Policy Analysis

No. 675 May 16, 2011

Leashing the Surveillance State
How to Reform Patriot Act Surveillance Authorities

by Julian Sanchez

Executive Summary

Congress recently approved a temporary extension of three controversial surveillance provisions of the USA Patriot Act and successor legislation, which had previously been set to expire at the end of February. In the coming weeks, lawmakers have an opportunity to review the sweeping expansion of domestic counter-terror powers since 9/11 and, with the benefit of a decade's perspective, strengthen crucial civil-liberties safeguards without unduly burdening legitimate intelligence gathering. Two of the provisions slated for sunset—roving wiretap authority and the so-called "Section 215" orders for the production of records—should be narrowed to mitigate the risk of overcollection of sensitive information about innocent Americans. A third—authority to employ the broad investigative powers of the Foreign Intelligence Surveillance Act against "lone wolf" suspects who lack ties to any foreign terror group—does not appear to be necessary at all.

More urgent than any of these, however, is the need to review and substantially modify the statutes authorizing the Federal Bureau of Investigation to secretly demand records, without any prior court approval, using National Security Letters. Though not slated to sunset with the other three Patriot provisions, NSLs were the focus of multiple proposed legislative reforms during the 2009 reauthorization debates, and are also addressed in at least one bill already introduced this year. Federal courts have already held parts of the current NSL statutes unconstitutional, and the government's own internal audits have uncovered widespread, systematic misuse of expanded NSL powers. Congress should resist recent Justice Department pressure to further broaden the scope of NSL authority—and, indeed, should significantly curtail it. In light of this history of misuse, as well as the uncertain constitutional status of NSLs, a sunset should be imposed along with more robust reporting and oversight requirements.

Julian Sanchez is a Cato Institute research fellow.

CATO INSTITUTE

The Patriot Act significantly expanded government surveillance authorities with minimal Congressional deliberation.

Introduction

It is nearly a decade now since Congress responded to the terror attacks of 9/11 by granting its hasty approval to the USA Patriot Act, a sprawling piece of legislation comprising hundreds of amendments to an array of complex intelligence and law enforcement statutes.[1] As the *Washington Post* noted at the time, "members of both parties complained they had no idea what they were voting on, were fearful that aspects of the . . . bill went too far—yet voted for it anyway."[2]

Recognizing that Patriot had significantly expanded government surveillance authorities with minimal deliberation, Congress established expiration dates for 16 of the Act's most controversial provisions. It similarly established a sunset for the so-called "Lone Wolf" provision of the Intelligence Reform and Terrorism Prevention Act of 2004, which allowed non–U.S. persons to be monitored under the aegis of the Foreign Intelligence Surveillance Act even if they were unaffiliated with any foreign power.[3] In 2005, Congress made 14 of those provisions permanent, but retained sunsets for the Lone Wolf provision, as well as Patriot Act provisions authorizing the secretive Foreign Intelligence Surveillance Court to issue warrants for "roving wiretaps" and broad orders compelling the production of business records or any other "tangible thing."[4] In the process, legislators added a number of safeguards aimed, in part, at assuaging the concerns of civil libertarians.[5]

In late 2009, as the sunset date loomed, the judiciary committees of both the House and Senate held extensive hearings to consider how these new powers had been used and what modifications to the existing statutes might be appropriate.[6] Additionally, in response to a series of increasingly damning reports from the Justice Department's Office of the Inspector General, showing large-scale and systematic abuse of the Patriot Act's expanded authority to issue National Security Letters,[7] Congress held further hearings focused on these powerful tools, which allow the Federal Bureau of Investigation to demand a wide array of telecommunications and financial records without judicial approval.[8]

The hearings and associated debate generated both substantial press coverage[9] and an array of substantive reform bills.[10] Ultimately, however, and despite a temporary short-term extension aimed at allowing further debate, Congress passed—and President Obama signed—a one-year reauthorization of the expiring provisions without modification.[11]

The rationale for the limited reauthorization was that the intervening time would be used for fruitful deliberation on needed reforms, but that hope was not borne out. Until February, there had been almost no further debate in Congress concerning the expiring Patriot provisions or the pressing need for National Security Letter reform, and press attention had been correspondingly scant.

At least some legislators, however, appear to be growing weary of these deferrals. The same one-year reauthorization that easily garnered the two-thirds majority required for fast-track passage in 2009 fell short this year, to the surprise of many observers.[12] Instead, Congress approved an extension of the expiring provisions for just three months, with leaders in both parties pledging that there would now—finally—be serious deliberation on the need for substantive reform.[13]

As of this writing, most of the legislative proposals that have been advanced involve either long-term reauthorization without alteration or modest amendments. Sen. Dianne Feinstein (D-CA) supports reauthorization through the end of December 2013, along with an extension of the controversial FISA Amendments Act of 2008 to the same date,[14] while Sen. Chuck Grassley (R-IA) is seeking permanent reauthorization of the expiring provisions.[15] Sen. Patrick Leahy (D-VT), meanwhile, has reintroduced the

relatively mild reform legislation he sponsored in 2009, which at the time was approved by a bipartisan majority of the Senate Judiciary Committee.[16]

With additional time for deliberation, however, Congress should consider more far-reaching changes. With minor modifications, the roving wiretap provision can safely be made permanent, providing greater clarity and certainty to intelligence investigators. The Section 215 "tangible things" provision, by contrast, requires additional Congressional scrutiny: it should be extended only in a narrowed form, and with further reporting and auditing requirements. The Lone Wolf provision, which as of last year the Justice Department said had never been used, can simply be allowed to expire. (In the event that consensus has not been achieved when the new deadline arrives, there is little reason to believe their expiration would cause any near-term impediment to intelligence gathering: all three sunsetting provisions have been used fairly sparingly, and are, in any event, subject to a grandfather clause that would permit their continued use for investigations already underway.[17])

Most importantly, Congress should narrow the scope of National Security Letters, which have already proven susceptible to widespread abuse, and which federal courts have already found to be seriously constitutionally defective in their current form. At an absolute minimum, a series of procedural safeguards that the Justice Department has already agreed to implement on a voluntary basis should be codified in statute. Even with these added constraints, a new sunset for expanded NSL authorities should be established, along with mandatory auditing by the Office of the Inspector General, to ensure that they are subject to adequate congressional review.

I now turn to consider each of the sunsetting provisions, as well as National Security Letters, in detail. While many of the arguments below are framed in terms of the constitutional limits on government surveillance, they also provide policy grounds for reform. Insofar as these provisions impose heavier burdens on core privacy, speech, and association interests than is necessary to the protection of national security that should be sufficient reason to seek a better balance regardless of where one comes down on the legal question.

The Lone Wolf Provision

The extraordinary tools available to investigators under the Foreign Intelligence Surveillance Act, passed over 30 years ago in response to revelations of endemic executive abuse of spying powers,[18] were originally designed to cover only "agents of foreign powers." The Lone Wolf provision severed that necessary link for the first time, authorizing FISA spying within the United States on any "non-U.S. person" (that is, anyone not a citizen or legal permanent resident) who "engages in international terrorism or activities in preparation therefor," and allowing the statute's definition of an "agent of a foreign power" to apply to suspects who, bluntly put, are not in fact agents of any foreign power. According to a letter sent to Senator Leahy in September of 2009 by Assistant Attorney General Ronald Weich, the Lone Wolf provision's authority had never been invoked as of that date, and there has been no indication that it has been used since.[19]

As with many post-9/11 intelligence reforms, the Lone Wolf provision has its genesis in the misguided assumption that every intelligence failure is evidence that investigators lack sufficient surveillance authority—a convenient scapegoat—while internal institutional dysfunction often bears the lion's share of the blame.[20] In the aftermath of the attacks, it was initially alleged that FBI investigators who had wanted to obtain a warrant to search the laptop of so-called "20th hijacker" Zacarias Moussaoui were unable to do so because FISA lacked such a Lone Wolf provision. This claim, according to the Congressional Research Service, provided the "historical impetus" for Lone Wolf authority.[21]

Congress should narrow the scope of National Security Letters, which have already proven susceptible to widespread abuse.

But a 2003 bipartisan report from the Senate Judiciary Committee tells a very different story.[22] It notes that on September 11, 2001, investigators were able to obtain a conventional warrant using the exact same evidence that had previously been considered insufficient. Worse, the Committee found that supervisors at FBI Headquarters had failed to link related reports from different field offices, or to pass those reports on to the lawyers tasked with determining when a FISA warrant should be sought. Officials in charge, the Senate report concluded, misapplied such crucial legal standards as "probable cause" and falsely believed that they could not seek a FISA order unless the specific foreign terror group with which a target was affiliated could be definitively identified.

"In performing this fairly straightforward task," the report concludes, "FBI headquarters personnel failed miserably."[23] In short, the problem was not that investigators lacked Lone Wolf powers, but that they had not properly applied the powers they already had. Nevertheless, the new power was granted.

That it had not been used at the time of the last reauthorization debate suggests that the provision remedied no dire gap in existing surveillance authorities, but also that it has not yielded any practical harm. The Lone Wolf provision does, however, threaten to blur the vital and traditional distinction in American law between the constraints on strictly domestic national security investigations and foreign intelligence.

The problem was not that investigators lacked Lone Wolf powers, but that they had not properly applied the powers they already had.

Foreign Intelligence versus Domestic Security

Courts have always extended greater deference to the executive in the realm of foreign intelligence than in cases involving strictly domestic security concerns. In a seminal ruling in what has come to be known as the *Keith* Case, a unanimous Supreme Court held that the Fourth Amendment's warrant requirement applied with full force to strictly domestic intelligence investigations, even where the national security was implicated.[24] The Court did, however, echo the language of prior rulings, suggesting that less stringent limits might apply where foreign powers were concerned:

> Further, the instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country. The Attorney General's affidavit in this case states that the surveillances were "deemed necessary to protect the nation from attempts of *domestic organizations* to attack and subvert the existing structure of Government" (emphasis supplied). There is no evidence of any involvement, directly or indirectly, of a foreign power.[25]

The Court clearly saw the involvement of a foreign power as a crucial factor demarcating two constitutionally distinct realms. Prior to 2005, the Foreign Intelligence Surveillance Act tracked this distinction, enabling broad surveillance—subject to the oversight of a secret court, and governed by laxer restrictions than apply in domestic criminal investigations—of persons demonstrated to be tied to foreign powers, including international terrorist groups.[26] Absent the involvement of such a foreign power, the salient considerations bearing on investigations of true lone wolves are nearly indistinguishable from those that apply to investigation of domestic terrorists and violent criminals. While the *Keith* Court did suggest Congress might create procedures for domestic national security investigations distinct from those governing criminal investigations, the Lone Wolf provision simply adds an additional trigger condition to a framework otherwise exclusively used for investigations of foreign powers.

FISA's definition of international terrorism still requires some foreign "nexus" before a suspected lone wolf can be targeted, but the statute provides only the vague guidance that its aims or methods "transcend" national boundaries. Construed strictly, this

might be sufficient to keep the boundary between foreign and domestic intelligence intact. But Justice Department officials have suggested that the definition would cover a suspect who "self-radicalizes by means of information and training provided by a variety of international terrorist groups via the Internet," which potentially makes a YouTube clip the distinction between a domestic threat and an international one.[27] Activities "in preparation" for terrorism, according to the legislative history, may include the provision of "personnel, training, funding, or other means" for either a particular act of terrorism or for a group engaged in terrorism.[28]

The FISA definitions of an agent of a foreign power applicable to citizens explicitly require that a U.S. person targeted under the statute must knowingly assist a foreign power. They also prohibit investigations conducted exclusively on the basis of protected First Amendment activities, such as political advocacy.[29] There are no such explicit limitations in the Lone Wolf provision.

Moreover, while international terrorism is defined by statute, an analysis by the Syracuse University's Transactional Records Access Clearinghouse, a research institution focused on government oversight, suggests that government entities apply the classification inconsistently. Federal prosecutors decline to bring charges in a substantial majority of the terrorism cases referred for prosecution by intelligence and law enforcement agencies, but in the recent cases where charges *have* been brought, more than a quarter of defendants identified as terror related by the Justice Department's National Security Division were not so categorized by prosecutors. Only 8 percent of defendants appeared on all of three lists of terror-related cases independently compiled by the Justice Department, federal prosecutors, and federal courts.[30] In light of this discrepancy—and especially in the absence of the scrutiny imposed by a sunset—there are grounds to worry that removing the bright-line requirement of a link to a foreign power may permit the FISA process to be invoked for investigations involving non-citizens that would more properly be classified as criminal inquiries.

