Statement of Lisa Graves[1]
Executive Director
Center for Media and Democracy[2]
Before the
United States Senate Judiciary Committee
September 23, 2009

Reforming the USA PATRIOT Act and Expanded Surveillance of Americans

Chairman Leahy, Ranking Member Sessions, and Members of the Senate Judiciary Committee, thank you for the opportunity to testify today.

I am pleased to endorse the improvements in the Patriot Act Sunset Extension Act that was introduced this week by Senator Leahy, a staunch defender of liberty and security. He was right to vote against the deeply flawed Patriot Act expansion in 2006, and his determination to begin this reform of these powers is worthy of support. These reforms are an important down-payment toward restoring liberties that have been lost. I hope these and additional reforms of federal surveillance powers that have been excessively expanded will be adopted by Congress and signed into law by President Obama.

I. These Powers Are About Us, About Who We Are as Americans

Let me begin with someone far braver and more eloquent than me, Captain Ian Fishback, a U.S. soldier in Iraq who challenged the abuse of prisoners and wrote about "the larger question that this generation will answer":

> Do we sacrifice our ideals in order to preserve security? Terrorism inspires fear and suppresses ideas like freedom and individual rights. Overcoming the fear posed by terrorist threats is a tremendous test of our courage. Will we confront danger and adversity in order to preserve our ideals, or will our courage and commitment to individual rights wither at the prospect of sacrifice? My response is simple. If we abandon our ideals in the face of adversity and aggression, then those ideals were never really in our possession. I would rather die fighting than give up even the smallest part of the idea that is "America."[3]

I agree that we must transcend the fear others want to trigger in our hearts, and we need to summon tremendous courage to help preserve and restore ideals that truly make America the land of the free.

---

[1] I previously served as Deputy Director of the Center for National Security Studies (CNSS), the Senior Legislative Strategist for the American Civil Liberties Union (ACLU), the Chief Nominations Counsel for Senator Leahy, the Deputy Chief of the Article III Judges Division of the U.S. Courts, and Deputy Assistant Attorney General in the Office of Legal Policy/Office of Policy Development at the U.S. Department of Justice. I am indebted to the work of my former colleagues with the ACLU—Michelle Richardson, Mike German, and Jeani Murray of the legislative office and Ann Beeson, Jameel Jaffer, Melissa Goodman who were litigating these issues during my tenure there, among other devoted civil libertarians—my former partner, Kate Martin, of CNSS who has been challenging these issues since before 2001, intelligence expert Suzanne Spaulding whom I am testifying alongside today, and other great civil liberties advocates in the national security surveillance coalition I have helped lead since the 2005 debate over Patriot Act reauthorization and in the ongoing challenges to warrantless wiretapping. I would also like to thank Kate Rhudy for her assistance with this testimony and all her help over the past two years as my law clerk and now as a lawyer. My testimony reflects my own views, of course, and any mistakes are my own.

[2] The Center for Media and Democracy, which was founded by John Stauber in 1993, is an independent, non-profit, non-partisan public interest organization dedicated to promoting transparency and informed debate by exposing government propaganda and corporate spin. Among our priorities is countering misinformation by investigating public relations campaigns by the government and informing grassroots citizen activism that promotes human rights as well as other policies to make the world a better place. CMD's investigations have been praised by leading journalists, such as Amy Goodman of Democracy Now! who observed that "The Center's work in exposing government and corporate propaganda is absolutely essential to our democracy."

[3] Quoted by Andrew Sullivan in THE ATLANTIC, "Dear President Bush" (October 2009).

One of the challenges in this area is whether we have the will to see beyond a particular investigation or crisis, press for the truth, insist on answers, and demand the strong checks and balances that are essential to the idea of America. One of the most important reasons our system of government is so successful, why our democracy has endured, is that we set limits on government power. Elected leaders and government bureaucrats are bounded by the Constitution, laws passed by Congress, and the availability of review of actions taken by independent courts staffed with impartial judges. Checks on power help guarantee that we stay a free country, but these important checks have been greatly eroded.

