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.