (2000) 9

Statutes

Electronic Communications Act, Pub. L. No. 99-508, 100 Stat. 1848
(1986) 11

U.S.A. PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) 11

Other Authorities

Caleb Garling, *Firms Seek to Explain to Users; Tech Surveillance; Some Companies Urge Government Agencies to Allow Transparency*, SAN FRANCISCO CHRONICLE, June 18, 2013 7

Clarence Page, *Secrecy Scandal? Not So Much, Really*, CHICAGO TRIBUNE, June 12, 2013 2

Editorial, *President Obama's Dragnet*, N.Y. TIMES, June 7, 2013 2

Oversight of the Federal Bureau of Investigation (FBI): Hearing Before the H. Judiciary Comm., 113th Cong. 47 (June 13, 2013) 3

Jessica Guynn, *Tech Firms Try to Regain Trust; Apple is the Latest to Try to Reassure Public That It Didn't Give U.S. Direct Access to Data*, LOS ANGELES TIMES, June 18, 2013 7

Matthew DeLuca & Kasie Hunt, *NSA Snooping Has Foiled Multiple Terror Plots: Feinstein*, NBC NEWS, June 6, 2013 3

Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary, 113th Cong. (June 19, 2013) 3

Robert H. Bork, *Neutral Principles and Some First Amendment Problems*, 47 IND. L.J. 1, 27-28 (1971) 6

Statement by the President, Office of the Press Secretary (June 7, 2013) 3

Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 879 (1963) 7

Zechariah Chafee Jr., FREE SPEECH IN THE UNITED STATES (1967) 7

STATEMENT OF AMICI

Amici are public interest organizations dedicated to the preservation of civil liberties. They respectfully submit this brief to set forth their views as to the special impact of the First Amendment's protection of free expression on the resolution of the motions filed by Google, Inc. ("Google") and Microsoft Corporation ("Microsoft") seeking declaratory judgments confirming their ability to disclose limited numerical information in aggregate form as to requests that each may have received from the government pursuant to the Foreign Intelligence Surveillance Act ("FISA").

DESCRIPTION OF THE AMICI

Amicus First Amendment Coalition ("FAC") is a section 501(C)(3) nonprofit organization dedicated to First Amendment freedoms—primarily freedom of speech and the press—and government transparency. Founded in 1988, FAC works to enhance and protect these rights through a free legal consultation service, educational and information services, public advocacy of various kinds, and litigation, including the initiation of litigation in its own name and the filing of briefs *amicus curiae*. FAC receives support from foundations and from its members, who include individuals and corporations.

Amicus American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's civil-rights laws. Since its founding in 1920, the ACLU has appeared before the federal courts as direct counsel and as *amicus curiae* in numerous cases involving the First Amendment. It has also appeared before this Court on several occasions.

Amicus Center for Democracy & Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other com-

munications networks, and associated technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

Amicus Electronic Frontier Foundation ("EFF") is a member-supported organization dedicated to protecting civil liberties in the digital world. Founded in 1990, EFF fights to ensure that the rights and freedoms we enjoy are enhanced as our use of technology grows. EFF has filed actions and has appeared before this Court and also advocates for greater transparency about government requests for user information.

Amicus TechFreedom is a nonprofit, nonpartisan public policy think tank. Its work on a wide range of information technology policy issues rests on a belief that technology enhances freedom and freedom enhances technology. TechFreedom has been involved in debates over both free speech and privacy and believes that restrictions on the flow of information, whether to protect national security or to achieve some other state interest, must be reconciled with the speech interests burdened by regulation.

All parties have consented to the filing of this brief *amici curiae*.[1]

ARGUMENT

A. THE FIRST AMENDMENT IMPOSES A HEAVY BURDEN ON ANY EFFORT TO BAR DISCLOSURE HERE

The Google and Microsoft motions arise in the context of an ongoing national debate about the nature and extent of government surveillance intended to protect national security. There is widespread national interest in the topic, *compare, e.g.*, Editorial, *President Obama's Dragnet*, N.Y. TIMES, June 7, 2013, *with* Clarence Page, *Secrecy Scandal? Not So Much, Really*,

---

[1] *Amici* certify that no counsel for a party authored this brief in whole or in part, and no person or entity other than *amici curiae* or their counsel made a monetary contribution to its preparation or submission.

CHICAGO TRIBUNE, June 12, 2013, which is reflected in acknowledgment by the highest officials of the Executive branch and Congressional leaders of both parties that a robust national debate about that subject is appropriate.[2] The President has emphasized the need for such a debate: "I welcome this debate. And I think it's healthy for our democracy. I think it's a sign of maturity, because probably five years ago, six years ago, we might not have been having this debate." Statement by the President, Office of the Press Secretary (June 7, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president. Similarly Republican Senator Charles E. Grassley has observed that "open and transparent discussion of these programs is the only way that the American people will have confidence in what their government's doing." *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (June 19, 2013) (stmt. of Sen. Charles E. Grassley).