That is why Americans from all walks of life have stood up against actions by a handful of leaders and operatives who acted in secret and in violation of our laws—with practices like monitoring Americans without court warrants or any proof of wrongdoing, detaining people in secret prisons without redress by the courts, and torture. The Chairman was right to call for a truth commission to ensure that there is accountability to our system of government. Unfortunately, that common sense call has been rebuffed, and the vacuum left by the lack of accounting has been filled with self-serving claims that these policies "work." And, there has been precious little space to have a real conversation about better alternatives that would be both more effective and more consistent with needed checks and balances.

While some of the powers at issue allow people to be monitored without any proof of wrongdoing, the government always concedes that conducting surveillance of everyone is not possible or efficient. But that concession masks the true extent and the true costs of the massive web of secret surveillance of Americans that has been erected over the past several years. Due to the cloak of secrecy that envelopes these powers, it is difficult to picture what is really happening behind closed doors. And, we want to believe that government agents are focused only on the bad guys, but the record tells a different story. Not only does evidence show that many innocent Americans are being secretly swept in, but also the record shows this is happening *because* of recent changes to how the law is written or interpreted, not in spite of the law. Meanwhile, key facts have been kept hidden or been disclosed quite selectively, while other "facts" have turned out to be deliberately misleading, if not outright lies or propaganda. That is one of the reasons that while this debate is often cast in terms of the other, the enemy, it is more properly focused on what we stand *for* as a free people, what our rules should be for surveillance in *this* country, and whether we will call out misinformation and demand the truth as sovereign citizens.

II. The Current Patriot Act Debate and What Should Be on the Table

Today's hearing is focused on the three provisions designated by the Patriot Act reauthorization bill to be up for renewal this year: Section 215, secret orders for records or information about you held by third parties; Section 206, secret roving wiretaps; and the so-called "lone wolf" provision. Rather than adopt this format, I am going to focus on how some of the powers set to expire relate to broader issues at stake and other provisions that should be on the table. I simply do not think this White House and this Congress should accede to the agenda for this debate dictated by the Republican-controlled Congress and White House in 2006. Other secret surveillance powers that undermine Americans' privacy can and should be on the table, and so I would urge this Committee, this Congress, and the new Administration not to feel bound by the narrow topics teed up back in 2006 for debate today.

That is one of the reasons I am very appreciative of the Chairman's decision to include changes to the National Security Letter (NSL) provisions expanded by Section 505 of the Patriot Act and by the 2006 reauthorization, among others. I hope a majority of this Committee will support Senator Feingold's amendments to sensibly update the standards for issuing NSLs and revise other powers that are dangerously overbroad or unjustified, as detailed in his JUSTICE Act. (I am especially proud to be here as a new constituent of Senator Feingold, who bravely stood alone against Patriot in 2001.)

A. Domestic Surveillance that Undermines the Privacy of Americans' Personal Records

1. § 215 Orders Cover Any Tangible Thing and Require No Wrongdoing by You

One way to think of the scope of the power covered by Section 215 of the Patriot Act is to think of a giant file into which literally "any tangible thing" held by a third party about you can be put, that is, can be secretly obtained by government agents. Any tangible thing. It could be your DNA, your genetic code, from tests taken by your doctor for your health. It could be records about the books you buy or read. It could be information about websites you have visited. To search your home for these types of personal records, the government would have to have a warrant based on probable cause of wrongdoing, but to obtain them from your doctor or others you do business with, such as your internet service provider or your employer, no such probable cause is required under the statute since 2001.

In fact, any tangible thing about you can be secretly obtained without any evidence that you are a suspected terrorist. Virtually everything about you can be seized through secret 215 orders if you have any contact with a suspect. On the surface that might sound reasonable, but when you think it through you can see that every day through work or business you come into contact with dozens of people, at work, at schools, at conferences, in the cafeteria, at sporting events, at the mall, and if any one of them is the subject of an investigation your sensitive, personal private information might get swept up and kept in government files for decades. That amounts to hundreds of people a year and mere contact, however brief, can trigger this law, which requires the secret Foreign Intelligence Surveillance Court to presume your sensitive personal records are relevant to an investigation and grant a secret access.