The Broad Scope of FISA Surveillance

Though the evidentiary showing needed to target a person under FISA is looser than under criminal law, the surveillance powers it affords are substantially broader. So-called "Title III" wiretaps in criminal cases require evidence of a "nexus" between suspected criminal activity and each location or communications facility monitored.[31] Even then, agents are only supposed to record conversations that are pertinent to the investigation.

Once someone is designated as an agent of a foreign power, by contrast, information collection is "heavily weighted toward the government's need for foreign intelligence information," meaning that "large amounts of information are collected by automatic recording to be minimized after the fact," with the minimization of irrelevant information occurring "hours, days, or weeks after collection."[32] In general, FISA "permits acquisition of nearly all information from a monitored facility or a searched location."[33] And as the discussion of the other provisions analyzed below should make clear, even casual associates of a target of FISA surveillance become susceptible to acquisition of private records detailing their activities.

Even when information has been formally minimized, it may remain, in practice, available to intelligence agencies. In the 2003 case *U.S. v. Sattar*, the FBI had reported that it had conducted FISA surveillance subsequent to which "approximately 5,175 pertinent voice calls . . . were not minimized." When it came time for the discovery phase of a criminal trial against the FISA targets, however, the FBI "retrieved and disclosed to the defendants over 85,000 audio files . . . obtained through FISA surveillance."[34] Moreover, while targets of Title III surveillance are typically eventually informed of the eavesdropping, after the investigation has finished, FISA targets are not—enhancing the secrecy of intelligence practices, but removing a powerful check against abuses.[35]

Removing the bright-line requirement of a link to a foreign power may permit the FISA process to be invoked for investigations that would more properly be classified as criminal inquiries.

Recommendations

In sum, any investigation authorized under FISA will tend to sweep quite broadly, collecting a more substantial volume of information about innocent Americans than would be the norm under Title III wiretaps. These significant differences may make sense in the context of spying aimed at targets who have the resources of a global terror network to draw upon, and who will often be trained to employ sophisticated countersurveillance protocols in their communications with each other.

The need for secrecy is heightened when the target is a member of a larger group generally beyond the immediate reach of U.S. authorities—a group that may even have some capability to infiltrate traditional law enforcement systems. The interest in continued investigation of that larger group—whether by turning or simply continuing to monitor their agent in the United States—also means that intelligence investigations may not have criminal prosecution of the target as their goal. As a rule, these considerations simply do not apply to genuine lone wolves.

In the absence of the special needs created by the involvement of foreign powers, then, reliance on the more stringent provisions of Title III should be the norm. This should pose no problem for investigators, because any application meeting the standard for the Lone Wolf provision, if legitimately construed to cover actual terror plotters, will also meet the standards of Title III.

Because Lone Wolf authority does not yet appear to have been invoked, it is difficult to gauge the appropriate level of concern about its potential future uses. Since, however, it does not appear to have been necessary in practice, and by its own terms would only properly apply when parallel criminal authorities would also be available, there is little good reason to leave it on the books.

Roving Wiretaps

Section 206 of the Patriot Act established authority for multipoint or roving wiretaps under the auspices of the Foreign Intelligence Surveillance Act. The idea behind a roving wiretap should be familiar to fans of the acclaimed HBO series *The Wire*, in which drug dealers rapidly cycled through disposable "burner" cell phones to evade police eavesdropping. A roving wiretap is used when a target is thought to be employing such measures to frustrate investigators, and allows the eavesdropper to quickly begin listening on whatever new phone line or Internet account her quarry may be using, without having to go back to a judge for a new warrant every time. In 2009, FBI Director Robert Mueller testified that roving authority under FISA had been used 147 times.[36]

Roving wiretaps have existed for criminal investigations since 1986.[37] There is broad agreement, even among staunch civil libertarians, that similar authority should be available for terror investigations conducted under the supervision of the Foreign Intelligence Surveillance Court.[38]

Serious civil liberties concerns remain about the specific statutory language authorizing roving intelligence wiretaps.

Serious civil liberties concerns remain about the specific statutory language authorizing roving intelligence wiretaps, however. To understand why, it's necessary to examine some of the broad differences between electronic surveillance warrants under FISA and the Title III wiretaps employed in criminal investigations.

The Fourth Amendment imposes two central requirements on warrants authorizing government searches: "probable cause" and "particularity."[39] Under Title III, that means warrant applications must connect the proposed surveillance to some specific criminal act, and must "particularly [describe] the place to be searched and the persons or things to be seized." For an ordinary non-roving wiretap, law enforcement satisfies that requirement by establishing a nexus between evidence of a crime and a particular place (such as a phone line, an e-mail address, or a physical location). This will often involve a named target, but it need not. For example, a warrant might be obtained to bug a location known to be used for gang meetings, or a mobile phone used to discuss criminal

activity with another target already under surveillance, even if the identities of the persons making use of those facilities are not yet known. The requirement of a demonstrable nexus to criminal activity remains, however. Authority to bug Tony Soprano's office will not entail a power to eavesdrop on his therapy session or bug his bedroom, absent good reason to think he's discussing mob activity in those places. Since places and communications facilities may be used for both criminal and innocent purposes, the officer monitoring the facility is only supposed to record what's pertinent to the investigation.

When a roving wiretap is authorized under Title III, things necessarily work somewhat differently.[40] For roving taps, the warrant application shows a nexus between the suspected crime and an identified target person rather than a particular facility. Then, as surveillance gets underway, the eavesdroppers can "go up" on a line once investigators have "ascertained" that the target is "proximate" to a location or communications facility. Perhaps in part because they require an additional showing that a traditional facilities-based wiretap is unlikely to succeed, these broad warrants are used relatively sparingly: only 16 were issued in 2009 at the state level, and none at the federal level.[41]

Problems of Particularity

A number of Fourth Amendment challenges have been raised to Title III criminal roving wiretaps, on the grounds that a warrant naming a target, rather than a specific place or facility, cannot meet the constitutional particularity requirement. In rejecting such challenges, the courts have invariably stressed that, in the modern context, the substitution of a *named target* for a named facility is a key feature that allows Title III multipoint wiretap orders to pass the particularity test. For instance, in *United States v. Bianco*, the Court of Appeals for the Second Circuit emphasized that:

> unlike other orders under Title III, which requires identification of the anticipated speaker only "if known," Section 2518(1)(b)(iv), to satisfy the roving intercept statute, the person targeted for roving interception must be identified, and only conversation involving the specified individual may be intercepted.[42]

Similarly, in *United States v. Petti*, the Ninth Circuit wrote:

> The statute does not permit a "wide-ranging exploratory search," and there is virtually no possibility of abuse or mistake. Only telephone facilities actually used by an identified speaker may be subjected to surveillance, and the government must use standard minimization procedures to ensure that only conversations relating to a crime in which the speaker is a suspected participant are intercepted.[43]

The Patriot Act's roving wiretap provision, however, includes no parallel requirement that an individual target be named in a FISA warrant application, giving rise to concerns about what have been dubbed "John Doe" warrants that specify *neither* a particular interception facility *nor* a particular named target.

An amendment in 2006 did at least add the requirement that the description identify a specific target—which would *appear* to entail that each target must be a particular individual person, rather than some indeterminate group or class of persons satisfying a general characterization. But when the identity of the target cannot be determined conclusively, this too becomes difficult to guarantee. So, for example, an application targeting the person residing at a particular location or using a particular phone will be indeterminate in scope if (unbeknownst to the applicant) multiple people in fact fit the description—rendering the communications of those other (potentially innocent) persons over multiple facilities susceptible to interception. A similar error may cause an

Challenges have been raised to Title III criminal roving wiretaps on the grounds that a warrant naming a target cannot meet the constitutional particularity requirement.

An *identity*—as opposed to a description—is a key to a broad universe of records, and thus provides a multidimensional stream of information that can be used for error correction.

agent to follow the wrong person to a new facility in the case of a warrant with a named target—but then, at least, the fact that there clearly *is* a wrong person enables the error to be corrected more readily and acquisitions falling outside the scope of the warrant to be decisively identified.

A reported intelligence violation uncovered by a Freedom of Information Act request from the Electronic Frontier Foundation provides a concrete illustration of the point.[44] In an investigation of an apparently named, identified couple under FISA roving authority, a clerical error resulted in a line no longer used by the targets being included in an order renewing electronic surveillance. Subsequently, a phone apparently used by a young child was monitored for five days until agents realized the mistake. The error was detected, in part, because technicians noticed that the subjects identified in the warrant had previously been assigned the targeted line, but disconnected their service. Knowledge of the identity of the subjects also gave analysts a series of expectations about the parties to the communication, against which the fruits of surveillance could be checked. An *identity*—as opposed to a description—is a key to a broad universe of records, and thus provides a multidimensional stream of information that can be used for error correction. It might become apparent, for example, that a phone is making calls from one location when the target specified in the warrant is known to be elsewhere. When the target is known only by a description sufficiently specific to enable targeting of a wiretap, robust error correction is far less likely.

The Risks of "John Doe" Warrants

While permitting John Doe warrants under Title III would be problematic for all these reasons, the risk of improper overcollection is actually far greater in the intelligence context because, as discussed above in the analysis of the Lone Wolf provision, FISA surveillance is in general far broader than its Title III counterpart. "[L]arge amounts of information are collected by automatic recording to be minimized after the fact," and that after-the-fact "minimization" may not always entail the destruction of the "minimized" information.[45] Had the case discussed above occurred under Title III, real-time minimization should have prevented recording of communications on the targeted line unless a known target could be positively identified as party to the conversation.

This risk may be especially high when surveillance involves the use of sophisticated online filtering technology at an array of unknown facilities. Such overcollection is a risk even when a target *is* named, because the global scope of the Internet increases the likelihood that (for example) multiple users with similar names, or who have connected from the same IP address at different times, will hold accounts at a new facility. In the course of a recent criminal investigation, for example, the FBI inadvertently obtained the full e-mail archives of an unrelated person because of a typo in a warrant application.[46] But the risk is greatly heightened without the anchor of a named target.

As an illustration, consider the hypothetical (but presumably representative) wiretap order described at a 2009 surveillance conference by attorney Joel M. Margolis, who handles government surveillance requests for the telecommunications company Neustar.[47] Margolis outlined the difficulties an Internet service provider might face interpreting an order instructing an ISP to target the keyword, or virtual identifier, "RedWolf" using Deep Packet Inspection technology.[48]

Targeting on a virtual identifier will often be perfectly legitimate, provided there is evidence that the person using that ID at a particular website or online service is acting as an agent of a foreign power. Indeed, in the case of a warrant naming a specific facility, "the person using the ID RedWolf might be an adequately specific characterization of the target *within the context of surveillance directed at that facility*. But even when there is an identified target, such monitoring creates an inferential gap between the individual target

and the mechanism used to acquire his communications. John Doe" warrants add a second inferential gap.

Investigators will presumably be fairly sophisticated about this; they are likely to understand, for instance, that evidence sufficient to target RedWolf at *one particular site* will not by itself justify acquisition on that identifier elsewhere on the Internet. But the probability of error is inevitably magnified when a descriptive targeting mechanism is transplanted across facilities, and especially when the target is unknown *independently* of that description. We are, as a result, far removed from the scenario in *Petti*, where there was "virtually no possibility of abuse or mistake."[49] In light of the range of powerful tools that will already be available to investigators by the time probable cause is established—including wiretaps of specified facilities, National Security Letters, and Section 215 orders—it should be possible to determine a name for most targets without an unacceptable delay. If this is not possible, however, we should question whether the same tools that are inadequate to yield a target's identity *will* permit that target to be reliably tracked from facility to facility.

Why Ex Post Oversight Isn't Enough

Congress made some effort to address such concerns when it reauthorized Section 206 in 2005, adding the aforementioned requirement that FISA applications describe a specific target. Under the revised roving statute, eavesdroppers must inform the FISA Court within 10 days of any new facility they eavesdrop on (60 days if cause for delay is shown), and explain the "facts justifying a belief that the target is using, or is about to use, that new facility or place."[50] That is a step in the right direction, but back-end checks and oversight are unlikely to be an adequate substitute for front-end limitations on the scope of covert surveillance, and indeed, may create a false sense of security.