Yet even basic facts of central relevance in this debate are unknown and currently unknowable to the public, facts ranging from how extensive the government surveillance programs are to how many users or accounts they affect. It is against this backdrop that Google and Microsoft now seek to disclose (1) the number of FISA requests that each may have received and (2) the number of users or accounts encompassed within any such requests. Google and Microsoft have each filed motions seeking a declaration from this Court that they are not prohibited

---

[2] *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (June 19, 2013) (stmt. of Sen. Leahy) ("We have to have an open debate about the efficacy of these tools, particularly, in light of the Boston marathon bombing in April, not only [] how we collect them, but what we do with it once it's [collected]."); *Oversight of the Federal Bureau of Investigation (FBI): Hearing Before the H. Judiciary Comm.*, 113th Cong. 47 (June 13, 2013) (stmt. of Rep. Jeffries) ("But it is clear that he has become a lightning rod that has sparked what I think is a very important debate in this country that we in the Congress should have as to the proper balance between legitimately held security concerns and concerns for privacy and liberty, which are essential to the preservation of our democracy."); Matthew DeLuca & Kasie Hunt, *NSA Snooping Has Foiled Multiple Terror Plots: Feinstein*, NBC NEWS, June 6, 2013, *available at* http://usnews.nbcnews.com/_news/2013/06/06/18796204-nsa-snooping-has-foiled-multiple-terror-plots-feinstein?lite ("We are always open to changes. But that doesn't mean there will be any. It does mean that we will look at any ideas, any thoughts, and we do this on everything." (quoting Sen. Feinstein)).

from doing so. *See* Br. at 4, *In re Motion for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders*, No. Misc. 13-03 (June 18, 2013) ("Google Br."); Br. at 4, *In re Motion to Disclose Aggregate Data Regarding FISA Orders*, No. Misc. 13-04 (June 19, 2013) ("Microsoft Br."). Both companies state that they would publish this data in a way that would not allow "any particular individual user to infer that he or she had been targeted." Microsoft Br. at 5; *see also* Google Br. at 4.

Amici submit this brief in support of those motions. Google asserts that "no applicable law or regulation" bars it from making the disclosures it seeks to make. *See* Google Br. at 4; *see also* Microsoft Br. at 4. *Amici* also are not aware of any such bar but recognize that they have more limited information as to the procedures and rules applicable to the applications of the government and the rules of this Court and so do not address that issue as such. Instead, we aim (1) to highlight the fundamental First Amendment interests implicated by any rule, whatever its origin, that prohibits the disclosures that Google and Microsoft seek to make here; and (2) to emphasize the very heavy burden that the proponent of any such rule would have to sustain in light of the First Amendment's requirements.

Any rule precluding disclosure as to what a party itself is asked to do bears an extremely high burden of justification under broad principles protecting free expression even where the non-disclosure might be sought in service of national security. And those principles have, in fact, been applied in the closely related "National Security Letter" context to determine that even an explicit statutory prohibition on far more specific disclosures than those at issue here was unconstitutional. We write to put both these general principles and their specific application in this context before this Court. *Amici* believe that these First Amendment principles, when applied to the limited proposed disclosures—disclosures central to an ongoing national debate—argue strongly for the grant of the declaratory relief being sought.

In making this argument, we are not insensitive to concerns for national security. But even those important concerns do not easily, let alone routinely, trump the First Amendment. *See, e.g.*, *United States* v. *Morison*, 844 F.2d 1057, 1081 (4th Cir. 1988) (Wilkinson, J., concurring) ("The First Amendment interest in informed popular debate does not simply vanish at the invocation of the words 'national security'"). As Judge Gurfein recognized many years ago in his ruling in the Pentagon Papers case, "[t]he security of the Nation is not at the ramparts alone [but] also lies in the value of our free institutions." *United States* v. *New York Times Co.*, 328 F. Supp. 324, 331 (S.D.N.Y. 1971).

The "free institution" at risk here is nothing less than the guarantee of free expression contained in the First Amendment. The expression at issue on the present motions—speech by Google and Microsoft about their own conduct in responding to any government requests—is central to a significant political debate at the heart of self-government. It implicates the most fundamental First Amendment values and should yield only to a government interest of the highest order subjected to the most searching judicial inquiry. The government's burden is a heavy one, as both broad principles of First Amendment law and narrower decisions issued in strikingly similar national security contexts make clear.

The First Amendment embodies "a profound national commitment" to the principle that "debate on public issues should be uninhibited, robust, and wide-open," *New York Times Co.* v. *Sullivan*, 376 U.S. 254, 270 (1964), and that Amendment was "fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes," *Roth* v. *United States*, 354 U.S. 476, 484 (1957). Nowhere is this commitment more pronounced than in the context of a national public debate on pressing political issues:

> Speech is an essential mechanism of democracy, for it is the means to hold officials accountable to the people. The right of citizens to inquire, to hear, to speak, and to use information to reach consensus is a precondition to enlightened self-government and a necessary means to protect it.

Citizens United v. *Federal Election Commission,* 558 U.S. 310, 339 (2010) (citation omitted); *see also Garrison* v. *State of Louisiana*, 379 U.S. 64, 74-75 (1964) ("For speech concerning public affairs is more than self-expression; it is the essence of self-government.").