And, under the law as amended in 2006, your employer, doctor, or librarian, for example, who may have known you since childhood, cannot ever tell you your privacy has been breached without going to court, even if you are never charged with any wrongdoing. And, it bars them from even challenging such orders for your personal, private information for a year. And, even then, the law as amended in 2006 makes it almost impossible for that person or business to prevail, by creating a conclusive presumption against disclosure if a government official certifies the request should be kept secret for various reasons, without providing the court with any facts to test such assertions.

It is no wonder that librarians and booksellers and other groups devoted to protecting freedom of conscience strongly oppose these far-reaching and excessive secret powers. At every juncture, the prior administration eliminated checks and balances that would help protect the innocent and ensure these powers were properly focused. Senator Leahy's bill would require that the government provide facts showing why they think the records they are seeking are actually relevant rather than just show any contact with a subject of an investigation, and it would allow recipients to challenge orders for the disclosure of any tangible thing sought. These changes would untie the court's hands in assessing the original request and any challenge to it or to the related gag order. Senator Feingold's bill would make similar changes and also require that any restriction on freedom of speech related to receiving such an order be narrowly tailored, in accordance with First Amendment law, and it would allow the use of these tangible things to be challenged in court just like any other evidence. Both bills would also require more court oversight of how the things obtained with these orders are used or disseminated.

These are important steps toward containing and refocusing this far-reaching power. In my view, to better protect innocent Americans, this power should be predicated on more than mere contact—it should require some reason to believe the subject is knowingly aiding a suspect rather than merely in the wrong place at the wrong time while engaged the innocent business of daily life. Congress should also probe the findings of the Inspector General that, after a rare denial of a requested Section 215 order, the FBI circumvented the court by using an NSL and should prevent this from happening again.

2. Extreme Secrecy Was Used to Obscure the Truth and Distort the Debate

The Section 215 power was subjected to a sunset, or time limit, back in 2001 because it was a newly created, far-reaching power. In the debate over the Patriot Act in 2005, the Bush Administration made a deliberate decision to voluntarily de-classify statistics about how infrequently this power was used. The power had been used only a few dozen times, and this fact was used to attack opponents as over-reacting to the potential danger of this power. Since then, the government has used this power much more regularly, resulting in a ten-fold increase in Section 215 orders in just two years.

At the same time, the administration adamantly refused to disclose the number of demands for third party records being issued under the changes made by Section 505 of the Patriot Act, which is known as the National Security Letter (NSL) power. NSLs were not made subject to the sunset in 2005 because they were a power that pre-dated the Patriot Act, even though those powers were greatly expanded in 2001. One way to think about the relationship between Section 215 orders for any tangible thing and Section 505 demands for information about financial transactions, phone records, internet transactions (who you e-mail and who e-mails you), and credit reporting information is to think of a circle within a circle. Everything covered by a Section 505 demand also counts as a tangible thing under Section 215, but not every tangible thing is a financial, internet, phone, or credit record.

However, notwithstanding the dangers of permissive access to any tangible thing about you without any showing of probable cause, Section 505 NSLs are even more dangerous to individual liberty. This is because NSLs are issued by the FBI without any court approval whatsoever. These are unilateral, coercive, and secret demands by FBI agents to businesses for personal, private information about you, without even having to show the secret FISA court in Washington any evidence supporting the request. So, of course, we in the civil liberties community believed these powers were being widely used. And, even though this controversial power became a major part of the reauthorization debate in 2005, the administration refused to make public even the number of requests made, while touting the assertion that it had used the related Section 215 powers sparingly, only a handful of times. The ACLU filed a FOIA request for the numbers and ended up with six-page document in which nearly every entry related to the number of NSLs was redacted except for the words "Grand Total." It literally took an act of Congress to dislodge the information about how often NSLs had been used, through required audits and reporting, which were some of the only real improvements made in the deeply flawed 2006 reauthorization of the Patriot Act.

But, in November 2005 as the Patriot Act was being delayed by a mounting filibuster in the Senate, an investigative piece by the Washington Post's Bart Gellman quoted government sources reporting that the number of NSL requests had exploded to over 30,000 per year.[4] The Justice Department harshly attacked the article in a letter to then-Chairman Specter signed by William Moschella, and calling the 30,000 figure "inaccurate." I myself heard from a number of staff and reporters that the administration had absolutely denied that anywhere near this number of demands had been made, just as the NSL powers were being debated on the Hill and in public. Congress responded to the controversy by requiring an audit of the number of times the power was being used.