Consider that in fiscal year 2008 alone, the FBI collected 878,383 hours (or just over 100 years) of audio, much of it in foreign languages; 1,610,091 pages of text; and 28,795,212 electronic files, the majority pursuant to FISA warrants. A recent audit of FBI backlogs by the Office of the Inspector General found that fully a quarter of the audio collected between 2003 and 2008 remained unreviewed (including 6 percent of counterterror acquisitions and 31 percent of counterintelligence acquisitions, the two categories covered by FISA wiretaps).[51] Meaningful independent review of this volume of intelligence collection must, in practice, be fairly superficial. Indeed, when the target is known only by description, a mistaken collection may not be immediately obvious even after the fact.

Other structural features of the criminal justice system do provide a form of de facto after-the-fact oversight for electronic surveillance in criminal investigations. Because Title III wiretaps aim at criminal prosecution, investigators must anticipate that they will be subject to a distributed form of de facto review by defense counsel, who have a right to seek discovery and a powerful incentive to identify any improprieties. Even when an investigation does not result in charges being brought, wiretap targets must be notified of the surveillance after the fact.[52]

FISA surveillance, by contrast, is covert by default, and often seeks intelligence for purposes other than criminal prosecution.[53] Even when the fruits of FISA collection are used at trial, discovery is far more limited.[54] Defenders of this and other Patriot Act provisions often assert that they only provide intelligence agencies the same tools available in criminal investigations, but almost invariably neglect the profound structural differences between criminal and intelligence law.

Recommendations

Because FISA surveillance is in practice subject to less robust ex post scrutiny, it is, if anything, *more* important to constrain the discretion of investigators in selecting target facilities at the acquisition stage. Ide-

Defenders of the FISA provision and other Patriot Act provisions almost invariably neglect the profound structural differences between criminal and intelligence law.

ally, Congress should impose a requirement, parallel to Title III, that the target of a roving wiretap be a named individual—as in all likelihood is already the case for the vast majority of the 22 roving FISA wiretaps issued, on average, each year. For the small number of unnamed targets, the array of other FISA tools that would already be available—including facilities-based wiretaps and authority to acquire business records—should enable identification of the target before roving surveillance begins. With that change, FISA roving authority could safely be made permanent.

If experience with previous roving investigations suggests that greater flexibility is truly essential, FISA could permit a John Doe application to make the showing needed to justify roving authority, but remain limited upon issuance to a specified set of facilities. Roving authority would be triggered only after agents had positively identified the John Doe target, and made a submission to the FISA Court of the facts supporting the conclusion that the target described in the initial order had been identified. The FISA Court would need to ratify this identification within a relatively short period—10 days seems reasonable—but without the need to approve an entirely new application. With the latter modification, roving authority could be renewed, but should not be made permanent without a further period of review.

In either case, the Justice Department's annual FISA report to Congress should be required to include a tally of the number of roving orders issued each year and, if applicable, the number of those issued without a named target. To the extent possible, any opinion of the FISC involving substantive interpretation of the scope of roving wiretap authority should be made available in a public, redacted version. Finally, Congress should direct the Justice Department's Office of the Inspector General to conduct periodic audits of roving wiretap orders and prepare reports on their use, which should be redacted as necessary to permit public release.

Third-party custodians of records would have few incentives beyond sheer public-spiritedness to expend resources challenging Section 215 orders.

Section 215 Orders

Section 215 of the Patriot Act vastly expanded the ability of investigators to compel the production of sensitive records. Between 1998 and 2001, FISA allowed the Foreign Intelligence Surveillance Court to issue orders demanding records from a few specified categories of business, provided the FISC found there to be "specific and articulable facts" supporting the belief that the records pertained to a "foreign power or an agent of a foreign power."[55] During that time, the business records authority was invoked only once.[56]

The Patriot Act expanded this authority in three crucial respects. It removed the limitation on the types of businesses to which production orders could be issued; it expanded the items covered by the orders from business records to any "tangible thing"; and perhaps most importantly, it removed any requirement that the information sought pertain to a person suspected of involvement with terrorism or a foreign government.

These demands are subject to gag orders prohibiting the recipients from disclosing their existence. Unlike National Security Letters, these gag orders are at least imposed by a federal judge, but their breadth and the highly deferential standard of review to which they are subject parallels language in the NSL statutes that has already been held incompatible with the Fourth Amendment by the U.S. Court of Appeals for the Second Circuit.[57] Third-party custodians of records would have few incentives beyond sheer public-spiritedness to expend resources challenging these orders under any circumstances, and fewer still when the reviewing judges are instructed to treat the mere assertion of a national security need for secrecy as "conclusive."[58] A challenge under such a standard requires a willingness to tilt at windmills with a gold-plated lance.

The initial wording of Section 215 required only that the records be sought for a foreign-intelligence investigation. Congress subsequently raised this standard, requiring

a recitation of facts providing "reasonable grounds to believe" that the information is relevant to an authorized investigation to protect against terrorism *or* an intelligence investigation whose target is not a U.S. person.[59] This is "an undemanding standard that requires the government to show that the tangible things may have a bearing on or produce information probative of the investigation."[60] But the FISC is further required to find that records are *presumptively* relevant on a showing that they pertain to an agent of a foreign power, a person in contact with an agent of a foreign power, or the activities of such an agent.[61]

In the modern context, that standard permits the acquisition of a wide array of sensitive information about an enormous number of Americans with no connection to terrorism, on the basis of the most tenuous connection to any actual suspect. "When combined with the broad sweep of the three areas in which a tangible-things order is presumptively relevant," according to the manual coauthored by the former head of the Justice Department's National Security Division, "FISA appears to allow the government to obtain a tangible-things order with a minimal showing that the items it seeks are connected to the activities of a foreign power or agent of a foreign power." This might include, for example, "the bank records of the grade school teacher of the child of a person who is suspected of being an agent of a foreign power."[62]

Like National Security Letters—which are issued entirely without advance judicial approval—Section 215 orders need not be supported by the individualized suspicion or finding of probable cause normally required for a Fourth Amendment search. In both cases, the legal theory underpinning such a procedure is the so-called "third-party doctrine," which rests on the dubious proposition that persons normally waive their "reasonable expectation of privacy" when they provide documents to third parties, even when those parties are contractually or statutorily bound to confidentiality.[63]

How Protected are Third-Party Records?

During the initial debate over the Patriot Act, Senator Leahy justified the expansion of Section 215 on the grounds that "the Fourth Amendment does not normally apply to such techniques and the FBI has comparable authority in its criminal investigations."[64] Supporters of the provision, since the Act's passage, have routinely invoked similar comparisons to such tools as administrative- or grand-jury subpoenas, despite significant differences between these authorities.[65]

While a detailed analysis of the third-party doctrine is beyond the scope of this paper, it bears noting that it has long been the subject of blistering criticism by legal scholars, especially as technological change has increased the quantity of personal information about each of us held by third parties.[66] One of its lonely defenders in the academy has characterized it as "the Fourth Amendment rule scholars love to hate. . . . the *Lochner* of search and seizure law, widely criticized as profoundly misguided."[67] Numerous state supreme courts have rejected it, in whole or in part, under state constitutional provisions parallel to the Fourth Amendment.[68]

If we stipulate the general validity of the third-party doctrine for the sake of argument, however, it is worth noting that it has traditionally been applied precisely to *records*, retained by firms whose employees have access to them for ordinary business purposes. It is not a blanket Fourth Amendment exception for *any* item in the possession of a third party. The exception does not, for instance, extend to the contents of rented storage lockers.[69] A recent appellate ruling has similarly suggested that it does not apply to the contents of remotely stored e-mail, which a 25-year-old federal statute had hitherto permitted to be obtained without a probable-cause warrant in many circumstances.[70]

Even within the category of records, appellate courts have begun indicating that the third-party doctrine will not always apply. The Third Circuit recently held that location records held by mobile phone provid-

The relevancy standard permits acquisition of sensitive information about Americans with no connection to terrorism.

There are a range of First Amendment interests implicated by government access to online transactional data and other records that may reveal expressive activity.

ers *do* enjoy Fourth Amendment protection, in part because "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[71] A parallel argument could easily be made for much of the transactional information, or metadata, generated by online activity and collected by websites or service providers.[72] As these cases should make clear, courts are still in the early very stages of grappling with the proper application of the Fourth Amendment to the Internet era.

Moreover, there are a range of distinct First Amendment interests implicated by government access to online transactional data and other records that may reveal expressive activity, which are explored in greater detail in the section dealing with National Security Letters below.[73] In brief: numerous courts have found that heightened scrutiny is necessary when the compulsory production of records would burden the right to speak, read, or associate anonymously. Judges reviewing applications under Section 215 may, of course, take such considerations into account *sua sponte*, but with respect to covert national security investigations, recipients of these orders will typically have neither the incentive nor—just as crucially—the information necessary to mount an effective challenge on these grounds when appropriate.

Language in the amended Section 215 does explicitly limit the scope of orders to items that could be obtained via grand-jury subpoena or similar compulsory process.[74] But the secrecy surrounding the orders, coupled with the broad scope of "tangible things" authority, invites uses that push the boundaries of the already overbroad Fourth Amendment loophole upon which this authority is premised, even as courts begin moving to clarify and narrow it. Secret proceedings before the FISC are, to put it mildly, not the ideal forum to test the outer limits of an evolving area of law.

Section 215 in Practice

Fortunately—and owing in part to the substantial controversy surrounding Section 215—the Justice Department was at least initially relatively circumspect in its use of this authority, limiting itself to seeking actual business records during the period covered by the Inspector General's audits.[75] Indeed, expanded Section 215 authority was not used at all for two years after the passage of the Patriot Act, and appears to have been used relatively sparingly since then.[76] Moreover, the FISC appears to be fairly active in keeping the scope of Section 215 orders narrow: of the 21 sought in 2009, for example, the Court made modifications to 9 of the orders.[77]

There are, nevertheless, several reasons for concern. First, the relatively sparing use that has been made of Section 215 may is attributable in large measure to the extraordinary breadth of post–Patriot National Security Letters, which make a wide array of the most useful records available to investigators without the need for a court order. FBI agents interviewed by the Office of the Inspector General have made it clear that, in light of the substantial delays associated with Section 215 orders,[78] they are regarded as a tool of "last resort," employed only when National Security Letters or other authorities are unavailable.[79] Indeed, the first uses of the authority appear to have been motivated primarily by a desire to justify its existence to legislators: as a Justice Department attorney explained to the Office of the Inspector General, by the summer of 2003, "there was a recognition that the FBI needed to begin obtaining Section 215 orders because . . . Congress would be scrutinizing the FBI's use of the authority in determining whether to renew the authority."[80]

Should NSL authority be narrowed along the lines recommended below, however, it is highly probable that a sharp increase in the use of Section 215 would ensue. This would be an unambiguous improvement, insofar as it substituted judicial authority for agency fiat in compelling the production of records, but could lead to attenuated scrutiny unless adequate resources are allocated to the application-review process.

Second, the Justice Department's relatively conservative approach to Section 215 appears to be, at least in part, a function of the scrutiny associated with the authority's sunset. In popular discourse, the provision has often been referred to as the "library provision" because it has generated strong opposition from librarians chary of government inquiries into their patrons' reading habits.[81] In at least one case, investigators seeking production of library records were told that a "supervisor would not permit the request to go forward because of the political controversy surrounding 215 requests for information from libraries."[82] That reticence could easily diminish were the provision made permanent.

Finally—and perhaps most worryingly—testimony from Justice Department officials during the 2009 reauthorization debate revealed that Section 215 "supports an important sensitive collection program" about which a few select legislators had been briefed.[83] The heavily redacted public versions of reports from the Office of the Inspector General do not discuss uses of Section 215 connected with this program, which in any event appears to postdate the audit period. Lawmakers familiar with the program, however, have suggested that crucial "information about the use of Section 215 orders that . . . Congress and the American people deserve to know" is absent from the public debate.[84]

In 2005, legislative language narrowing Section 215 authority to require a factual showing that records being sought pertain to terrorists and spies, or their associates, had been approved unanimously by both the Senate Judiciary Committee and the full Senate, but was ultimately removed from the reauthorization bill signed by the president. When a similar reform was rejected in 2009, apparently as a result of a classified briefing in which intelligence officials alleged that such a modification would interfere with this "sensitive collection program," Sen. Richard Durbin (D-IL) complained:

> [T]he real reason for resisting this obvious, common-sense modification of Section 215 is unfortunately cloaked in secrecy. Some day that cloak will be lifted, and future generations will whether ask our actions today meet the test of a democratic society: transparency, accountability, and fidelity to the rule of law and our Constitution.[85]

The most troubling and direct statement on the subject came from former senator Russ Feingold (D-WI), then a member of both the Intelligence and Judiciary Committees, who asserted that he had become aware of specific abuses of Section 215 unknown to the general public and, indeed, to most members of Congress:

> I recall during the debate in 2005 that proponents of Section 215 argued that these authorities have never been misused. *They cannot make that statement now; they have been misused***.** I cannot elaborate here, but I recommend that my colleagues seek more information in a classified setting. [Emphasis added.][86]

In short, while the limited public reporting on the use of Section 215 indicates that it was used relatively conservatively through 2006, there are ample grounds for concern that the provision's broad language permits far more sweeping information collection about innocent Americans—and, indeed, there are hints that steps in this direction may have already been taken.