Even scholars who have advanced the most restrictive view of the scope of the First Amendment by questioning whether it should protect artistic speech, have strongly affirmed that speech about governmental interaction with the citizenry is at the heart of what the Amendment protects. *See, e.g.*, Robert H. Bork, *Neutral Principles and Some First Amendment Problems*, 47 IND. L.J. 1, 27-28 (1971) ("The category of protected speech should consist of speech concerned with governmental behavior, policy or personnel, whether the governmental unit involved is executive, legislative, judicial or administrative."). And, as the Supreme Court has recognized, there is "practically universal agreement" that the First Amendment's protections are at their zenith when applied to "the free discussion of governmental affairs." *Mills* v. *Alabama*, 384 U.S. 214, 218 (1971). Here, in seeking to provide the public with information about the number of government requests received and the number of affected subscriber accounts, Google and Microsoft each seeks to engage in speech that addresses governmental affairs in the most profound way that any citizen can: by describing their own interaction with the government process that is the subject of the national debate. Such speech, relating to the "structures and forms of government" and "the manner in which government is operated or should be operated," is at the very core of the First Amendment, *e.g.*, *Mills*, 384 U.S. at 218; *see also Roth*, 354 U.S. at 484, and thus occupies "the highest rung of the hierarchy of First Amendment values, and is entitled to special protection," *Snyder* v. *Phelps*, 131 S. Ct. 1207, 1215 (2011) (quoting *Connick* v. *Myers*, 461 U.S. 138, 145 (1983)).

This speech also implicates another fundamental aspect of the First Amendment, the protection for self-expression. *E.g.*, *Consolidated Edison Co. of New York, Inc.* v. *Public Service Commission of New York*, 447 U.S. 530, 534 n.2 (1980); *First National Bank of Boston* v. *Bellot-*

ti, 435 U.S. 765, 783 (1978). That interest reflects the principle at the very foundation of the First Amendment that freedom of expression is tied to freedom of thought and to a speaker's very identity. *E.g.*, *Procunier* v. *Martinez*, 416 U.S. 396, 427 (1974) (Marshall, J., concurring) (self-expression "is an integral part of the development of ideas and a sense of identity"); *Police Department of City of Chicago* v. *Mosley*, 408 U.S. 92, 95-96 (1972) (First Amendment "assure[s] self-fulfillment for each individual" by guaranteeing the "right to express any thought, free from government censorship"); *see also* Zechariah Chafee Jr., FREE SPEECH IN THE UNITED STATES 33 (1967); Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 879 (1963). The speech at issue here is expression about the speakers' own actions, actions taken under government compulsion for which the speakers have been publicly criticized[3] and that they now seek to explain and to defend.[4] Banning such speech strikes at the heart of the First Amendment's preservation of speech. It is antithetical to the First Amendment to restrict the ability of a person to mount a defense against public accusations by responding with speech setting forth the truth about one's own actions.[5]

---

[3] *See, e.g.*, Caleb Garling, *Firms Seek to Explain to Users; Tech Surveillance; Some Companies Urge Government Agencies to Allow Transparency*, SAN FRANCISCO CHRONICLE, June 18, 2013, at D1 ("But it is clear that some Internet users have come to view these tech giants as proxy spies as a result of their assumed compliance."); Jessica Guynn, *Tech Firms Try to Regain Trust; Apple is the Latest to Try to Reassure Public That It Didn't Give U.S. Direct Access to Data*, LOS ANGELES TIMES, June 18, 2013, at B2 ("Scrutiny of the role technology companies played in a clandestine government surveillance program is intensifying, and nowhere have the revelations that companies turned over users' personal information been more unsettling than in Silicon Valley.").

[4] The element of government compulsion here distinguishes this situation from that in *Seattle Times Co.* v. *Rhinehart*, 467 U.S. 20, 32-34 (1984), and *Snepp* v. *United States*, 444 U.S. 507, 509 n.3 (1980) (per curiam), where the speaker's *voluntary* participation in a government process that restricted his ability to disseminate materials obtained through that process resulted in diminished First Amendment concerns, *see United States* v. *Aguilar*, 515 U.S. 593, 606 (1995) (distinguishing such cases from those involving "efforts to impose [speech] restrictions on *unwilling* members of the public" (emphasis added)).

[5] Any prohibition on the proposed numerical disclosure would bar truthful speech about a matter of profound national significance and is therefore particularly pernicious given our commitment to protect truthful speech against government restrictions. *See, e.g.*, *Bartnicki* v. *Vopper*, 532 U.S. 514, 533-34 (2001) (noting that challenged measure "implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern"); *cf. The Florida Star* v. *B.J.F.*,

Footnote continued on next page.

The Supreme Court has recognized the special concern that attends prohibitions on speaking about one's own experiences. *See, e.g.*, *Butterworth* v. *Smith*, 494 U.S. 624 (1990) (First Amendment violated by rule prohibiting witness publicly disclosing his own prior grand jury testimony). Indeed Rule 6(e) of the Federal Rules of Criminal Procedure makes a pointed distinction between the general secrecy imposed on participants in the grand jury process and the witnesses before such grand jury, who are not subject to the general secrecy rule. In *Butterworth*, the Supreme Court recognized the importance of a witness' "ability to make a truthful public statement" notwithstanding the longstanding recognition of societal interest in grand jury secrecy. *Id* at 635. Lower courts have frequently struck down orders precluding banks and other institutions from disclosing that the institution had received a subpoena for a customer's records. *See, e.g.*, *In re Grand Jury Proceedings*, 814 F.2d 61 (1st Cir. 1987); *In re Grand Jury Subpoena*, 574 F. Supp. 85 (S.D.N.Y. 1983). The point is not that a non-disclosure rule as to governmental inquiries is precluded in all circumstances, but rather that courts have recognized that First Amendment interests must be weighed very heavily when the government seeks to ban truthful disclosure of information concerning a person's own actions even where other significant societal concerns are at stake. At the least, the government must make a substantial and particularized showing to justify any such ban. *See In re Grand Jury Proceedings*, 574 F. Supp. at 86 (recognizing "the important freedoms, including speech and association" at issue and rejecting request that bank be barred from disclosing to its customer fact of subpoena because of government's failure to make "particularized showing of need for secrecy").