That is how in 2007 we learned that the true number of NSL requests issued in 2004, the year before the article was published, was over 56,000.[5] The number reported in the press was not too big; it was

---

[4] Barton Gellman, "The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans" WASHINGTON POST, A01 (Sunday, November 6, 2005).

[5] For my detailed assessment of the 2007 NSL audit, *see* www.intelligence.house.gov/Media/PDFS/Graves032807.pdf.

too small! The administration attempted to sidestep this dispute by asserting that its statements were based on counting only the number of letters and not the number of requests. Yet, administration officials had to know that individual letters often had multiple requests. To this day, there has been no real accountability for the way the public was misled by DOJ at the crucial moment in this debate. In another instance of deliberately distorting the public debate in 2005, while the prior administration was asserting that the government was not interested in library records it was simultaneously seeking records from the Library Connection in Connecticut and gagging those librarians from telling Congress and rebutting the misleading assertions of the government. Both the Leahy and Feingold bills amend the law to address the constitutional flaws noted by the U.S. Court of Appeals for the Second Circuit in that case regarding the gag order that accompanies an NSL. These improvements are essential.

3. Weakened Standards for NSLs Have Swept in Numerous Innocent People

The Department of Justice's own Annual Performance and Accountability Report in 2006 described in stark terms how the current standards for using NSLs affect ordinary Americans:

> Likewise, investigative and intelligence authorities enacted or expanded in the Patriot Act [and the 2005 reauthorization] invest broad new information-gathering powers in FBI agents and their supervisors . . . on a minimal evidentiary predicate. For example, . . . it authorized the FBI to collect information such as telephone records, Internet usage, and credit and banking information on persons who are not subjects of FBI investigations. This means that the FBI—and other law enforcement or Intelligence Community agencies with access to FBI databases—is able to review and store information about American citizens and others in the United States who are not subjects of FBI foreign counterintelligence investigations and about whom the FBI has no individualized suspicion of illegal activity.

www.usdoj.gov/ag/annualreports/pr2006/2006par.pdf (adding that therefore these powers need "aggressive oversight" internally).

The Feingold bill redresses this problem with an important update to NSLs to require the bare minimum that should be required in a free society: that the FBI have individualized suspicion about the person records it wants pertain to, instead of permitting an internal government assertion or boilerplate certification of relevance to an "authorized investigation." This is critically important because the Executive Branch re-wrote the rules to allow a "preliminary inquiry" to count as an authorized investigation, even though the statute intended that these intrusive powers only be used when a full investigation was underway, which required at least some evidence of a reasonable likelihood of wrongdoing. Even the FBI Director conceded to Senator Wyden in 2005 that these newly renamed "preliminary investigations" had "no particular standard of proof." (And, I would strongly urge the Committee to look more closely at the revised AG Guidelines for investigations, which also need to be changed to protect against increased monitoring of First Amendment activities.)

Under the current weakened "standard," as the Inspector General noted, the FBI has used NSLs to obtain information about people two or three degrees of separation away from the target/subject of an investigation. This is important for ensuring that these powers are sensibly focused. Assuming, conservatively, that an average person is in contact with a hundred people between family, friends, co-workers, and merchants, two degrees of separation is 10,000 people (100 x 100)—and, it is documented that one investigation in 2004 alone used a nine NSLs to obtain information about over 11,000 people. And, three degrees of separation could sweep in 100,000

people (10,000 x 100). It is far too permissive and unreasonable to allow these intrusive powers such a broad, almost arbitrary reach into Americans' lives and communities.

It is also the case that FBI agents told the Inspector General that NSLs were very useful in clearing people and closing files, but the FBI General Counsel has asserted that private records about people who are cleared be kept for perpetually, purportedly to help clear them again. Indeed, in 2007, the Inspector General made clear that nothing in DOJ or FBI policies require "the purging of information derived from NSLs in FBI databases, regardless of the outcome of the investigation. Thus, once information is obtained in response to a national security letter, it is indefinitely retained and retrievable by the many authorized personnel who have access to various FBI databases." How many of the people subject to the over NSL requests are innocent? We do not know for certain, but we do know that the government conducts only a couple dozen international terrorism prosecutions per year, according to the Transactional Records Access Clearinghouse.