Recommendations

Notwithstanding these concerns, greater future reliance on a properly circumscribed Section 215—as a substitute, in many cases, for National Security Letters, which lack adequate judicial supervision—would constitute a significant improvement from a civil liberties perspective, and the Justice Department and FISC should be allocated such resources as may be necessary to render

Former senator Russ Feingold (D-WI) asserted that he had become aware of specific abuses of Section 215 unknown to the general public.

Section 215 should be tightened so as to foreclose the possibility of fishing expeditions through the sensitive records of innocent Americans.

this feasible. In order to effectively play this role, Section 215 authority that is somewhat more expansive than what existed under the pre–Patriot Act FISA may be appropriate. To compensate for the heightened risks to civil liberties inherent in covert intelligence gathering, however, the scope of Section 215 orders and the standard of review FISC judges apply to them should be tightened so as to foreclose the possibility of fishing expeditions through the sensitive records of innocent Americans only tenuously connected to terror suspects.

First, in light of the evolving state of jurisprudence concerning data entrusted to third parties, Section 215 authority should be explicitly restricted to business records whose subjects lack a Fourth Amendment expectation of privacy in their contents. This would clarify that Section 215 does not apply, for example, to private documents held by cloud-based storage systems, or to the increasingly precise and detailed information about a person's day-to-day physical movements that may be derivable from mobile-device records. It would also recognize explicitly that courts continue to grapple with the question of how far citizens' "reasonable expectation of privacy" extends to other records created by third-party information processing, but not normally subject to human review.[87] FISA's physical search and electronic surveillance authorities, subject to a probable-cause standard, would remain available for protected records and other tangible things.

Second, the presumption of relevance for certain categories of records—which the attorney general has previously indicated the Justice Department does not require—should be repealed.[88] Instead, applications for a Section 215 order should be required to cite specific and articulable facts demonstrating that the records sought are *both* relevant to an investigation *and* fall under one of three categories: records pertaining to a suspected agent of a foreign power who is the subject of an authorized investigation, to persons in contact with such suspected agent, or to the activities of such a person or group when this is the least intrusive available means of identifying the persons involved in those activities.[89]

This dual requirement would give FISC judges a clearer basis for evaluating the evidentiary showing in Section 215 applications, and ensure that something beyond mere casual contact with a suspect justifies acquisition of Americans' sensitive records. At the same time, the relative laxity of the relevance standard ensures that agents are not burdened with too high an evidentiary bar in the exploratory phases of an investigation. On the basis of the limited information available in the inspector general's public reports, it appears highly probable that most—if not all—of the Section 215 orders issued between 2003 and 2006 would already meet this standard. Where there is a compelling argument for broader routine access to specific types of records, and such access would have minimal effect on speech or privacy interests, Congress may wish to consider more narrowly tailored legislation, along the lines of the rules governing importation or sale of certain precursor chemicals for narcotics or explosives.

Finally, the process for challenging Section 215 gag orders should be explicitly altered to comport with the Second Circuit's ruling in *Doe v. Mukasey*, which held that a parallel review process in the National Security Letter statutes failed to adequately respect the First Amendment interests of recipients.[90] That standard requires recipients to wait a full year before challenging a nondisclosure order, burdens them with establishing that there is "no reason" to believe disclosure "may" interfere with any investigation or harm national security, and requires judges to treat certification by a high-ranking Justice Department official as "conclusive" on that question.[91]

The required one-year delay should be removed, and the burden of establishing some realistic likelihood of an identifiable harm shifted to the government. FISC judges will naturally—and appropriately—extend sub-

stantial deference to the government's assessment of such risks, but 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."[92] Nondisclosure orders should be narrowly tailored and, whenever possible, time limited to ensure recipients' speech rights are not constrained past the point necessary to protect national security. Similarly, the one-year delay imposed on challenges to the underlying orders—which denies recipients access to judicial review until long after the production of records—should also be removed.

While Section 215 could, in all likelihood, be made permanent if modified along these lines, it would be prudent to establish at least one additional sunset period to enable the Office of the Inspector General to audit the use of the amended authority—especially given that modifications to the National Security Letter statutes may substantially increase reliance on Section 215. If, as its proponents assert, this provision is not being used to engage in overbroad "fishing expeditions," these common-sense limitations should have a minimal practical effect on legitimate investigations.

National Security Letters

National Security Letters—once all but unknown to the general public—have emerged as perhaps the most controversial surveillance tool augmented by the Patriot Act and its successors, and with good reason.[93] This previously narrowly limited power was transformed into a sweeping mechanism enabling the FBI to acquire, without advance judicial approval, a wide array of sensitive information about Americans who are not even *suspected* of any connection with terrorism. As with Section 215 orders, the recipients are barred from disclosing the request. The ensuing explosion of NSLs has been characterized by government officials as a "hundred-fold increase over historic norms."[94] Perhaps unsurprisingly, the expanded authority has already been subject to what the inspector general called "widespread and serious misuse."[95]

NSLs have their origin in an exemption from federal privacy statutes created in the late 1970s, which permitted the voluntary disclosure of otherwise protected financial records when they concerned a suspected foreign spy. They have evolved over time into a set of extraordinarily broad compulsory tools akin to administrative subpoenas. NSLs now permit the FBI and certain other agencies to demand detailed financial records, consumer credit reports, and telecommunications transactional records without judicial authorization.[96] While there are currently five distinct NSL authorities, spread across four federal statutes, this paper will focus on the two types used exclusively by the FBI that account for the overwhelming majority of NSLs issued.

NSLs under the Right to Financial Privacy Act[97] are used to compel the production of records from "financial institutions," a statutorily defined category now encompassing a wide array of entities that, in the words of former Assistant Attorney General David Kris, "would not ordinarily be considered financial institutions."[98] NSLs under the Electronic Communications Privacy Act[99] are used to obtain telephone and Internet transaction records. They may be served on traditional telecommunications firms and Internet service providers, but also any other online service that gives users "the ability to send messages or communications to third parties"—such as Facebook, Gmail, or AOL Instant Messenger.[100] The precise range of records that can be obtained with ECPA NSLs is currently contested, but the FBI has traditionally asserted the right to demand—and has apparently received—almost anything short of actual communications content.[101] The language of the statute refers to "toll records"—traditionally meaning records of telephone numbers dialed and received—but in the modern era is generally understood

National Security Letters have emerged as perhaps the most controversial surveillance tool augmented by the Patriot Act with good reason.

to encompass Web IP addresses visited and e-mail sender and recipient addresses, at the very least.

The Patriot Act and subsequent intelligence legislation vastly expanded these authorities along multiple dimensions. The most significant is the removal of any requirement of a link to a suspected foreign power. Previously, NSLs applied only the records of persons suspected, on the basis of "specific and articulable facts," of being foreign spies (or to their contacts, if only basic subscriber information was sought).[102] In their current form, NSLs need only certify that the records sought are relevant to an authorized investigation, according to the FBI's own determination.

As the Justice Department itself explains, this "minimal evidentiary predicate . . . 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."[103] While the more limited pre-Patriot authority required direct approval by a high-ranking official at FBI headquarters, power to issue NSLs has now been delegated to the Special Agents in Charge of all 56 FBI field offices.[104]

Even the weak limitation of a required connection to an authorized investigation is ultimately subject to executive branch discretion: two years *after* the passage of the Patriot Act, the Attorney General's guidelines for national security investigations were revised to permit "preliminary" inquiries—which the FBI acknowledges are subject to "no particular standard of proof"—to count as "authorized investigations."[105] Though previously restricted to full investigations, nearly half of the NSL requests in the years following the guideline change were issued in connection with preliminary inquiries.[106]

Later amendments also dramatically expanded the scope of NSLs for financial records, allowing them to be served not only on traditional financial institutions, such as banks and credit card companies, but also:

> insurance companies, pawnbrokers, dealers in precious stones or jewels, travel agencies, telegraph companies, licensed money transfer companies, automobile dealers, real estate closing companies, casinos, the Post Office, government agencies involved in financial transactions, and any other business "whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters."[107]

RFPA NSLs, therefore, now cover "almost any record" in the custody of "virtually any commercial or government entity that handles cash transactions with customers."[108]

The problem was not inadequate information *collection*, but inadequate sharing and analysis of information already collected.

The Explosive Growth of Post-Patriot NSLs

Three extensive reports from the Office of the Inspector General show that the dramatic expansion of these authorities has led to an equally dramatic increase in their use.[109] While no reliable data exists for 2001–2002, the OIG counted nearly 200,000 NSL requests issued by the FBI from 2003–2006, with more than 56,000 issued in a single year—up from the 8,500 issued in 2000.[110] As the OIG notes, however, poor recordkeeping and reporting in the early years mean that the true figure is almost certainly substantially higher.[111]

Moreover, the proportion of those requests pertaining to U.S. persons has risen sharply over time. In 2003, roughly 39 percent of NSL requests were related to investigations of citizens or legal residents. By 2006, that figure had risen to 57 percent—meaning a total of 11,517 Americans had their records scrutinized pursuant to NSL authorities.[112]

The figures calculated by the OIG are not strictly comparable to those reported to Congress by the Department of Justice each year, which include only NSL requests pertaining to U.S. persons, and (perhaps more signifi-

cantly) exclude requests for basic subscriber information under ECPA's NSL authority. Despite these limitations, more recent reports suggest that the FBI continues to rely heavily on NSLs. In 2009, the most recent year for which reported figures are available, the FBI issued 14,788 NSL requests for information about 6,114 U.S. persons (again, not counting requests for basic subscriber information).[113]

The vast majority of those Americans are almost certainly not even suspected of involvement in espionage or terrorism. As then assistant attorney general David Kris explained in 2009, NSLs are used to "sweep more broadly than just the individual who may end up being the defendant or identified as a terrorist precisely because [investigators] are trying to develop the case."[114] NSLs are often used to map a "community of interest" based on an initial suspect's "calling circle," a process that may entail gathering information about persons "two or three steps removed" from the target.[115] Often FBI officials who signed off on boilerplate NSL language seeking broad "community of interest" data "were not even aware that they were making such requests."[116] As the OIG noted, given the statutory requirement that records be obtained via NSL only following a determination of relevance by designated officials, this practice "violated the ECPA, the Attorney General's NSI Guidelines, and FBI policy."[117]

More Letters, Diminishing Returns

Agents interviewed by the OIG have generally indicated that they find NSLs highly useful—but as with Section 215 orders, much of this usefulness consists in generating new leads and then eliminating the probable dead ends.[118] While this is, of course, an important goal, the ease of NSL information gathering may also lower the threshold for which leads are worth pursuing. It may even create a vicious cycle, where gathering more information generates more leads, requiring that still more information be collected in order to shrink the ballooning pool of potential suspects. As Michael Woods, a former senior FBI attorney has explained, reflecting on the post-9/11 climate at the Bureau:

> All of a sudden, every lead needed to be looked at. The atmosphere was such that you didn't want to be the guy who overlooked the next Moussaoui. . . . If you're telling the FBI people over and over you need to be preemptive, you need to get out there before something happens, you're pushing people toward a fishing expedition. We heard over and over again, connect the dots, and we were pushing the envelope and doing things that, in the old days, would have seemed beyond the pale.[119]

This makes sense, however, only if the inability to exhaustively pursue a large number of lower-threshold leads is a significant cause of intelligence failure. But there is little evidence for this proposition. Several perpetrators of the 9/11 terror attacks—notably Khalid al-Midhar and Nawaf al-Hazmi—were known al Qaeda associates who had been monitored by the Central Intelligence Agency well before they entered the United States. The failure to detect and disrupt that plot, then, cannot be attributed to an excessively high threshold for following up leads: those individuals plainly met any reasonable threshold for investigation, and indeed, could clearly have been extensively monitored pursuant to pre-Patriot authorities. As in the case of Zacarias Moussaoui, the problem was not inadequate information *collection*, but inadequate sharing and analysis of information already collected.[120] Other provisions of the Patriot Act and subsequent legislation have properly aimed to remedy some of these structural (and, indeed, cultural) problems—but it is far less clear that a paucity of raw data prior to the expansion of NSL authority was a genuine problem requiring a solution.