Any attempt to overcome First Amendment concerns implicated by the speech at issue here would have to be subjected to the most searching scrutiny. First, the nature of the re-

---

Footnote continued from previous page.

491 U.S. 524, 533-34 (1989) (discussing constitutional protection afforded for dissemination of lawfully obtained truthful information concerning matters of public significance).

strictions is that of a prior restraint.[6] Such restraint is "the most serious and the least tolerable infringement on First Amendment rights," *Nebraska Press Ass'n* v. *Stuart*, 427 U.S. 539, 559 (1976), and would carry a "heavy presumption against its constitutional validity," *New York Times Co.* v. *United States*, 403 U.S. 713, 714 (1971) (per curiam) (quotation omitted). Second, even if not a prior restriction, any bar focused on disclosure would be based on the speech's content and, therefore, subject to strict scrutiny, which it could survive only if it were narrowly tailored to promote a compelling government interest in the least restrictive means available. *See, e.g.*, *United States* v. *Playboy Entertainment Group, Inc.*, 529 U.S. 803, 813 (2000).

The institutional role of the judiciary also argues strongly for the most rigorous vetting of any proposed bar to disclosure here. That role is relevant in two distinct ways: first, in the interest of the citizenry in observing the workings of the judicial system; and second, in the crucial role that the judiciary has historically played in weighing the claims of the other branches of government against each other and against the interests of the citizenry at large.

As the Supreme Court has recognized in setting out the constitutional concerns supporting open trials, the public's interest in seeing the government process at work, including the judicial process, is a fundamental element of our heritage. "People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing." *Richmond Newspapers, Inc.* v. *Virginia*, 448 U.S. 555, 572 (1980). *Amici* recognize that this Court routinely deals with sensitive information. But when, as with the current applications, disclosure is sought that can bring some transparency to the process and inform the national debate, it is imperative for reasons relating to process as well as the ultimate

---

[6] "The term prior restraint is used to describe administrative and judicial orders forbidding certain communications when issued in advance of the time that such communications are to occur." *Alexander* v. *United States*, 509 U.S. 544, 550 (1993) (quotations omitted).

substantive decision, that any effort to bar disclosure require the most extraordinary showing of potential harm if it is even to be entertained.[7]

And this Court's role in assessing any such effort is crucial. The judiciary's role is that of the "great bulwark of public liberty" in our system of separated powers. *See* 3 The Miscellaneous Writings of Justice Story 209 (ed. William M. Story 1852). That role is undiminished even when those "public liberties" are set against interests of such undeniable exigence as national security. *See Holder* v. *Humanitarian Law Project*, 130 S. Ct. 2705, 2727 (2010) ("[C]oncerns of national security and foreign relations do not warrant abdication of the judicial role" and courts must "not defer to the Government's reading of the First Amendment, even when such interests are at stake."); *Hamdi* v. *Rumsfeld*, 542 U.S. 507, 536 (2004) ("We have long since made clear that a state of war is not a blank check . . . when it comes to the rights of the Nation's citizens.").[8] Indeed, the judiciary's role as bulwark is all the more significant in a context such as this, where proceedings are essentially *ex parte* and where information about those proceedings is of particular value to the public. The broad scope of First Amendment jurisprudence makes clear the rigorous standard that must be required of any claim that would preclude disclosure here. And, as discussed below, these principles have been applied in a specific context closely akin to the present one and held to impose just such a requirement of specific factual proof.

---

[7] As the *Richmond Newspapers* decision also recognized, "[t]he First Amendment goes beyond protection of the press and self-expression of individuals to prohibit government from limiting the stock of information from which members of the public may draw." 448 U.S. at 575-76 (citation omitted). This public interest in "the stock of information" provides a separate First Amendment interest at issue here.

[8] Indeed, the role as arbiter assumes still greater significance when fundamental constitutional guarantees are tested in times of even the gravest insecurity. *E.g.*, *Ex parte Milligan*, 71 U.S. 2, 120-21 (1866) ("The Constitution of the United States is a law for rulers and people, equally in war and in peace, and covers with the shield of its protection all classes of men, at all times, and under all circumstances."); *Home Building & Loan Ass'n* v. *Blaisdell*, 290 U.S. 398, 425-26 (1934) (constitutional rights "were determined in the light of emergency and they are not altered by emergency[;] even the war power does not remove constitutional limitations safeguarding essential liberties").

B. FIRST AMENDMENT PRINCIPLES HAVE BARRED OVERBROAD NON-DISCLOSURE RULES IN THE CONTEXT OF NATIONAL SECURITY

The broad principles described in the preceding section animated the decision in *John Doe, Inc.* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008), which sustained a First Amendment challenge to portions of the Electronic Communication Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986), as amended by the U.S.A. PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). The decision held unconstitutional a blanket prohibition on the recipient of a National Security Letter disclosing information about that letter. The Second Circuit held that a perceived threat to national security could justify restraining the speech there at issue only if the government articulated a sound basis for its judgment to that effect. *See id.* at 881-82. To do otherwise would "cast Article III judges in the role of petty functionaries, . . . stripped of capacity to evaluate independently whether the executive's decision is correct." *Id.* at 881 (quoting *Gutierrez de Martinez* v. *Lamagno*, 515 U.S. 417, 426 (1995)). As that court explained:

> The fiat of a governmental official, though senior in rank and doubtless honorable in the execution of official duties, cannot displace the judicial obligation to enforce constitutional requirements. "Under no circumstances should the Judiciary become the handmaiden of the Executive."