4. The Number of NSL Requests Dwarf the Number of 215 Orders

Cumulatively, we know that over 230,000 NSL requests have been issued in the past eight years, but even this number is too low. Despite receiving a personal assurance by the Director of the FBI that some reasonable estimate of the of NSLs issued in 2001 and 2002 would be made public, those numbers remain undisclosed. Plus, the figures reported for 2007 and 2008 exclude the number of NSL requests for internet transaction information. So, the true number could be 300,000, more or less.

Even that number would not include any NSLs that were withdrawn or threatened, as Gellman reported occurred when Las Vegas casinos shared over 1,000,000 hotel records in late 2003/early 2004. (Hotel/casinos were swept into the NSL powers when the law was amended to construe "financial institution" to include casinos, as well as insurance companies, jewelers, boat sellers, and the U.S. Postal Service, among other institutions that are not banks but that have some cash business.) Those figures are not included in the statistics, which demonstrates how even mandatory reporting about the mere numbers of NSLs can be sidestepped through other tools, such as "voluntary" compliance with requests, the use of grand jury subpoenas, and grounded or groundless assertions of emergency or exigency, none of which currently require public reporting and which should be fixed. This also underscores a little-noticed fact that has emerged: NSLs are not the exclusive means for obtaining Americans' financial, credit, internet, or phone records. This creates uncertainty for agents and a real lack of adequate controls to protect the public. Fortunately, the Feingold bill includes a provision to ensure that the FBI's unlawful use of so-called exigent letters is barred and emergencies are bona fide.

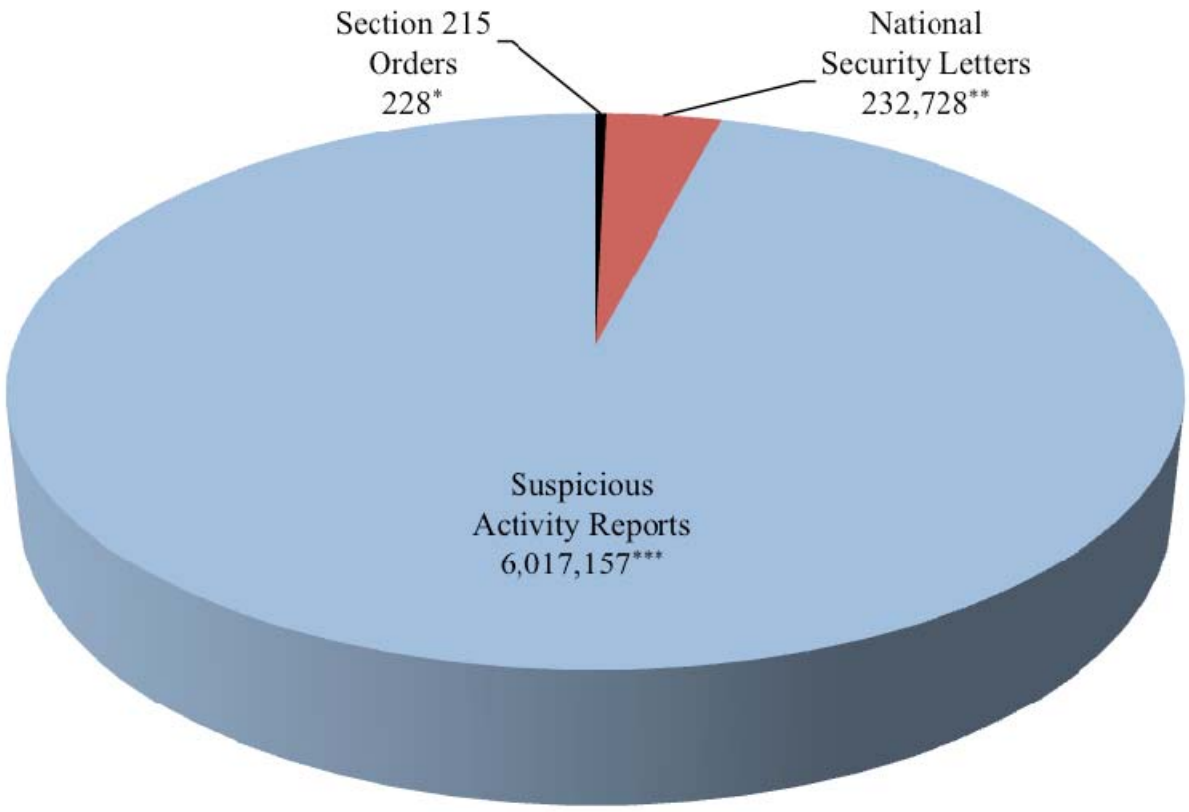
Even assuming the 230,000 figure were not significantly understated, the number of 215 orders is dwarfed by the number of NSL demands. At a minimum, there are almost a thousand NSLs issued for every 215 order issued. NSLs are affecting tens of thousands more people in the U.S. than Section 215 orders, and yet the focus on the expiring powers is effectively distracting from the more widely used NSLs. Additionally, NSLs are being used increasingly against United States citizens who now represent the majority of individuals about whom and NSL has been issued. (In 2006, 60% of NSLs were about U.S. persons, compared with approximately a third in 2003.)