Any tool used as frequently as NSLs will, of course, retrospectively be seen to have played a role in some successful investigations. But

Investigative efforts are expanding, with easier access to records enabling a larger number of investigations to be pursued with a lower threshold of suspicion.

Records were improperly obtained on reporters for the *Washington Post* and the *New York Times*—in violation of both the law and internal regulations.

this is a poor metric of their general utility, especially when their primary function is preliminary filtering of large numbers of people to identify individuals—such as terrorists—with extremely low frequency in the population. We do not normally test the general public for very rare diseases, because even a very accurate test will tend to produce an unacceptably high number of false positives for each accurate diagnosis.[121] In intelligence no less than in epidemiology, the proper policy question is not whether any particular tool generates some data that is useful in a successful investigation, but whether it provides enough *necessary* information at the margin—information that could not have been obtained using (for example) a combination of narrower, pre-Patriot NSLs and judicially authorized Section 215 orders—to justify the costs of diminished privacy and resources expended chasing false positives. On the basis of these very considerations, an independent review by an expert panel of the National Research Council has cautioned against reliance on predictive data mining in the War on Terror.[122]

Though it is difficult to say definitively without access to classified records, publicly available data provides some reason to believe we have passed the point of diminishing returns. Of the fraction of FBI terror investigations ultimately referred to U.S. attorneys in 2001, immediately after the 9/11 attacks, 66 percent resulted in prosecutions in 2002. By 2009, the number had fallen to 21 percent—meaning federal prosecutors were declining to pursue nearly 80 percent of the cases referred to them by the FBI.[123] The average prison sentence for international terrorism prosecutions resulting in convictions fell from 40 months in 2004 to 5 months in 2006, suggesting that the great majority involved offenses substantially less serious than planned attacks on Americans.[124]

In short, it seems at least plausible that investigative efforts are expanding to fill the available space created by enhanced authorities, with easier access to records enabling a larger number of investigations to be pursued with a lower threshold of suspicion. If it is argued that NSLs are necessary to quickly sort through large numbers of ultimately unproductive leads, we should at least insist on evidence that there is some measurable benefit to opening so many investigations in the first place. It is telling, as the American Civil Liberties Union notes, that "every time an NSL recipient has challenged an NSL in court, the government has ultimately withdrawn its demand for records"—a pattern that is extremely difficult to reconcile with claims that those demands are essential to safeguard against terror attacks.[125]

After investigations are closed—and regardless of whether they result in prosecution, or any grounds for suspicion that the persons whose records have been obtained are guilty of anything—"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."[126] Some 13,000 users, within both the FBI and other government agencies, have access to the billions of records contained in one of the most extensive databases, the Investigative Data Warehouse.[127] As recent large-scale releases of classified documents by the whistleblowing website WikiLeaks have shown, a single user in the digital era—whether acting from misguided idealism or more sinister motives—may be able to extract enormous quantities of sensitive information, even from putatively secure databases.[128]

A History of "Widespread and Serious Misuse"

Already, these sweeping authorities have been subject to widespread misuse. A review by the Electronic Frontier Foundation of some 800 violations of the law or internal guidelines reported to the Intelligence Oversight Board from 2001–2006 found that nearly a third involved National Security Letters.[129] Still more troubling, a small sample of case files reviewed by the OIG found that 22 percent contained potential violations that had *never* been reported, many involv-

ing the acquisition and retention of records beyond the legitimate scope of the NSL.[130]

Perhaps the most disturbing violations of the rules governing surveillance powers involve the use of so-called "exigent letters" and informal requests for telecommunications data to bypass the NSL approval and oversight process. Between 2003 and 2006, agents in the FBI's Communications Analysis Unit issued 722 of these exigent letters to obtain data from providers without appropriate legal process, often indicating that an NSL or subpoena would be provided later.[131] While ECPA does contain a provision covering disclosure in genuine emergencies, as when an attack is believed to be imminent, that exception was not invoked in these instances, and would have applied to only a tiny fraction of the putatively exigent cases.[132] Among those whose records were improperly obtained were reporters for the *Washington Post* and the *New York Times*—in violation of both the law and internal regulations requiring that the attorney general approve such requests.[133]

Still more incredibly, investigators sought records pertaining to more than 3,500 telephone numbers *without any process at all*, simply requesting records "verbally during telephone calls or visits to the providers' Communications Analysis Unit work stations, or on pieces of paper, such as Post-it notes."[134]

FBI officials would later attempt to cover these improprieties after the fact by issuing blanket NSLs covering hundreds of phone numbers.[135] But at least 266 phone numbers for which records were improperly acquired "were related to criminal investigations or domestic terrorism investigations for which NSLs are not an authorized technique under the ECPA NSL statute, the Attorney General's NSI Guidelines, or FBI policy."[136]

When the OIG interviewed the personnel responsible for these practices, it found that "no one could satisfactorily explain their actions," instead offering only "a variety of unpersuasive excuses."[137] Supervisors had, at one point, attempted to implement a database to track requests to telecommunications providers, but agents refused to use the new system "because they did not want the responsibility for inputting the data."[138] While it is conceivable that this reluctance stemmed from an extreme aversion to clerical work, it may also indicate that at least some of them may have had doubts about the legality of the prevailing practices. It is similarly telling that when information obtained by these extralegal means was later cited in the small sample of warrant applications to the secret Foreign Intelligence Surveillance Court reviewed by OIG, "FBI personnel filed inaccurate sworn declarations with the FISA Court to the effect that the subscriber or calling activity information was obtained in response to NSLs or a grand jury subpoena, when in fact the information was obtained by other means, such as exigent letters."[139] Again, while it is possible to ascribe these false statements to innocent error, they are also consistent with a desire to avoid FISC scrutiny of the use of exigent letters and informal requests.

The Nature of Intelligence Abuses

While the use of exigent letters was finally formally barred in 2007, it seems clear that the broad and discretionary nature of NSL authority was a key factor in allowing the practice to continue for several years—well after supervisors and Department of Justice attorneys became aware of it. While presumably *this particular form* of abuse is not now likely to continue, its scale and persistence confirms the general tendency for admirably dedicated investigators, precisely as a function of their dedication, to stretch the limits of their authority when unchecked by a neutral and detached magistrate. It demands too much to expect agents properly focused on what is expedient in a specific investigation to simultaneously balance their needs against the aggregate interest in preserving a general system of liberties and privacy protections.

Indeed, from a systemic perspective, excessive focus on particular "abuses" may be something of a red herring. It would, after

It would be troubling if the authority to acquire records were simply broadened so far that almost nothing counted as an abuse.

National Security Letters permit the collection and retention of an enormous amount of sensitive information about innocent Americans for the most part innocent.

all, be far more troubling if the authority to acquire records were simply broadened so far that almost nothing counted as an abuse. The real issue is that even if used precisely as intended, NSLs permit the collection and retention of an enormous amount of sensitive information about innocent Americans for the most part.

The history of intelligence abuses in the United States suggests that the existence of such large databases in itself increases the risk of abuse, even if the initial collection itself is consistent with the letter of the law. While our system of checks and balances is designed to exclude improperly obtained information at trial, historical abuses of intelligence surveillance have more often involved the extralegal use of information to intimidate or harass political dissidents, journalists, and even judges and legislators.[140] As the Senate committee headed by Sen. Frank Church summarized the results of its intensive investigation in the 1970s:

> Too many people have been spied upon by too many Government agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone "bugs," surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity.
>
> Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. Unsavory and vicious tactics have been employed—including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths. Intelligence agencies have served the political and personal objectives of presidents and other high officials. While the agencies often committed excesses in response to pressure from high officials in the Executive branch and Congress, they also occasionally initiated improper activities and then concealed them from officials whom they had a duty to inform.[141]

In many cases—although not all—the initial monitoring of domestic targets was itself improper, and there has been an understandable tendency to see this as the sine qua non of abuse. But in a 21st- century technological context, an enormous quantity of information about group political activities, which previously would have been obtainable only via targeted direct surveillance, may be derivable by means of sophisticated analysis of telecommunications metadata swept up in the course of facially legitimate investigations. Under rules that permit the sweeping collection of such data—especially if dead-end leads are both numerous and disproportionately concern unpopular (but nonviolent) political and religious groups—the potential for inappropriate future use of information will not necessarily be linked with improper intent at the acquisition stage. Minimization rules limiting retention and dissemination of data—which should be strengthened—can mitigate this risk to some extent. But harms of this type are inherently difficult to detect, and the mere existence of such massive databases has the potential to chill protected political activity.

Just Another Subpoena?

Like Section 215 orders, National Security Letters are routinely defended on the grounds that they only grant intelligence investigators "the same" authority that is available to criminal investigators via such mechanisms as administrative or grand-jury subpoenas.[142] Even in the criminal context, it bears noting that the routine investigative use of third-party document subpoenas is a late 20th-century development that has occasioned fierce criticism from Fourth Amendment scholars.[143] But these analogies also typically elide a number of important and fundamental differences between NSLs and the subpoenas typically used in criminal investigations.

While the grand jury, as it exists today, is often subordinate to prosecutors in practice, the "theory of its function," as Justice Antonin Scalia has written, "is that it belongs to no branch of the institutional Government, serving as a kind of buffer or referee between the Government and the people."[144] This "unique role in our criminal justice system" is intimately related to its broad investigatory powers, which may be exercised in service of "determining whether or not a crime has been committed."[145] This function bears the greatest resemblance to the most frequent use of National Security Letters—as a tool for exhaustively following-up leads, typically in order to close off unpromising avenues of investigation—except that recipients of grand-jury subpoenas are generally not subject to indefinite gag orders barring disclosure of their own testimony. Trial subpoenas issued at the discretion of federal prosecutors, by contrast, are bound by more stringent procedural restrictions: they are typically tied to a particular criminal offense that there are grounds for believing has been or will be committed, and they are meant to be relatively narrowly calculated to produce admissible evidence of that offense.[146]

Perhaps the most important practical difference, however, is that National Security Letters are fundamentally secret tools whose recipients are, in most cases, indefinitely bound from disclosing even their existence to the general public. The details of their use typically remain shrouded, not merely for the duration of a specific investigation, but effectively forever. This not only removes one important kind of check on the agents using the authority, but also importantly alters the incentives facing the recipients of demands for information.

A comparison with the recent case of *Gonzales v. Google* is instructive here.[147] The Internet search-giant Google moved to quash a subpoena seeking a sample of user search queries, which the government hoped would be relevant to its defense of the controversial Child Online Protection Act against a challenge by the American Civil Liberties Union. The company made clear that a primary basis for its challenge was the fear of losing users' trust, and that "even a perception that Google is acquiescing to the Government's demands to release its query log would harm Google's business."[148] Though relatively unmoved by this "business goodwill" argument, the court *sua sponte* raised its independent concerns about the implications of the request on the privacy of Google's users, and ultimately rejected the demand for even anonymized query logs. While Google's reputational interest did not prove decisive in blocking the demand for information, it did provide an important motive for the judicial review that allowed user privacy interests to be weighed against the government's need for information.

Contrast the track record of National Security Letters, where in many cases employees from major telecommunications firms not only failed to object to improper requests, but were to a substantial degree the *instigators* of the abusive practices.[149] In the sample of reported violations surveyed by the Electronic Frontier Foundation, more than *half* of those related to NSLs occurred because "the private entity receiving the NSL either provided more information than requested or turned over information without receiving a valid legal justification from the FBI."[150] In one particularly egregious

The potential for inappropriate future use of collected telecommunications metadata will not necessarily be linked with improper intent at the acquisition stage.

case, a provider responded to a request for e-mail "header information" with "two CDs containing the full content of all e-mails in the accounts."[151] As EFF concluded:

> Companies were all too willing to comply with the FBI's requests, and —in many cases—the Bureau readily incorporated the over-produced information into its investigatory databases.[152]

This presents a potentially serious problem, because even where the Fourth Amendment does not protect data against disclosure, government searches of telecommunications records, in particular, may implicate distinct First Amendment interests. The permanent secrecy surrounding National Security Letters—which, again, appear to be used primarily to obtain information about people who are not ultimately found to be engaged in wrongdoing—means that the recipients will typically lack both the information that would be necessary to determine when a challenge on First Amendment grounds might be appropriate and, as importantly, the incentive to do so.