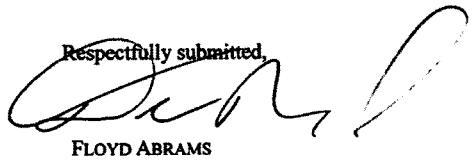
Id. at 882-83 (quoting *United States* v. *Smith*, 899 F.2d 564, 569 (6th Cir.1990)). A similar appreciation of First Amendment concerns informed the recent decision in *In re National Security Letter*, No. C 11-02173 (SI), 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013), where the court perceived no justification for a general prohibition on disclosure of the mere fact of receiving a National Security Letter, *see id.* at *10-11, and concluded that the same statutes as were at issue in *Mukasey* violated the First Amendment. Each of those cases involved challenges to disclosures as to the letters themselves, surely a potentially more revealing disclosure than revelation of numerical totals.

The same core First Amendment principles reflected in those decisions apply with at least equal force to the disclosures at issue here and counsel that any restriction of that speech can be sustained only if such restriction survives the most searching judicial review of a detailed presentation of facts supporting such non-disclosure. *Amici* find it difficult to comprehend how national security could be threatened by the disclosures that Google and Microsoft seek to make here. *Amici* have no doubt, however, that any restriction premised on the suggestion of such alleged threat must be subjected to the strictest of scrutiny and the proponents of any such restriction must overcome the very highest level of First Amendment protection.

* * *

Pursuant to FISC Rule of Procedure 7(h)(1), Attorneys for the *Amici* certify that each of the undersigned Attorneys for *Amici* is a licensed attorney and a member, in good standing, of the bar of United States District Court for the Southern District of New York. Pursuant to FISC Rule of Procedure 7(i), Attorneys for the *Amici* further certify that the undersigned do not currently hold a security clearance.

Respectfully submitted,



OF COUNSEL:

PETER SCHEER
First Amendment Coalition
ALEXANDER ABDO
American Civil Liberties Union
KEVIN BANKSTON
Center for Democracy and Technology
MATT ZIMMERMAN
MARK RUMOLD
Electronic Frontier Foundation
BERIN SZOKA
TechFreedom

FLOYD ABRAMS
DEAN RINGEL
PHILIP TISNE
CAHILL GORDON & REINDEL LLP
80 Pine Street
New York, New York 10005
(212) 701-3000
fabrams@cahill.com

Attorneys for Amici Curiae

RESPONSES OF PAUL ROSENZWEIG TO QUESTIONS SUBMITTED BY SENATOR FLAKE

Written Questions of Senator Jeff Flake
"The Surveillance Transparency Act of 2013"
U.S. Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
November 20, 2013

Professor Paul Rosenzweig

1. In your testimony before the subcommittee, you stated you supported having an advocate appear before the Foreign Intelligence Surveillance Courts, but only if it would not cause procedural difficulties, be adverse to national security, or result in time delays. Do you have any concern that S. 1467, one of the proposals to create a special advocate, could cause procedural difficulties, be adverse to national security, or result in time delays?

Thank you very much for the opportunity to answer additional questions relating to the Foreign Intelligence Surveillance Court ("FISC") and the proposal for an advocate to appear before the court. As I said at the hearing, I am generally supportive of such a proposal on theoretical grounds. My broad take on the idea is as follows:

We should look to create a standing team of attorneys to respond to and present a counter argument before the FISC to requests for permission to collect information against an individual or entity. This team of attorneys should either be from within the government (such as the DNI's Civil Liberties and Privacy Officer), and not a cadre of non-government attorney's with clearances.

There is much to be said in favor of this proposal. With regular criminal warrants the ex parte nature of the application for a warrant does not systematically create a lack of a check on overreaching because of the possibility for post-enforcement review during criminal prosecution with its adversarial process. By contrast, in intelligence investigations that post-execution checking function of adversarial contest is often missing -- few if any intelligence collection cases wind up before the courts. As a result there is no systematic way of constraining the authority of the United States government in this context. Providing for an adversarial advocate would give us the general benefits of adversarial presentation and provide a useful checking function on the overarching broad effect of FISA law on the public.

To be sure, this would be a novel process. We don't typically do pre-enforcement review of investigative techniques. And if poorly implemented, this sort of process risks slowing down critical time sensitive investigations. Perhaps most importantly, many worry (not without justification) that the adversarial advocate will in the end have an agenda that may distort legal developments.

On balance, this seems to be a positive idea – but only if it is implemented in a limited way for novel or unique questions of law. It should be is limited to situations where the FISA court itself requests adversarial presentation. That would limit the number or circumstances where the process was used to those few where new or seminal interpretations of law were being made. The adversarial advocate should not appear routinely and should not appear on his or her own motion. The court is, in my view, capable (and likely) to define when it can benefit from adversarial argument quite well.