5. And, the Number of NSLs Is Dwarfed by Suspicious Activity Reports

Title III of the Patriot Act expanded immunity and incentives for financial institutions to secretly file Suspicious Activity Reports (SARs) on their customers. SARs are sent from banks, for example, to the U.S. Department of the Treasury, which transmits these reports to the FBI for inclusion in the Investigative Data Warehouse. Even though SARs are not issued by the government, they are part of

the broader issues resulting in the tremendous expansion in FBI files about ordinary Americans. Most of the hearings about this issue have featured government witnesses talking about connecting the dots and stopping the flow of terrorist money. But, little has been done to examine the exponential growth in the number of private financial records being secretly and voluntarily shared with the government. Back in 2000, the number of SARs was about 160,000 per year, and the annual figure has increased ten-fold in less than a decade, with over 1.2 million issued in 2007 alone.

Section 215 Represents a Tiny Slice of the Data FBI Is Now Collecting



Sources for chart data (with thanks to the ACLU's recent report on the Patriot Act):
* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS 77 (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703a/final.pdf (number of Section 215 orders in 2001 through 2005); U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006, 84 (Mar. 2008), *available at* http://www.usdoj.gov/ oig/special/s0803a/final.pdf (number of Section 215 orders in 2006); Letter from Brian A. Benczkowski, Principal Deputy Assistant Attorney General, U.S. Department of Justice, to Nancy Pelosi, Speaker, U.S. House of Representatives (Apr. 30, 2008), *available at* http://www.fas.org/irp/ agency/doj/fisa/2007rept.pdf (number of Section 215 orders in 2007); Letter from Ronald Weich, Assistant Attorney General, U.S. Department of Justice, to Harry Reid, Majority Leader, U.S. Senate (May 14, 2009), *available at* http://www.fas.org/irp/ agency/doj/fisa/2008rept.pdf (number of Section 215 orders in 2008).

** *See* U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 37, 120 (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf (number of NSL requests in 2000 through 2005); U.S. DEP'T OF JUSTICE, OFFICE OF INSPECTOR GENERAL, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006, 107 (Mar. 2008), *available at* http://www.usdoj.gov /oig/special/s0803b/final.pdf (number of NSL requests in 2006); Letter from Ronald Weich, Assistant Attorney General, U.S. Department of Justice, to Harry Reid, Majority Leader, U.S. Senate (May 14, 2009), *available at* http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf (number of NSL requests in 2007 and 2008).

*** U.S. DEP'T OF THE TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW – BY THE NUMBERS, ISSUE 12, 4 (June 2009), *available at* http://www.fincen.gov/news_room/rp/files/sar_by_numb_12.pdf.

Plainly, the majority of Americans who have now had the personal, financial information involuntarily turned over to the federal government through the voluntary actions of their banks have not been charged with any wrongdoing. But, these records will stay in the federal databases indefinitely. Even though the Senate Judiciary Committee does not have primary jurisdiction over FinCEN matters, it should explore how these powers relate to the demands for financial information with NSLs.

