Statement of Julian Sanchez
Research Fellow
Cato Institute
Before the United States Senate Judiciary Committee
Subcommittee on Crime, Terrorism and Homeland Security
"The Reauthorization of the PATRIOT Act"
March 9, 2011

It is nearly a decade now since Congress responded to the terror attacks of September 11th by passing the USA PATRIOT Act, a sprawling piece of legislation comprising hundreds of amendments to an array of complex intelligence and law enforcement statutes. 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."

In recognition of the great haste with which that legislation had been approved, Congress wisely established sunset provisions designed to force review of several of the most controversial elements of Patriot and its successors. While a number of judicious improvements to the original statue have already been made, these emergency powers should not be made permanent until they are further tailored to ensure that the tools employed to investigate and apprehend terrorists are consistent with our Constitutional tradition of respect for the privacy and civil liberties of innocent Americans.

My testimony today is based on a forthcoming Cato policy paper that examines these provisions in much greater detail, and with the indulgence of the chair, I request that it be included in the record.

Lone Wolf

The extraordinary tools available to investigators under the Foreign Intelligence Surveillance Act (FISA), passed over 30 years ago in response to revelations of endemic executive abuse of spying powers, 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" 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. As of late 2009, the Justice Department indicated that it had not had a need to invoke Lone Wolf authority.

The original impetus for Lone Wolf was the concern that the absence of such authority had prevented the FBI from obtaining a FISA warrant to search the laptop of so-called "20th Hijacker" Zacarias Moussaui. But as with so many of the intelligence gaps that preceded 9/11, it now appears that the real problem was a failure to connect the dots, not an inability to collect enough dots. A bipartisan 2003 report from the Senate Judiciary Committee notes that on 9/11, investigators were

able to obtain a conventional warrant on Moussaui using evidence already in their possession. More importantly, the report concluded that a FISA warrant could, in fact, have been sought earlier, but supervisors at FBI Headquarters had failed to link related reports from different field offices, or to pass those reports on to the lawyers in charge of processing FISA applications.

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. Lone Wolf does, however, threaten to blur the vital and traditional distinction in American law between domestic national security investigations and foreign intelligence, where courts have always extended greater deference to the executive branch. In the seminal "Keith" case, holding that the Fourth Amendment's warrant requirement applied with full force to domestic national security investigations, the Supreme Court stressed that there was no "evidence of any involvement, directly or indirectly, of a foreign power," suggesting that this was the key factor separating two constitutionally distinct realms.

While the statutory definition of “international terrorism” does still require some international nexus, a recent analysis by the Transactional Records Access Clearinghouse at Syracuse University suggests that government entities apply this classification inconsistently—with a substantial percentage of cases categorized as “terror related” by the Justice Department not identified that way by courts or federal prosecutors. It is not unreasonable to worry that, without the anchor of a demonstrable connection to a foreign power, it may be used in the future to invoke the sweeping powers of FISA for investigations involving non-citizens that would more properly be classified as ordinary criminal inquiries.

Once someone is designated an “agent of a foreign power,” as the FISA court has explained, information collection is “heavily weighted toward the government's need for foreign intelligence information,” meaning "acquisition of nearly all information from a monitored facility or a searched location,“ with the result that "large amounts of information are collected by automatic recording to be minimized after the fact.” This is in sharp contrast to the more narrowly targeted surveillance authorized under the aegis of title Title III’s criminal wiretap provisions.

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. But they also necessarily entail that 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 in the criminal context. While this may be necessary in light of the special challenges of investigating the heightened threat posed by sophisticated teams of Al Qaeda–trained terrorists, there is little reason to think the FBI cannot deal with loners radicalized by watching foreign YouTube videos using more conventional investigative tools.

By its own terms, Lone Wolf authority would only be available in circumstances where the standard for Title III surveillance has already been met. In the absence of the special needs created by the involvement of foreign powers, therefore, reliance on that authority should be the norm.

Roving Wiretaps

Section 206 of the Patriot Act established authority for "multipoint" or "roving" wiretaps under the auspices of the Foreign Intelligence Surveillance Act. In 2009, FBI Director Robert Mueller testified that roving authority under FISA had been used 147 times.

Roving wiretaps have existed for criminal investigations since 1986, and even the staunchest civil libertarians agree that similar authority should be available for terror investigations conducted under the supervision of the Foreign Intelligence Surveillance Court.

But in order to meet the "particularity" requirements of the Fourth Amendment, criminal roving wiretaps are required to name an identified target. As the Ninth Circuit explained in upholding that authority:

> 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.

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. Even with the safeguards imposed during the previous reauthorization, this is disturbingly close to the sort of "general warrant" the Founders were so concerned to prohibit when they crafted our Bill of Rights.