This analysis gives you some idea of my thinking about the specifics of S. 1467. I had not read that particular bill prior to my testimony before the Subcommittee and I appreciate the opportunity to examine the matter in more detail. My conclusion is that the provisions of S. 1647, while aimed at a salutary purpose, would prove too intrusive and risk slowing down time-critical investigations. In particular:

- I do not think that a dedicated independent advocate is necessary to review every application to the FISC. Most such application will not pose issues of novel legal construction;
- I do not think that the advocate should have the right to request to participate in matters before the FISC. That decision is best left to the sound discretion of the court; and
- Most notably, I do not think that creating a dedicated issue-specific advocate will prove, in the end, advantageous. We have had experience with single-focused "independent" officers in the past, and it has not proven to be a successful model. *E.g. Morrison v. Olson,* 487 U.S. 654, 731-32 (1988) (Scalia, J., dissenting) ("isolation from the Executive Branch and the internal checks and balances it supplies ... heighten[s] . . . the danger of too narrow a focus, of the loss of perspective, of preoccupation with the pursuit of one alleged suspect to the exclusion of other interests"). Rather, a cadre of government privacy attorneys would serve the function better.

My recommendation would be to modify S.1467 to be less intrusive in its approach, while preserving the important principle of creating a system of adversarial advocacy.

Opening Statement of GEN Keith B. Alexander, Director, NSA
before the Senate Committee on the Judiciary
2 October 2013

- Chairman Leahy, Ranking Member Grassley, distinguished members of the Committee, thank you for the opportunity to provide opening remarks.

- I am privileged today to represent the work of the dedicated professionals at the National Security Agency who employ the authorities provided by Congress, the federal courts and the Executive Branch to help protect the nation and protect our civil liberties and privacy.

- If we are to have an honest debate about how NSA conducts its business, we need to step away from sensationalized headlines and focus on facts.

- Our mission is defend the nation and to protect our civil liberties and privacy. Ben Wittes from the Brookings Institution said about the media leaks and specifically about these two FISA programs: "shameful as it is that these documents were leaked, they actually should give the public great confidence in both NSA's internal oversight mechanisms and in the executive and judicial oversight mechanisms outside the Agency. They show no evidence of any intentional spying on Americans or abuse of civil liberties. They show a low rate of the sort of errors any complex system of technical collection will inevitably yield. They show robust compliance procedures on the part of the NSA. And they show an earnest, ongoing dialogue with the FISA court over the parameters of the Agency's legal authority and a commitment both to keeping the court informed of activities and to complying with its judgments on their legality."

- Today I'd like to present facts to specifically address:

  - Who we are in terms of both our mission and our people;

  - What we do: adapt to technology and the threat; take direction from political leadership; operate strictly within the law and consistent with explicit intelligence priorities; and ensure compliance with all constraints imposed by our authorities and internal procedures;

  - What we have accomplished specifically for our country with the tools we have been authorized; and

  - Where do we go from here?

<u>Who We Are – Our Mission</u>

- NSA is a foreign intelligence agency with two missions:

  - We collect foreign intelligence of national security interest and

  - We protect certain sensitive information and U.S. networks.

- All this while protecting our civil liberties.

- NSA contributes to the security of our nation, its armed forces, and our allies.

- NSA accomplishes this mission, while protecting civil liberties and privacy – because the constitution we are sworn to protect and defend makes no allowances to trade one for the other.

- NSA operates squarely within the authorities granted by the president, congress and the courts.

Who We Are – Our People

- I'm proud of what NSA does and more proud of our people.
  - National Security Agency employees take an oath to protect and defend the constitution of the United States of America.
  - They have devoted themselves to protecting our nation.
  - Just like you, they will never forget the moment terrorists killed 2,996 Americans in New York, Pennsylvania, and the Pentagon.
  - They witnessed the first responders' efforts to save lives. They saw the military shift to a wartime footing. They committed themselves to ensuring that another 9/11 would not happen and our deployed forces would return home safely.
  - In fact, they deploy with our armed forces into areas of hostility.
    - More than 6,000 deployed in support of operations in Iraq, Afghanistan, and CT.
    - 22 paid the ultimate sacrifice since 9/11; sadly adding to a list of NSA/CSS personnel numbering over 170 killed in the line of duty since NSA's formation in 1952.
    - Theirs is a noble cause.

- NSA prides itself on its highly skilled workforce.
  - We are the largest employer of mathematicians in the U.S. (1,013).
  - 966 PhDs and 4,374 computer scientists.
  - Linguists in more than 120 languages.
  - More patents than any other Intelligence Community agency and most businesses.
  - They are also Americans and they take their privacy and civil liberties seriously.

What We Do – Adapt to Technology and the Threat

- Today's telecommunications system is literally one of the most complex systems ever devised by mankind.
- The fact that over 2.5 billion people all connect and communicate across a common infrastructure is a tribute to the ingenuity of mankind. The stark reality is that terrorists, criminals and adversaries make use of the same infrastructure.
- Terrorists and other foreign adversaries hide in the same global network, use the same communications networks as everyone else, and take advantage of familiar services: Gmail, Facebook, Twitter, etc. Technology has made it easy for them.
- We must develop and apply the best analytic tools to succeed at our mission; finding the communications of adversaries while protecting those of innocent people, regardless of their nationality.

What We Do – Take Direction from Political Leadership (NIPF)

- NSA's direction comes from national security needs, as defined by the nation's senior leaders.
- NSA does not decide what topics to collect and analyze.
- NSA's collection and analysis is driven by the national intelligence priorities framework and received in formal tasking.
- We do understand that electronic surveillance capabilities are powerful tools in the hands of the state. That's why we have extensive mandatory internal training, automated checks, and an extensive regime of both internal and external oversight.