Financial records now represent a significant component of the FBI's data "warehouse," which reported having almost 1 billion records as of late 2008. That is three times more records than people in the U.S. As the Electronic Frontier Foundation has noted, that is more records than are held by the largest library in the world, the Library of Congress, which has "138 million items in its collection."[6] As Bart Gellman reported in 2005, the Investigative Data Warehouse only began five years ago, in 2004, and already it has accumulated a billion records. If the number of records contained in the IDW were compared to the pie chart on the prior page, the IDW pie would be 50 times larger. Yet, there has been almost no public examination or hearings focused on this gargantuan database. And the IDW is focused primarily on U.S. records and people in the U.S. The FBI has a whole separate data warehouse, the Foreign Terrorist Tracking Task Force (FTTTF) "Datamart," for foreign terrorism investigations focused abroad, and that database has even more records in it than the IDW.

Additionally, despite revelations by Mr. Gellman and others, there has been no public examination of how the FBI is using contracts it has with the databroker ChoicePoint or with LexisNexis' financial assets databases to obtain or verify and obtain information about Americans. It is certainly the case that the Executive Branch has elsewhere said that it is determined to exploit so-called "open source" data and that the government has a right to information that commercial companies have, but it is not clear precisely what rules the FBI is operating under when its agents access ChoicePoint, for example, or how this relates to compelling versus voluntary disclosures by traditional financial institutions under NSLs or 215 orders or other claimed authority. It is also not clear how much taxpayer money is going into these contracts and what meaningful privacy protections, if any, are being applied. There is no information about how much private companies may be profiting by selling access to this data to the federal government. And, there has been no reporting about how many Americans have had information about them that may have been accumulated by ChoicePoint accessed by the government. And, the public has a right to know the answers to these questions.

These issues may seem complicated on the surface, but they are really about a fundamental question in a democracy: how much information should the government be able to accumulate about a person, without any evidence of any wrongdoing. I would submit that the answer should be very little, but it seems the government thinks the answer should be almost unlimited. And, nowadays, there is no need to create a separate file on a particular person when all the data can easily be aggregated at the touch of a button through the use of internal search engines that can accumulate information about a person.

B. Section 206 and Related Secret Wiretapping Needed Reforms

Just as the discussion of Section 215 of the Patriot Act implicates other powers with broader impact on individual privacy, Section 206 cannot be reasonably understood without reference to FISA powers. Before news broke that President Bush violated federal laws requiring judicial approval to conduct electronic surveillance in the US in investigations to prevent terrorism, he misled the American people,

[6] http://www.eff.org/issues/foia/investigative-data-warehouse-report. For a comprehensive examination of the IDW, access EFF's report.

telling Marylanders and Ohioans in 2005 that the government "needs a federal judge's permission to wiretap a foreign terrorist's phone, a federal judge's permission to track his calls . . . ." Back in 2004, in an effort to blunt controversy about his powers, President Bush assured New Yorkers: "Any time you hear the United States government talking about a wiretap, it requires—a wiretap requires a court order. Nothing has changed, by the way. When we're talking about chasing down terrorists, we're talking about getting a court order before we do so."

Once Eric Lichtblau and James Risen of the New York Times broke the story about the extraordinary electronic surveillance the administration was engaging in without warrants and in violation of the law, President Bush and his aides claimed that he was not misleading because he was talking about the Patriot Act's roving wiretap provisions. But, that was just more misinformation. The false implication was that the Patriot Act was totally separate from the laws the administration had broken. The Patriot Act amended the law President Bush broke but did not repeal the requirement of individualized judicial warrants for terrorism wiretaps.

Indeed, before the story broke, even the President's own advisors used to concede: "the primary provision in the Patriot Act makes amendments to the Foreign Intelligence Surveillance Act [FISA], which is the secret court you hear about that issues secret wiretaps. . . for over 25 years that have been tested in the courts that strike the proper balance between expanding our fight against terrorism, but protecting civil liberties at the same time." This is what John Yoo, former Bush appointee in DOJ's Office of Legal Counsel, told this to CNN in 2005. Yet, Mr. Yoo knew the administration was not following these rules because Mr. Yoo helped write the memos that rationalized evading the very requirements he was extolling on national television.