The breadth of FISA surveillance makes inadvertent overcollection especially likely when a description of an unknown target initially linked to a particular "facility" is used as the basis for interception across an ever-growing variety of diverse online services. With criminal roving wiretaps, the discretion of the investigator is generally limited to one inferential leap—that this same known person is making use of a new facility—limiting the probability of error. But since same username, account, or IP address will often—sometimes unwittingly—be used by multiple people at different times or places, that inferential gap is dramatically widened without the anchor of a named target.

Moreover, intelligence wiretaps lack an important type of distributed after-the-fact safeguard that exists in the criminal context, where the purpose of surveillance is

generally to produce admissible evidence at trial. Investigators know that their targets will eventually be notified of the wiretap, and defense attorneys armed with a right of discovery will have an incentive to uncover any improprieties. FISA surveillance normally remains covert, and post-hoc scrutiny by the FISA Court or sporadic Inspector General audits cannot realistically provide a substitute. Bear in mind that, in fiscal 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 bulk of it pursuant to FISA warrants. The Inspector General has found that much of that material cannot be reviewed in a timely fashion by the Bureau itself—never mind independent overseers.

At the very least, then, the absence of these systemic "back-end" safeguards entails that the "front-end" checks on the scope of interception need to be as strong under FISA as they are under the parallel criminal authority.

§215 Orders and National Security Letters

Unlike the enhanced authority to obtain business records and other "tangible things" under section 215 of the Patriot Act, expanded National Security Letters are not currently scheduled to sunset. But I believe it is important to consider these two complimentary powers together. As the Inspector General has made clear, the use of judicially authorized 215 orders has been limited by both internal awareness of the continuing political controversy surrounding them and—more importantly—the extraordinary breadth of National Security Letters.

There would be little point in tightening the requirements on a tool used a few dozen times per year with judicial supervision without also reforming the authority invoked *tens of thousands* of times annually, at the discretion of FBI supervisors, to acquire the sensitive financial and telecommunications records of Americans who are not even suspected of involvement in terrorism. Conversely, whatever changes to NSL authority may be contemplated in light of the "widespread and serious misuse" of that authority uncovered by the Inspector General, it is important to bear in mind that limitations on NSLs are likely to increase reliance on §215. That would be welcome development insofar as it would substitute judicial approval for administrative fiat, but may reduce what currently appears to be a high level of engagement by the FISC in narrowing overbroad applications.

While both powers have been expanded along multiple dimensions since 9/11, the main cause for concern in both cases has been the removal of the requirement that there be some evidence—not "probable cause," but *some* evidence—linking the people whose records are sought to terrorism or espionage. Now records need only be "relevant" to an investigation, and in the case of §215 orders the court is *required* to deem records "relevant" if they pertain to someone connected, however tenuously, to a suspect under investigation. As the Justice Department readily acknowledges, these tools are used in the early phases of an investigation to broadly

sweep in large amounts of data, mostly about innocent people, which is then stored indefinitely in classified government databases.

Here, again, we should bear in mind that while the easiest and most obvious response to any intelligence failure is always to grant more power to collect more information, the evidence is very thin that the problem before 9/11 was a lack of raw data. On the contrary, reflexively expanding collection authorities can exacerbate what has been colorfully characterized as the problem of "drinking from a firehose." This can even lead to a vicious cycle, where it comes to seem that more and more data is needed to close down all the dead-end leads generated by indiscriminate data collection.

Since these powers are often compared by their proponents to administrative or grand jury subpoenas—on the premise that they only provide "the same" authorities already available to criminal investigators—some crucial distinctions should be borne in mind. First, those tools are generally focused on either the activities of heavily regulated corporate entities (in the first case) or on some specific crime that already has been or is being committed, and in the latter case, the grand jury is meant to serve—in theory if not always in practice—as a "buffer or referee between the government and the people," to borrow the words of Justice Scalia.

Second, it is impossible to overstate the significance of the *transparency* that normally surrounds the acquisition of documents by those means. This acts as a powerful check on government overreach in itself, but also creates a vital incentive to challenge improper demands. The recent case of *Google v. Gonzales* is illuminating here: In an effort to gather information for litigation over the Child Online Protection Act, the government served Google with a subpoena for a sample of the search queries entered by users in a particular time period. Google moved to quash the subpoena on the grounds that it would lose the trust of users if it were publicly seen to comply with such a broad request. The court—emphasizing its independent concern for the privacy of those users more than the potential harm to Google's reputation—agreed.

By contrast, the widespread misuse of National Security Letter authority described by the Inspector General took place with not just the compliance, but often the enthusiastic encouragement of the telecommunications companies. Many of the violations of these powers that have been reported involve the overproduction of records by custodians who have every incentive to err on the side of turning over the maximum amount of information.