What We Do – Use Lawful Programs and Tools to Do Our Mission

- The authorities we have been granted and the capabilities we have developed help keep our nation safe.
- Since 9/11 we have disrupted terrorist attacks at home and abroad using capabilities informed by the lessons of 9/11.
- The Business Records FISA program, NSA's implementation of Section 215 of the PATRIOT Act, focuses on defending the homeland by linking the foreign and domestic threats.
- Section 702 of FISA focuses on acquiring foreign intelligence, including critical information concerning international terrorist organizations, by targeting non-U.S. persons who are reasonably believed to be located outside the United States.

- NSA also operates under other sections of the FISA statute in accordance with the law's provisions (such as Title 1 and Section 704).

- It is important to remember that in order to target a U.S. person anywhere in the world under the FISA statute, we are required to obtain a court order based on a probable cause showing that the prospective target of the surveillance is a foreign power or agent of a foreign power.

- NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order (EO) 12333.

- As I have said before, these authorities and capabilities are powerful; we take this responsibility seriously.

What We Do – Ensure Compliance

- We stood up a Director of Compliance in 2009 and repeatedly train our entire workforce in privacy protections and the proper use of capabilities.

- We do make mistakes. The vast majority of compliance incidents reflect the challenge of implementing very specific rules in the context of ever-changing technology.

- Compliance incidents, with very rare exception, are unintentional and reflect the sort of errors that will occur in any complex system of technical activity.

- The press claimed evidence of "thousands of privacy violations."

- This is false and misleading.

- According to NSA's independent Inspector General, there have been only 12 substantiated cases of willful violation over 10 years – essentially one per year from a population of NSA/CSS personnel numbering in the tens of thousands. But the relatively small number of cases does not excuse any infraction of the rules. We took action in every case referring several to the department of justice for potential prosecution; appropriate disciplinary action was taken in others.

- We hold ourselves accountable every day.

- Most of these cases involved improper tasking or querying regarding foreign persons in foreign places.

- I am not aware of any intentional or willful violations of the FISA statute, which is designed to be most protective of the privacy interests of U.S. persons.

- Of the 2,776 incidents noted in the press from one of our leaked annual compliance reports, about 75% are not violations of approved procedures at all but rather NSA's detection of valid foreign targets that travel to the U.S. and a record that NSA stopped collecting, in accordance with the rules (roamers).

- Let me also start to clear the air on actual compliance incidents.

- The vast majority of the actual compliance incidents involve foreign locations and foreign activities, as our activities are regulated by specific rules wherever they occur.

- For the smaller number that did involve a U.S. person, a typical incident involves a person overseas involved with a foreign organization who is subsequently determined to be a U.S. person. All initial indications and research before collection point the other way, but NSA constantly re-evaluates indications.

- NSA detects and corrects and – in most cases – does so before any information is even obtained, used, or shared outside of NSA.

- Despite the difference, between willful and not, we treat incidents the same: we detect, we address, we remediate – including removing or purging information from our databases in accordance with the rules. And we report.

- We hold ourselves accountable and keep others informed so they can do the same.

- On NSA's compliance regime Ben Wittes said at last Thursday's Intelligence Committee hearing: "but one thing we have learned an enormous amount about is the compliance procedures that NSA uses. They are remarkable. They are detailed. They produce data streams that are extremely telling – and, to my mind, deeply reassuring."(26 September)

- We welcome an ongoing discussion about how the public can, going forward, have increased information about NSA's compliance program and its compliance posture, much the same way all three branches of the government have today. From our perspective, additional measures that will increase the public's confidence in these authorities and our use of them, can and should be open for discussion.

<u>What We have Accomplished for Our Country</u>

- NSA's existing authorities and programs have helped "connect the dots," working with the broader Intelligence Community and homeland and domestic security organizations, for the good of the nation and its people.

- NSA's programs have contributed to understanding and disrupting 54 terror related events: 25 in Europe, 11 in Asia, 5 in Africa, and 13 related to the homeland.

- This was no accident nor coincidence.

- These were direct results of a dedicated workforce, appropriate policy, and well scoped authorities created in the wake of 9/11 to make sure 9/11 never happened again.

- This is not the case in other countries. In the week ending 23 September there were 972 terror-related deaths in Kenya, Pakistan, Afghanistan, Syria, Yemen and Iraq. [Kenya, 62; Pakistan, 75; Afghanistan, 18; Syria, 504; Yemen, 50; and Iraq, 263].

- Another 1,030 were injured in the same countries.

- We need these types of programs to protect against having these types of statistics on our soil.

- NSA's global system is optimized for today's technology on a global network.

- Our analytic tools are effective at finding terrorist communications in time to make a difference.

- This global system and analytic tools are also what we need for cybersecurity.

- This is how we see in cyberspace, identify threats there, and defend networks.

Reforms

- On 9 August the President laid out some specific steps to increase the confidence of the American people in our foreign intelligence collection programs.

- We are always looking for ways to better protect privacy and security. We have improved over time our ability to reconcile our technology with our operations and with the rules and authorities. We will continue to do so as we go forward and strive to improve how we protect the American people – their privacy and security.

- Regarding NSA's telephone metadata program, policy makers across the Executive and Legislative Branches will ultimately decide whether we want to sustain or dispense with a tool designed to detect terrorist plots across the seam between foreign and domestic domains. Different implementations of the program can address the need, but each should be scored against several key attributes:

  - Privacy – privacy and civil liberties are protected.

  - Agility – queries can be made in a timely manner so that, in the most urgent cases, results can support disruption of imminent terrorist plots.

  - Duration – terrorist planning can extend for years, so the metadata repository must extend back for some period of time in order to discover terrorist plans and disrupt plots.