The suggestion that these binding laws somehow do not apply to terrorism ignores the plain language of the laws that were broken. It is important to recall that the Bush Administration asked for, and Congress passed, several amendments to the electronic surveillance provisions of FISA in the Patriot Act, which is titled "Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." And FISA expressly constituted the "exclusive" rules for foreign intelligence surveillance in the US, including electronic surveillance to prevent "international terrorism," making it a crime to wiretap without court approval.

Under classic FISA, it does not matter whether the wiretaps involve multiple phones, known as multi-point or "roving" wiretaps, or involve just one phone. Federal law requires judicial approval for all electronic surveillance of Americans. To accept the assertions would require accepting the false claim that the only time judges are required is when the person tapped is using more than one phone. The law required individual warrants no matter how few or how many phones or email accounts are tapped.

Until last year, FISA required that the government identify the telephone or device to be tapped in a secret wiretap order. But, with last year's passage of the FISA Amendments Act (FAA), the government is not required to disclose to the court the "facility" where the acquisition of electronic information takes place, let alone particular phones, for surveillance that meets the FAA's test. So, the Section 206 rules that permit what have become known as "John Doe roving wiretaps" apply to a narrow category of cases within the U.S. that are not covered by the broad orders for electronic surveillance of international communications that are permitted under the FAA, orders that I and others believe are unconstitutional. That is why I support not just Senator Feingold's amendments to cure the flaws in the roving wiretap powers, but also the much needed changes he proposes to the revised FISA authorities. I support Senator Feingold's amendments in Title III of his bill to address these issues.

The amendment against bulk collection is particularly important because of the way the FISA Amendments Act could be construed and especially in light of the "over-collection" revelations earlier this year. Additionally, I know that the FISA Amendments Act attempted to bar using blanket orders for electronic collection from being used to acquire purely domestic communications. However, President Bush and his allies inserted language in the bill making the bar on collecting domestic calls or e-mails applicable only when the government knows "at the time of acquisition" that the sender and all recipients are physically located in the U.S. This weasel language permits ignorance to be bliss when it comes to rules intended to protect purely domestic calls or emails. The other amendments in Title III are also important and would help restore civil liberties in this country.

Even though there is little political appetite to revisit the FISA rules, I think doing so is important in the context of the Patriot reauthorization debate. For example, the public has never received a clear answer about the published reports that FBI agents were distracted by ineffective and wasteful surveillance leads generated from the NSA's illegal electronic surveillance program.[7] Here is part of that report:

> In the anxious months after the Sept. 11 attacks, the National Security Agency began sending a steady stream of telephone numbers, e-mail addresses and names to the F.B.I. in search of terrorists. The stream soon became a flood, requiring hundreds of agents to check out thousands of tips a month. But virtually all of them, current and former officials say, led to dead ends or innocent Americans. . . . "We'd chase a number, find it's a school teacher with no indication they've ever been involved in international terrorism - case closed," said one former FBI official, who was aware of the program and the data it generated for the bureau. "After you get a thousand numbers and not one is turning up anything, you get some frustration."

As Suzanne Spaulding has previously suggested, and Kate Martin and I have repeatedly urged, we need a comprehensive examination of the domestic surveillance authorities and uses. Until this kind of far-ranging review is complete, the American people will be stuck with a patchwork of authorities that serve neither liberty nor security well.

C. Other Powers in Need of Reform

In addition to these powers, I would urge Congress to take a closer look at Section 213 of the Patriot Act, which granted sneak and peek powers in routine criminal cases, overwhelmingly in cases that have nothing to do with terrorism. I would also urge that the Committee take another look at the so-called "lone wolf" provision, which has reportedly not be used by the government, as well as other provisions addressed in Senator Feingold's set of amendments.

I would also like to commend Senator Leahy again for the base bill he has introduced on this issue, and all he has done and continues to do to defend individual rights and support common-sense improvements to the law. I understand that there is precious little time to resolve all these issues before the end of this Session of Congress, but I urge that these issues be examined and be resolved publicly to the extent possible.

Thank you again for the invitation and for considering my views.

---

7 Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr., "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," THE NEW YORK TIMES (January 17, 2006).