Where the Fourth Amendment Meets the First Amendment

As Justice Powell observed in his majority opinion in the *Keith* case, national security investigations "often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech."[153] These concerns are far from hypothetical: in at least one case noted by the Inspector General, the FBI initially sought a Section 215 order for records, which the FISA court denied on the basis of First Amendment concerns. The Bureau then proceeded to obtain the very same records using National Security Letters, even though the NSL statutes are nominally subject to the same First Amendment constraints as Section 215 orders. [154]

In many cases employees from major telecommunications firms not only failed to object to improper requests, but were the *instigators* of the abusive practices.

One obvious interest implicated by NSLs seeking information about Internet activities is that of anonymous speech. The Supreme Court has held that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."[155] The Constitution itself, after all, owes its existence in no small part to the pseudonymously-published pamphlets we now know as *The Federalist Papers*.

For this reason, a growing number of courts have found it appropriate to apply heightened standards to civil subpoenas whose purpose is to uncover the identity of an anonymous online speaker.[156] While the precise standards employed vary from court to court, common features include a requirement of notice (via an intermediary) to the defendant before his identity is disclosed to the plaintiff, some prima facie showing to establish the strength of the plaintiff's case, and a judicial balancing of the plaintiff's interest against the burden on speech entailed by disclosure.[157]

The First Amendment protects not only the right to speak, but also a corollary "right to receive information and ideas."[158] Thus, some legal scholars have argued for a parallel right to read anonymously, which could similarly be burdened by NSLs targeting websites hosting controversial content.[159] Here, too, courts have suggested that subpoenas seeking to reveal the reading habits of a target would be subject to heightened scrutiny.[160] The Supreme Court of Colorado has extended this logic to impose heightened standards, even upon probable-cause search warrants "directed to bookstores, demanding information about the reading history of customers," on the grounds that they "intrude upon the First Amendment rights of customers and bookstores because compelled disclosure of book-buying records threatens to destroy the anonymity upon which many customers depend."[161]

There is no obvious reason to think this logic any less applicable to the Internet than

to bookstores—and, indeed, substantial circumstantial evidence that users rely, if anything, *more* heavily on the sense of anonymity the Web provides. For example, 40 percent of Internet users, by one estimate, visit pornographic websites each month.[162] More than a third have visited sites related to sensitive personal issues, such as online support groups or sites providing information about medical conditions.[163] The willingness of users to seek information on such sensitive topics will often depend on the belief that they remain anonymous in doing so.

Finally, the Supreme Court has recognized a First Amendment interest in "expressive association," holding in *NAACP v. Alabama* that "immunity from state scrutiny of membership lists" may be necessary to preserve the "right of the members to pursue their lawful private interests privately and to associate freely with others in so doing."[164] This is, necessarily, an interest that does not turn on whether a third party entity has access to the data in question. It is also an interest especially likely to be implicated as government agencies use NSL-derived data for link analysis aimed precisely at inferring group structures from patterns of communication. In the context of the War on Terror, there is ample evidence that the practice of using NSLs to "follow every lead" is particularly likely to sweep in data about members of controversial (but peaceful) political and religious groups, even if only for the purpose of establishing the *absence* of a connection with more dangerous groups that may hold superficially similar radical views.[165]

Obviously, as organizations make use of e-mail and the Internet to communicate with and coordinate their membership, requests for telecommunications metadata will often tend to reveal such group associations—and when the organization itself is targeted, will be tantamount to straightforward acquisition of a membership roster. Suppose, for example, an NSL "community of interest" request takes as its starting point a member of a group mailing list devoted to political advocacy. The acquisition of the "second degree" transactional records for the list's e-mail address will not only, in effect, reveal the full membership list of the group, but is also likely to provide fairly detailed information about which are the most active participants. This is true not only with respect to traditional, formally incorporated political entities, but self-organizing ad-hoc groups, which legal scholar Katherine Strandburg has dubbed "emergent associations."[166] These kinds of informal, bottom-up associations may be especially sensitive to chilling effects, precisely because they will often lack the institutional resources to protect themselves possessed by more formal, traditional activist entities such as the NAACP.

National Security Letters, then, give us an unfortunate confluence of features. Confirming Justice Powell's warning, they seem especially likely to intrude on protected domains of religious or political speech and association, as they are used in a sweeping effort to preemptively identify the miniscule number of dangerous needles in a largely benign haystack. The extreme secrecy surrounding them, meanwhile, effectively eliminates the practical mechanism by which judicial scrutiny is often brought to bear when those interests are implicated by (intrinsically narrower) criminal investigations. All of this coincides with massively increased capabilities to process, share, and indefinitely store whatever data is obtained, exacerbating the risk that the aggregate information contained in government databases may be subject to pernicious uses unforeseen—and perhaps unforeseeable—at the time any particular piece of data is acquired.

Recommendations

There is little doubt investigators find NSLs useful and convenient. But given the risk to core civil-liberties interests posed by such sweeping and discretionary tools, convenience is an inadequate justification. The secret acquisition, without judicial approval, of sensitive records pertaining to presumptively innocent Americans should not be

National Security Letters seem especially likely to intrude on protected domains of religious or political speech and association.

countenanced without clear evidence that it is necessary to the prevention of serious harm to national security, and that any more limited authority would be insufficient to accomplish this goal. Nothing in the public record suggests that this burden can be met.

Of the five types of National Security Letters, ECPA NSLs for communications records present the most serious threat to protected privacy interests and civil-liberties interests. The Patriot Act's expansion of ECPA NSL authority to investigations designed to protect against international terrorism should be retained, along with the delegation of issuing authority to field offices, assuming ongoing centralized review. Its scope should otherwise be returned to its pre-Patriot limits. ECPA NSLs for "toll records" or their Internet equivalent should be limited to persons believed, on the basis of specific facts, to be agents of some foreign power. Any effort to expand their scope from toll records to electronic communications transaction records generally should be especially resisted, since the practical implications for privacy interests of such broad authority are effectively impossible to predict given the speed of technological change. More restricted NSLs, seeking basic subscriber information, should be available for persons in direct communication with those suspected agents.

The secret acquisition of sensitive records pertaining to presumptively innocent Americans should not be countenanced without clear evidence that it is necessary to the prevention of serious harm to national security.

This structure properly balances the need for investigative flexibility with the privacy interests of largely innocent parties. It allows analysts to determine the identities of persons with whom actual investigative subjects are in contact, but does not permit the exposure of potentially sensitive patterns of communication and association on the basis of any casual link to a single suspect. In combination with evidence obtained by other investigative means, this should enable agents to establish which persons require further scrutiny.

If there is some reason to think the records of particular parties in contact with a target are relevant to the investigation, but there are insufficient grounds for concluding that those parties are themselves agents of a foreign power, the information obtained at that stage can be employed to make the requisite showing to the FISA court for a Section 215 order seeking more-detailed records. This structure *still* grants enormous flexibility to investigators, permitting access to records pursuant to a relatively permissive standard, but ensures that records implicating core speech and association interests are not routinely obtained about innocent persons without the approval of an independent magistrate. While it may be tempting to insist that a court order be obtained for *all* records, this could have the perverse consequence of yielding greater intrusion, as agents would have an incentive to sweep as broadly as possible in a single order—obviating the need for multiple applications—even when more-limited records would suffice.

A similar process should obtain for financial-record NSLs. That is, they should permit investigators to obtain detailed records only for persons believed, on the basis of specific facts, to be agents of foreign powers. They may also permit identification of other parties to those transactions—such as the recipient of a wire transfer. Records of *those* parties, however, should be acquired pursuant to a Section 215 order following a judicial determination that the records are relevant. Because full credit reports generally contain less-sensitive and detailed information, and are attended by lesser expectations of privacy, the current standard for credit report NSLs may be adequate, provided future audits confirm they are being used in an appropriately narrow fashion.

As with Section 215 orders, the gag provisions of the NSL statutes should be modified to conform to the ruling in *Doe v. Mukasey*.[167] The oversight and minimization procedures which the Justice Department has already agreed to implement on a voluntary basis should similarly be codified in statute to ensure they are not quietly eroded by the decisions of future administrations.[168] In particular, when an investigation is closed without further legal or intelligence action

being taken, records obtained in the course of that investigation should be purged from FBI databases, by default, after some fixed period of time. There is no legitimate reason to indefinitely retain detailed information about tens of thousands of Americans who are not suspected of involvement in terror or espionage. Notwithstanding any changes, the myriad problems already identified with the use of National Security Letters, and the incredible scale of their use, suggests that this expanded authority should be subject to a sunset and regular auditing by the Inspector General to ensure that they are subject to continuing review.

Conclusion

It has become commonplace over the last decade to speak of the need to balance privacy and security interests. While it is certainly true that trade-offs between these values are sometimes inevitable, we should not allow the metaphor to mislead us into viewing them as inherently conflicting. Often we can have both.

The reforms proposed in this paper are guided by that principle: they seek to limit the government's ability to invade the privacy of innocent Americans without compromising the effectiveness of tools the intelligence community truly requires to detect and apprehend terrorists. In the climate of panic and uncertainty following the attacks of 9/11—with no clear understanding of how the attackers had gone undetected, how many more might be waiting to strike again, or what methods might prove necessary to detect them—it should not be surprising that we erred on the side of granting government more power with fewer restrictions. Now, with the benefit of a decade's experience, we have an opportunity to do better.

Notes

1. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

2. Editorial, "Stampeded in the House," *Washington Post*, October 16, 2001.

3. Pub. L. No. 108-458 and 118 Stat. 3638 §6001. References throughout this paper to "Patriot provisions" or "Patriot authorities" should be understood as shorthand encompassing Lone Wolf and other changes to surveillance powers made by subsequent legislation.

4. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 120 Stat. 192–277 (2006). For further background on the three sunsetting provisions, see Anna C. Henning and Edward C. Liu, "Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009," CRS Report R40138, December 23, 2009.

5. For a more detailed account, see Brian T. Yeh and Charles Doyle, "USA PATRIOT Improvement and Reauthorization Act of 2005: A Legal Analysis," CRS Report RL33332, December 21, 2006.

6. See, for example, House Judicary Committee, "Hearing on the USA PATRIOT Act," September 22, 2009, http://judiciary.house.gov/hearingshear_090922.html; and Senate Judiciary Committee "Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security," September 23, 2009, http://judiciary.senate.gov/hearings/hearing.cfm?id=4062.

7. The most serious abuses are documented in Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," January 2010, http://www.justice.gov/oig/special/s1001r.pdf. For a summary of earlier findings of improprieties, see David Stout, "F.B.I. Head Admits Mistakes in Use of Security Act," *New York Times*, March 10, 2007, http://www.nytimes.com/2007/03/10/washington/10fbi.html.

8. Hearing on the Report by the Office of the Inspector General of the Department of Justice on the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records, April 14, 2010, http://judiciary.house.gov/hearings/hear_100414.html. See also the earlier Hearing on: H.R. 3189, the "National Security Letters Reform Act of 2007," April 10, 2008, http://judiciary.house.gov/hearings/hear_041508.html.

9. See, for example, Charlie Savage, "Battle Looms Over the Patriot Act," *New York Times*, September 20, 2009, http://www.nytimes.com/2009/09/20/us/politics/20patriot.html.

10. For a summary of the main proposals and how they would have differed from current law, see the comparison chart produced by the American Civil Liberties Union, "Comparison Chart," September 30, 2009, http://www.aclu.org/images/general/asset_upload_file577_41249.pdf; and "A Breakdown of the H.R. 3845, The USA PATRIOT Amendments Act of 2009," October 27, 2009, http://www.aclu.org/national-security/breakdown-hr-3845-usa-patriot-amendments-act-2009. The American Association of Law Libraries' Issue Brief "USA PATRIOT ACT and PATRIOT Reauthorization: Section 215," June 2010, http://www.aallnet.org/aallwash/ib082009.pdf, includes a detailed timeline of reform proposals and legislative action.

11. Michael B. Farrell, "Obama signs Patriot Act extension without reforms," *Christian Science Monitor*, March 1, 2010, http://www.csmonitor.com/USA/Politics/2010/0301/Obama-signs-Patriot-Act-extension-without-reforms.

12. David Kravetz, "House Fails to Extend Patriot Act Spy Powers," *Wired*, February 8, 2011, http://www.wired.com/threatlevel/2011/02/patriot-act-notextended/.