  - Breadth – repository of metadata is comprehensive enough to ensure query responses can indicate with high confidence any connections a terrorist-associated number may have to other persons who may be engaged in terrorist activities.

- As you consider changes in metadata storage location, length of storage, who approves query terms, and the number of hops, we must preserve these foundational attributes of BR FISA.

- Similarly as you entertain reforms to the FISC, operational and practical considerations must be weighed so that there are no inherent delays; emergency provisions are maintained; and any reform to the FISC structure is respectful of the nature of classified information.

Conclusion

- NSA looks forward to supporting the discussion of reforms. Whatever changes are made, we will exercise our authorities dutifully, just as we have always done.

- The leaks of classified NSA and partner information will change how we operate and what people know about us.

- However, the leaks will not change the ethos of the NSA workforce, which is dedicated to finding and reporting the vital intelligence our customers need to keep the nation safe, in a manner that is fully compliant with the laws and rules that authorize and limit NSA's activities and sustain the privacy protections that we as a nation enjoy.

- I look forward to answering your questions.

Responses to Questions for the Record
Submitted October 29, 2013
Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University

United States Senate, Committee on the Judiciary
Hearing on
Continued Oversight of the Foreign Intelligence Surveillance Act
October 2, 2013

I thank the Committee for the opportunity to respond to these Questions for the Record.

Senator Klobuchar's Question

I am very interested in your recommendation that the FISC should have greater in-house technological expertise to assess the government's bulk collection and surveillance requests. I'd like to ask you to flesh this out a bit more.

How would you recommend working technology experts into the current FISC process?

Response to Senator Klobuchar's Question

In the current FISC process, the government is the only party that files papers and argues before the Court. The most natural way to add independent technical expertise would be for the expert to assist the Court. The Court might follow the practice of some ordinary District Courts by retaining a Court-appointed expert, or by appointing a special master who has technical expertise.

If the FISC process is changed to add another party empowered to participate in FISC matters, such as a representative of the public or an advocate for civil liberties, then this party could retain technical experts to assist it in its argument. This expert assistance is important in allowing the independent party to do its job, because the government's argument before the FISC is well-supported by technical experts, and technical claims often play an important role in the government's argument.

If the process is indeed changed to add an independent party, it is important for this party to be able to challenge the government's technical claims. In an ordinary court case, this would occur via discovery, including expert reports, depositions, and cross-examination of experts. Although this full process might not be appropriate for FISC matters, it is important to ensure that the independent party is in a position to get the information it needs to evaluate and challenge technical assertions made by the government.

Finally, the sensitivity of information before the FISC will require that technical experts have the necessary security clearances. Some independent experts already have clearances, but there are relatively few such people who are not already working for or with intelligence agencies. Steps should be taken to make sure that clearance requests can be expedited for technical experts whom the FISC or an independent party want to engage.

Senator Franken's Question

(1) Professor Felten, in your written testimony you stated that "metadata is easy to analyze."

(a) Do you think the intelligence community has the technical ability to give a rough estimate of the number of American citizens and permanent residents whose communications metadata has been collected in their surveillance programs?

(b) Do you think that the intelligence community has the technical ability to give a rough estimate of the number of American citizens and permanent residents whose communications content has been collected in their surveillance programs?

Response to Senator Franken's Question

Yes, the government has the ability to give a rough estimate of the number of American citizens and permanent residents whose (a) metadata and (b) content has been collected.

(a) The intelligence community can give a rough estimate of the number of citizens and permanent residence whose communications *metadata* has been collected. There are several reasonable methods for doing this. Each method gives an estimate that is not exact but is of roughly the correct magnitude.

A first method is to determine the number of U.S. phone numbers that appear in collected metadata records, and then use this information to estimate the number of affected persons. U.S. phone numbers are easily distinguished from non-U.S. numbers by examining the country code and/or area code of the number. Once the number of affected phone numbers is known, this can be used to estimate the number of citizens and permanent residents by making two adjustments, the first to account for the possibility of one person using multiple affected phone numbers, and the second to account for the fact that a small percentage of U.S. phone numbers are owned by people who are neither citizens nor permanent residents.

A second method is to determine the number of distinct customers of each mobile phone carrier whose information is captured. On the assumption that few people have mobile accounts with multiple mobile carriers, this could be used to estimate the total number of affected persons, again correcting for the fact that a small percentage of accounts are owned

by people who are neither citizens nor permanent residents.

A third method, which appears to offer good accuracy if news reports are accurate, is simply to assume that every adult citizen or permanent resident has been on at least one end of a call whose metadata was captured, and therefore to use an estimate equal to the number of adult citizens plus permanent residents.

(b) It is a bit more challenging, but still feasible, for the intelligence community to give a rough estimate of the number of citizens and permanent residents whose communications *content* has been collected.

It is very likely that in all or almost all cases where call content is collected, the metadata about that same call is also collected. If so, then all that remains is to asssemble a database of metadata for calls whose content has been captured, and then to use this metadata to estimate the number of affected citizens and permanent residents. This could be done, for example, by using the first method described above in part (a).

Even if, for some reason, content collection is not accompanied by metadata collection for the same calls, it would be feasible to estimate the number of affected citizens and U.S. persons, using the existing metadata.

This is not meant as an exhaustive list of methods, and there are probably better and more accurate methods than the ones I have described here. The intelligence community employs a great many mathematicians, statisticians, and computer scientists, and prides itself on its ability to extract useful information from large data sets. Surely they are able to provide at least rough estimates of how many Americans are affected by their data collection.