Finally, the last decade has seen the courts beginning, however belatedly, to recognize the need for exceptions to the so-called "Third Party Doctrine" established in the very different technological context of the 1970s, according to which people lack a Fourth Amendment "reasonable expectation of privacy" in records maintained by third parties. This was the basis for the federal statute recently invalidated by the Sixth Circuit, which allowed e-mail to be obtained without a

probable cause warrant under some circumstances. Similarly, a growing number of courts are concluding that the information about people's physical location contained in cell phone records is subject to Fourth Amendment protection.

There are also important First Amendment interests implicated by monitoring of communications records in particular. The Supreme Court has long held that the rights of free expression protected by the First Amendment encompass a right to anonymous political speech—and I should point out here that the Cato Institute itself is named for a famous series of pseudonymous political pamphlets defending individual liberty against government power—a right to "receive information and ideas," and a right to "expressive association" without state scrutiny into the membership lists of the political organizations through which it is exercise, especially when those organizations are unpopular. Here, too, courts are increasingly recognizing the need for heightened standards when subpoenas would burden these vital interests.

In the intelligence context, associational interests would appear to be implicated by the routine use of business record authorities to map "communities of interest" or conduct "link analysis" using telecommunications records at two or three removes from the actual target of investigations. Judicial scrutiny can mitigate these concerns somewhat: Thanks again to the Inspector General, we know of at least one case in which the FISA court rejected a §215 application on the grounds that it targeted protected speech. Undeterred, however, the FBI went ahead and obtained the same information using National Security Letters.

Of special concern here is a "sensitive collection program" involving §215 alluded to by Acting Assistant Attorney General Hinnen last year in his testimony on these authorities. Though the Senate had previously unanimously approved an amendment limiting §215 authority to records pertaining to the activities of terror suspects or their associates, a similar reform appears to have been abandoned last year following claims by the Justice Department that such a change would hamper that secret program. Soon afterward, Sen. Russ Feingold purported to have knowledge of clear misuse of §215 unknown to the general public.

If nothing else, I would urge those with access to the relevant details to take a long, hard look at that. But I would also suggest that we should be highly skeptical of any intelligence program that cannot function within even those very modest limitations. The United States was able to observe the time-tested principle of individualized suspicion in a decades-long conflict with a hostile empire armed with nuclear weapons. We should not assume it is an insuperable handicap against scattered bands of religious fanatics.

Conclusion

As a final observation, I want to suggest that formal improprieties at the acquisition stage—while certainly very serious, especially in the case of National Security Letters—are not the sole cause for concern about these broad surveillance powers.

It would be more worrying, after all, if standards were lowered and safeguards weakened so far that *nothing* counted as a "misuse." The real danger is that the formally lawful collection of records is giving rise to a set of ever-growing databases—the FBI's comprising billions of records at last count—overflowing with potentially sensitive information about innocent Americans and their constitutionally protected activities.

As the recent publication of classified military and State Department records by Wikileaks demonstrates all too clearly, just one of the thousands of people with access to a database—whether inspired by misguided idealism or more sinister motives—can compromise an enormous amount of information. When that information is published on the Internet for all to see, however, it's at least possible to assess the extent of the harm and seek to identify the responsible parties. Similarly, when information obtained for intelligence purposes, subject to intelligence rules, is passed on to criminal prosecutors, we at least know that the safeguards of the criminal justice system remain in place.

But the ugly history of American intelligence abuses suggests that the gravest threat in this sphere involves the *secret* deployment of information for political purposes—the most notoroious example being the attempt to exploit recordings of Martin Luther King's extramarital liaisons to drive the civil rights leader to suicide. It was a commonplace, in my former life as a journalist, to say that fact-checking will catch a sloppy reporter, but not one intent upon deception. By the same token, internal oversight and auditing are reasonably good at catching honest mistakes. But under the veil of secrecy surrounding intelligence, the only sure way to prevent willful misuse of information about innocent Americans is to

You sometimes hear it said that civil libertarians are trapped in a "pre-9/11 mindset," stubbornly refusing to adapt to the demands of a world where non-state adversaries wield terrifying destructive capabilities. I would like to believe that's not true: With at respect to at least two of the three authorities under consideration today, I would not question whether the government should *have* these tools to investigate terrorists—but only how they should be tailored to ensure that they are focused on *terrorists* without intruding on the privacy of innocent Americans any further than is necessary to safeguard national security.

But I think it would be an equally serious mistake to lapse into what we might call a "pre–Church Committee mindset", to forget *why* we established a series of safeguards against overbroad surveillance, and to assume that abuse of intelligence powers can only happen in places like Egypt or China or Iran. As our Founders understood, and as the history of the 20th century teaches us, it can—and indeed did—happen here. If we lose sight of that historical lesson, history suggests it may be decades more before we know our mistake.