13. Thomas Ferraro and Phillip Barbara, "Congress votes to renew anti-terrorism powers," *Reuters*, February 17, 2011, http://www.reuters.com/article/2011/02/17/us-usa-security-congress-idUSTRE71G47T20110217.

14. S. 149, "To extend expiring provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005, the Intelligence Reform and Terrorism Prevention Act of 2004, and the FISA Amendments Act of 2008 until December 31, 2013, and for other purposes," http://www.govtrack.us/congress/billtext.xpd?bill=s112-149.

15. Fahima Haque, "GOP Senators Back Permanent Extension of Patriot Act," February 4, 2011, http://www.mainjustice.com/2011/02/04/gop-senators-back-permanent-extension-of-patriot-act/

16. Press Release, "Leahy Renews Effort To Extend Expiring PATRIOT Act Authorities, Increase Oversight," January 26, 2011, http://leahy.senate.gov/press/press_releases/release/?id=16e3e765-00e7-48eb-add7-a64f415e9c1d. For a more detailed overview of proposals, see Edward C. Liu, "Amendments to the Foreign Intelligence Surveillance Act (FISA) Set to Expire February 28, 2011," CRS Report R40138 (February 10, 2011), http://www.fas.org/sgp/crs/intel/R40138.pdf; and Charles Doyle, *National Security Letters: Proposals in the 112th Congress*, CRS Report R41619, February 1, 2011.

17. P.L. 107-56, § 224(b); P.L. 108-458, § 6001(b).

18. See "Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities," S. REP. NO. 94-755 (1976) [hereinafter "Church Committee Report"].

19. The letter is available at http://www.wired.com/threatlevel/2009/09/obama-backs-expiring-patriot-act-spy-provisions/.

20. See, for example, Amy Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton: Princeton University Press, 2007).

21. Lieu and Henning, above at note 4.

22. Patrick Leahy, Charles Grassley, and Arlen Specter: "Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures," February 2003, http://www.fas.org/irp/congress/2003_rpt/fisa.html.

23. Ibid. §III(C)(1).

24. *United States v. U.S. District Court*, 407 U.S. 297 (1972). Although FISA wiretaps—unlike those at issue in the Keith case—do involve advance judicial approval, the Foreign Intelligence Surveillance Court has acknowledged that because surveillance orders under FISA and Title III "diverge in constitutionally relevant areas—in particular, in their probable cause and particularity showings—a FISA order may not be a 'warrant' contemplated by the Fourth Amendment." In re: Sealed Case, 310 F.3d 717 (2002).

25. *Id.*, majority opinion of Justice Powell at 309. See also *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), holding that the foreign intelligence exception to the conventional Fourth Amendment warrant requirement applies "only when the object of the search or the surveillance is a foreign power, its agent or collaborators" because of the enhanced "need for speed, stealth, and secrecy" as well as "difficult and subtle judgments about foreign and military affairs."

26. See Peter P. Swire, "The System of Foreign Intelligence Surveillance Law," 72 *Geo. Wash. L. Rev.* 1306 (2004), section II.

27. See letter from Ronald Weich, above at note 17.

28. See H.R. Rep. No. 1283, Pt. I, 95th Cong., 2d Sess. 1978 U.S.C.C.A.N. 4048 (June 8, 1978) at 43.

29. See David S. Kris and J. Douglas Wilson, *National Security Investigations & Prosecutions* (Eagan,

MN: Thomson/West, 2007) §8 [hereinafter "Kris and Wilson"].

30. Transactional Records Access Clearinghouse, "Who is a Terrorist," September 28, 2009, http://trac.syr.edu/tracreports/terrorism/215/.

31. Named for the Omnibus Crime Control and Safe Streets Act of 1968, Title III, Pub. L. 90-351, 82 Stat. 212 (June 19, 1968) (codified as amended at 18 U.S.C. §§2510-22) [hereinafter "Title III"].

32. In re *All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (2002).

33. Kris and Wilson, §9:4.

34. *U.S. v. Sattar*, 2003 WL 22510435 (S.D. N.Y. 2003).

35. See notes 50–52, below, and accompanying text.

36. Carrie Johnson, "Director of FBI Urges Renewal of Patriot Act," *Washington Post*, March 26, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/03/25/AR2009032501862.html.

37. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, §106(d)(3), codified at 18 U.S.C. §2581(11). For a more detailed history, see Peter M. Thompson, "White Paper on The USA PATRIOT Act's 'Roving' Electronic Surveillance Amendment to the Foreign Intelligence Surveillance Act" (Washington: The Federalist Society, April 2004), http://www.fed-soc.org/publications/pubID.130/pub_detail.asp.

38. See, for example, James X. Dempsey, "Why Section 206 Should Be Modified" in *Patriot Debates: Experts Debate the USA PATRIOT Act*, ed. Stewart A. Baker and John Kavanaugh (Chicago: ABA Publishing, 2005), http://www.abanet.org/natsecurity/patriotdebates/section-206, which raises many of the concerns outlined here while agreeing that "It makes perfect sense that the FBI should have roving tap authority in intelligence investigations of terrorists."

39. The "particularity" requirement is meant to limit the discretion of officers executing a warrant. See *Maryland v. Garrison*, 480 U.S. 79, 84, 107 S. Ct. 1013, 94 L. Ed. 2d 72 (1987).

40. See Kris and Wilson §6:12.

41. Administrative Office of the United States Courts, "Wiretap Report 2009," April 2010, http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2009.aspx.

42. *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993), cert. denied, 114 S. Ct. 1644 (1994).

43. *United States. v. Petti*, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 113 S. Ct 1859 (1993).

44. See Mark Rumold, "Documents Obtained by EFF Reveal FBI Patriot Act Abuses," *Deeplinks Blog*, March 31, 2011, https://www.eff.org/deeplinks/2011/03/documents-obtained-eff-reveal-fbi-patriot-act.

45. See note 31.

46. "FBI Typo Triggers Errant E-Mail Search," *The Smoking Gun*, December 3, 2010, http://www.thesmokinggun.com/documents/fail/fbi-typo-triggers-errant-e-mail-search.

47. Remarks of Joel M. Margolis at the ISS World Americas Conference on the panel "Regulatory and CALEA Issues Facing Telecom Operators Deploying DPI Infrastructure," October 13, 2009. A link to a recording of the panel by security researcher Chris Soghoian is at http://paranoia.dubfire.net/2010/01/who-is-neustar.html.

48. For an introduction to DPI technology and analysis of its interaction with surveillance law, see Paul Ohm ,"The Rise and Fall of Invasive ISP Surveillance" *University of Illinois Law Review* 1417 (2009), http://ssrn.com/abstract=1261344.

49. See note 42.

50. See Yeh and Doyle, above at note 5, pp. 16–18.

51. Office of the Inspector General, "The Federal Bureau of Investigation's Foreign Language Translation Program (Redacted for Public Release)," Audit Report 10-02, October 2009, http://www.justice.gov/oig/reports/FBI/a1002_redacted.pdf.

52. 18 U.S.C. §2518(8)(d).

53. See Kris and Wilson §22:1.

54. *Id*. §27–§30.

55. The orders could be served on "a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility." Pub. L. 105-282, Title II, §215, 112 Stat. 2411 (October 20, 1998); 50 U.S.C. §1672(a) (1998).

56. Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of Section 215 Orders for Business Records," March, 2007, http://www.usdoj.gov/oig/special/s0703a/final.pdf [hereinafter OIG 215 Report I].

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

58. 50 U.S.C. §1861(f)(2)(ii).

59. 50 U.S.C. §1861(b)(2)(a).

60. Kris and Wilson §18:3.

61. See Yeh and Doyle, above at note 5, and OIG 215 Report I, pp. ii–v.

62. *Id*. note 59.

63. See *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979).

64. 147 Cong. Rec. S10993 (October 25, 2001).

65. See, for example, "USA PATRIOT Act Debate," *PBS NewsHour*, PBS, December 13, 2005, http://www.pbs.org/newshour/bb/congress/july-dec05/patriot_12-13.html. For a more detailed discussion of differences between these authorities, see notes 140–150 below and accompanying text.

66. For a very partial sample, see Daniel Solove, "The Fourth Amendment, Records, and Privacy," in *The Digital Person: Technology and Privacy in the Information Age* (New York: NYU Press, 2004); Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007) pp. 151–64; Gerald G. Ashdown, "The Fourth Amendment and the 'Legitimate Expectation of Privacy,'" *Vand. L. Rev.* 34 (1981): 1289, 1315; Patricia Bellia, "Surveillance Law Through Cyberlaw's Lens," *Geo. Wash. L. Rev.* 72 (2004): 1375, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=556467; Jack M. Balkin, "The Constitution in the National Surveillance State," *Minn. L. Rev.* 93 (2008): 1, 19; Stephen E. Henderson, "Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too," *Pepp. L. Rev.* 34 (2007): 975–76; Susan Freiwald, "First Principles of Communications Privacy," *Stan. Tech. L. Rev.* 3 (2007): 46–49, http://stlr.stanford.edu/pdf/freiwald-first-principles.pdf; Jim Harper, "Reforming Fourth Amendment Privacy Doctrine," *American University Law Review* 58 (June 2008): 5, http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1045; Matthew Tokson, "Automation and the Fourth Amendment," *Iowa L. Review* 96 (2010) 581–647, http://www.uiowa.edu/~ilr/issues/ILR_96-2_Tokson.pdf.

67. Orin S. Kerr, "The Case for the Third-Party Doctrine." 107 *Mich. L. Rev.* (2009), http://ssrn.com/abstract=1138128.

68. See Stephen E. Henderson, "Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third Party Information from Unreasonable Search," *Cath. U. L. Rev.* 55 (2006): 373.

69. See *Murdock v. State*, 664 P.2d 589, 598 (Alaska Ct. App. 1983) ("[The petitioner] had a reasonable expectation of privacy in the property stored [in a rented locker] at the YMCA."); *Ferris v. State*, 640 S.W.2d 636, 638 (Tex. App. 1982) ("Under proper circumstances, a storage locker is a place entitled to Fourth Amendment . . . protection.")

70. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

71. In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F. 3d 304, 319 (3d Cir. 2010) at 317.

72. See, for example, Kashmir Hill, "History Sniffing: How YouPorn Checks What Other Porn Sites You've Visited and Ad Networks Test The Quality of Their Data," *Forbes*, November 30, 2010, http://blogs.forbes.com/kashmirhill/2010/11/30/history-sniffing-how-youporn-checks-what-other-porn-sites-youve-visited-and-ad-networks-test-the-quality-of-their-data/.

73. See notes 151–64 below and accompanying text.

74. 50 U.S.C. 1861(c).

75. See OIG 215 Report I at viii. Ironically, the Justice Department appears to have been more conservative than Congress: the OIG report explains that the Office of Legal Counsel initially concluded that Section 215 did not override separate statutory protections for sensitive educational and medical records. Only when Congress explicitly established heightened standards for acquisition of such records—apparently believing itself to be *raising* the level of protection afforded them—did OLC authorize their acquisition pursuant to this authority. Language in a subsequent Inspector General's report suggests that Justice Department attorneys remain reluctant to process requests that do not fall within the traditional definition of business records, however. See Office of the Inspector General, "A Review of the FBI's Use of Section 215 Orders for Business Records in 2006," March 2008, http://www.justice.gov/oig/special/s0803a/final.pdf [hereafter OIG 215 Report II] at 48.

76. In 2005, 141 "combination" orders under Section 215 were issued in tandem with "pen register" orders, which permit monitoring of numbers dialed from a target phone, in order to

obtain subscriber information about persons in communication with the primary target. Following the 2006 reauthorization, this information can be obtained automatically under the pen register order alone.

77. See Ronald Weich, "FISA Annual Report to Congress 2009," April 30, 2010, http://www.fas.org/irp/agency/doj/fisa/2009rept.pdf.

78. In 2006, the average processing time for approved Section 215 orders was 147 days—and even longer for applications ultimately withdrawn. Tellingly, no agents interviewed by the Inspector General could identify any harm to national security as a result of these delays. OIG 215 Report II at 43.

79. *Id*. at 55.

80. OIG 215 Report I at 54.

81. See American Library Association, "Resolution on the USA PATRIOT Act and Libraries," June 29, 2005, http://www.ala.org/ala/aboutala/offices/oif/statementspols/ifresolutions/usapatriotactlibraries.cfm.

82. OIG 215 Report I at 28.

83. Testimony of Todd Hinnen, House Judiciary Committee Hearing, above at note 6.

84. Statement of Sen. Russ Feingold, Senate Judiciary Committee Hearing, above at note 6, http://judiciary.senate.gov/hearings/testimony.cfm?id=4062&wit_id=4083.

85. Remarks of Sen. Richard Durbin, Senate Judiciary Committee "Executive Business Meeting," October 1, 2009) http://judiciary.senate.gov/resources/webcasts/index.cfm?changedate=09-28-09&p=all.

86. Remarks of Sen. Russ Feingold, *ibid*.

87. See Tokson, above at note 64. Note that the government has argued successfully—and plausibly—that purely automated filtering of electronic communications for the purpose of isolating those belonging to a surveillance target does not constitute "interception" of all filtered communications. This argument seems difficult to square with the premise that persons normally waive their expectation of privacy in data similarly processed by private entities. See testimony of Donald M. Kerr Assistant Director, Laboratory Division, FBI, Before the U.S. Senate Committee on the Judiciary (September 6, 2000), http://www.loc.gov/law/find/hearings/pdf/00089583263.pdf.

88. See Leahy press release, above at note 16.

89. This tripartite scheme is based on the proposal previously approved unanimously by the Senate, and reintroduced in 2009 by Sen. Russ Feingold as part of the Judiciously Using Surveillance Tools In Counterterrorism Efforts (JUSTICE) Act, http://www.eff.org/files/HEN09874.pdf.

90. *Doe v. Mukasey*, note 56, above.

91. 50 U.S.C. §1862(f)(2)(C).

92. *Doe v. Mukasey* at 47, above at note 56.

93. A search by Prof. Peter Swire turned up only two brief mentions of NSLs in newspaper stories written prior to 2002. See testimony of Peter P. Swire before the U.S. Senate Judiciary Committee's Subcommittee on the Constitution, "Responding to the Inspector General's Findings of Improper Use of National Security Letters by the FBI," April 11, 2007, http://judiciary.senate.gov/hearings/hearing.cfm?id=2679.

94. Barton Gellman, "The FBI's Secret Scrutiny; In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans," *Washington Post*, November 6, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html.

95. Statement of Glenn A. Fine Inspector General, U.S. Department of Justice, House Judiciary Committee Hearing "Misuse of Patriot Act Powers: The Inspector General's Findings of Improper Use of National Security Letters by the FBI," March 21, 2007, http://judiciary.senate.gov/hearings/hearing.cfm?id=2616.

96. For detailed background see Kris and Wilson §19:2; Charles Doyle, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, CRS Report RL33320, September 8, 2009, www.fas.org/sgp/crs/intel/RL33320.pdf; Swire above at note 25.

97. 12 U.S.C. §3414.

98. Kris and Wilson §19:2 note 16; see note 105 below and accompanying text for examples.

99. 18 U.S.C. §2709.

100. See U.S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence* (2009) §3(B), http://www.cybercrime.gov/ssmanual/03ssma.html#B.1; *Kaufman v. Nest Seekers*, LLC, 2006 WL 2807177, at note 5 (S.D.N.Y. Sept. 26, 2006); Becker v. Toca, 2008 WL 4443050, at note 4 (E.D. La. September 26, 2008).

101. See Ellen Nakashima, "White House pro-

posal would ease FBI access to records of Internet activity," *Washington Post*, July 29, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/07/28/AR2010072806141.html.

102. Statement of Glenn A. Fine.

103. U.S. Department of Justice, "FY 2006 Performance and Accountability Report," http://www.justice.gov/ag/annualreports/pr2006/2006par.pdf.

104. See Swire, above at note 92.

105. See Testimony of Lisa Graves, Senate Judiciary Committee hearing, above at note 6.

106. U.S. Department of Justice, Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of National Security Letters," March 2007, [hereinafter OIG NSL Report I].

107. Kris and Wilson §19:5, summarizing 31 U.S.C. §§5312(a)(2) & (c)(1).

108. *Id*.

109. See OIG NSL Report I; "A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006," March 2008 [hereinafter OIG NSL Report II]; "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," January 2010 [hereinafter OIG NSL Report III], http://www.usdoj.gov/oig/special/index.htm.

110. OIG NSL Report II at 9. NSL *requests* are counted rather than simply NSLs because a single physical letter may contain multiple discrete demands for information—and in a few cases, hundreds.

111. See OIG NSL Report I at xlv. ("Overall, we found approximately 17 percent more national security *letters* and 22 percent more national security letter *requests* in the case files we examined in four field offices than were recorded in the OGC database. As a result, we believe that the total number of NSL requests issued by the FBI is significantly higher than the FBI reported.")

112. *Id*. note 108.

113. *Id*. note 76.

114. Remarks of David Kris, Senate Judiciary Committee Hearing, above at note 6, http://www.fas.org/irp/congress/2009_hr/patriot2.html.

115. See OIG NSL Report I at 109; OIG NSL Report III at 54–64.

116. OIG NSL Report III at 57.

117. *Id*. at 60.

118. OIG NSL Report II at 114.

119. Eric Lichtblau, *Bush's Law: The Remaking of American Justice* (New York: Pantheon, 2008) p. 92.

120. See Zegart, above note 20, chap. 1; James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008), Book I.

121. See Jeff Jonas and Jim Harper, "Effective Counterterrorism and the Limited Role of Predictive Data Mining," Cato Institute Policy Analysis no. 584, December 11, 2006, http://www.cato.org/pub_display.php?pub_id=6784.

122. See National Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment* (Washington: National Academies Press, 2008).

123. Transactional Records Access Clearinghouse, "As Terrorism Prosecutions Decline, Extent of Threat Remains Unclear," May 18, 2010, http://trac.syr.edu/tracreports/terrorism/231/.

124. Transactional Records Access Clearinghouse, "National Profile and Enforcement: Trends Over Time," 2006, http://trac.syr.edu/tracfbi/newfindings/current/.

125. See American Civil Liberties Union, "Internet Archive's NSL Challenge," April 29, 2008, http://www.aclu.org/national-security/internet-archives-nsl-challenge.

126. OIG NSL Report I at 110.

127. Ellen Nakashima, "FBI Shows Off Counterterrorism Database," *Washington Post*, August 30, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/08/29/AR2006082901520.html.

128. See Thom Shanker, "Loophole May Have Aided Theft of Classified Data," *New York Times*, July 9, 2010, https://www.nytimes.com/2010/07/09/world/09breach.html.

129. Electronic Frontier Foundation, "Patterns of Misconduct: FBI Intelligence Violations from 2001–2008" (January 2011), http://www.eff.org/pages/patterns-misconduct-fbi-intelligence-violations.

130. OIG NSL Report I at xxxiii.

131. See OIG NSL Report III at 25–44.

132. *Id.*, table 4.3 at 198.

133. *Id.* at 89–122.

134. *Id.* at 45.

135. *Id.* at 137–212.

136. *Id.* at 208.

137. *Id.* at 66.

138. *Id.* at 151.

139. *Id.* at 122..

140. See generally Ivan Greenberg, *The Dangers of Dissent: The FBI and Civil Liberties Since 1965* (Lanham, MD: Lexington Books, 2010); Athan Theoharis, *The FBI and American Democracy: A Brief Critical History* (Lawrence, KS: University of Kansas Press, 2004).

141. Church Committee Report, Book II.

142. See notes 63–64 above and accompanying text.

143. Christopher Slobogin, "Subpoenas and Privacy," 54 *DePaul L. Rev.* 805, 813–14 (2005).

144. *United States v. Williams*, 504 U.S. 36 at 48 (1992).

145. *United States v. R. Enterprises*, 498 U.S. 292 (1991).

146. See, for example, *United States v. Nixon*, 418 U.S. 683 (1974).

147. *Gonzales v. Google*, Inc., No. 5:06-mc-80006-W (N.D. Cal. Mar. 17, 2006).

148. *Id.*

149. See OIG NSL Report III, at 14–25.

150. "Patterns of Misconduct," note 26, above, at 8.

151. *Id.*

152. *Id.*

153. *United States v. U.S. District Court*, note 23, above.

154. OIG 215 Report II at 65–74.

155. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995).

156. See *Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088 (W.D. Wash. 2001); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999); *Mobilisa, Inc. v. Doe 1*, 170 P.3d 712 (Ariz. Ct. App. 2007); *Krinsky v. Doe* 6, 72 Cal. Rptr. 3d 231 (Ct. App. 2008); *Doe No. 1 v. Cahill*, 884 A.2d 451 (Del. 2005); *Dendrite Int'l, Inc. v. Doe*, No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); In re *Subpoena Duces Tecum to Am. Online, Inc.* (In re *AOL*), 52 Va. Cir. 26 (Cir. Ct. 2000), *rev'd on other grounds sub nom., Am. Online, Inc. v. Anonymous Publicly Traded Co.*, 542 S.E.2d 377 (Va. 2001).

157. Nathaniel Gleicher, "John Doe Subpoenas: Toward a Consistent Legal Standard," *Yale L.J.* 118 (2008): 320, http://www.yalelawjournal.org/the-yale-law-journal/content-pages/john-doe-subpoenas:-toward-a-consistent-legal-standard/.

158. *Stanley v. Georgia* 394 U.S. 557 (1969).

159. Julie E. Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' In Cyberspace," *Conn. L. Rev.* 28 (1996): 981, http://ssrn.com/abstract=17990.

160. In re *Grand Jury Subpoena to Kramerbooks & Afterwords Inc., Med. L. Rptr.* 26 (D.D.C. 1998): 1599.

161. *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1054. (Colo. 2002).

162. See David Crary, "Battle Brews as Porn Moves into Mainstream," *Breitbart.com*, April 1, 2006, http://www.breitbart.com/article.php?id=D8GNE P902&show_article=1.

163. Press Release, Pew Internet & Am. Life Project, Pew Research Ctr., "86% of Internet Users Want to Prohibit Online Companies from Disclosing Their Personal Information Without Permission," August 21, 2000, http://www.pewinternet.org/Press-Releases/2000/86-of-Internet-Users-Want-to-Prohibit-Online-Companies-From-Disclosing-Their-Personal-Inf.aspx.

164. *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460–63 (1958).

165. See Linda E. Fisher, "Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups," *Ariz. L. Rev.* 46 (2004): 621, 625, 662 n.224.

166. Katherine J. Strandburg, "Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance," *Boston College L. Rev.* 49 (2008): 741, http://works.bepress.com/katherine_strandburg/15.

167. See notes 89–90 and accompanying text.

168. See Press Release, "DOJ To Implement Provisions Of Leahy-Authored Patriot Act Reauthorization Proposal," December 9, 2010, http://leahy.senate.gov/press/press_releases/release/?id=355bb191-f539-4f78-a6f2-8a49e85c7c0b.

STUDIES IN THE POLICY ANALYSIS SERIES

674. **Fannie Mae, Freddie Mac, and the Future of Federal Housing Finance Policy: A Study of Regulatory Privilege** by David Reiss (April 18, 2011)

673. **Bankrupt: Entitlements and the Federal Budget** by Michael D. Tanner (March 28, 2011)

672. **The Case for Gridlock** by Marcus E. Ethridge (January 27, 2011)

671. **Marriage against the State: Toward a New View of Civil Marriage** by Jason Kuznicki (January 12, 2011)

670. **Fixing Transit: The Case for Privatization** by Randal O'Toole (November 10, 2010)

669. **Congress Should Account for the Excess Burden of Taxation** by Christopher J. Conover (October 13, 2010)

668. **Fiscal Policy Report Card on America's Governors: 2010** by Chris Edwards (September 30, 2010)

667. **Budgetary Savings from Military Restraint** by Benjamin H. Friedman and Christopher Preble (September 23, 2010)

666. **Reforming Indigent Defense: How Free Market Principles Can Help to Fix a Broken System** by Stephen J. Schulhofer and David D. Friedman (September 1, 2010)

665. **The Inefficiency of Clearing Mandates** by Craig Pirrong (July 21, 2010)

664. **The DISCLOSE Act, Deliberation, and the First Amendment** by John Samples (June 28, 2010)

663. **Defining Success: The Case against Rail Transit** by Randal O'Toole (March 24, 2010)

662. **They Spend WHAT? The Real Cost of Public Schools** by Adam Schaeffer (March 10, 2010)

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001 or call toll free 1-800-767-1241 (8:30-4:30 eastern time). Fax (202) 842-3490 • www.cato.org

CATO INSTITUTE