Statement of

Julian Sanchez

Research Fellow, Cato Institute

Before the

Senate Committee on the Judiciary

Hearing on "Continued Oversight of U.S. Government Surveillance Authorities"

December 11, 2013

Thank you Chairman Leahy, Ranking Member Grassley; it is a privilege to be invited to address this committee.

With the recent release of several Foreign Intelligence Surveillance Court opinions, concerning a now-defunct program to acquire Internet metadata in bulk under FISA's pen register/trap-and-trace authority, a pattern has begun to emerge—across multiple domains of intelligence activity.

First, an authority generally understood at the time of passage to be expansive but nevertheless limited and particularized—certainly by the general public, and apparently by many members of Congress as well—is secretly interpreted to permit bulk acquisition of information about vast numbers of Americans' communications. Once published, the legal rationale for this expansive reading is criticized as strained even by scholars generally sympathetic to the past decade's expansion of government surveillance powers. As Professor Orin Kerr

noted in *The New Republic*, the FISC's opinion in this case ignored "important statutory clues suggesting that the pen register authority does not extend to bulk programmatic uses."

Here as with the previously disclosed telephony metadata program, the Court rationalized this bulk collection by employing a strained and, for practical purposes, unlimited concept of "relevance to an authorized investigation," according to which a pool of thousands or millions of records pertaining to Americans' innocuous communications could be considered "relevant" on the grounds that subsequent analysis could detect the tiny fraction actually related to some foreign terror group. This is, however, the very definition of a fishing expedition: Indiscriminate collection untethered to any specific grounds for suspicion at the time of acquisition, on the premise that some evidence of wrongdoing is bound to turn up somewhere.

Perversely, this rationale depends on bulk collection *not* being more narrowly tailored. If, after all, the government sought to acquire in bulk all metadata pertaining to communications for an arbitrarily chosen city over some more limited time period, it could not plausibly claim that the data pool was statistically all but certain to contain records of *actually* relevant communications. On the government's theory, rather, the totality of the information obtained is relevant *because* acquisition is sweeping and indiscriminate—a train of logic that, once accepted, leaves scant incentive to develop more narrowly tailored collection criteria.

What is perhaps especially odd here is that the Court does not appear to have authorized the use of "big data" analytic tools—such as pattern matching to detect a group of targets who had changed phones or e-mail accounts—that might plausibly be said to truly *require* a comprehensive database, but rather limited queries of that data to selectors for which a particularized determination of reasonable suspicion had been made. At that point, of course, a more traditional and circumscribed conception of relevance would permit the same records to be obtained via targeted orders. Thus the full weight of the justificatory burden for untargeted collection is effectively borne by the argument that it is necessary to enable historical access to records that might ultimately be determined to be relevant.

In other words, everything is relevant now because anything might turn out to be relevant in the future. The government has gestured toward the need to articulate a limiting principle to its collection powers by stressing that communications records in particular can be fruitfully analyzed in bulk to reveal networks of association—but to the extent that the real weight of the argument is borne by the putative necessity of historical access, it would apply to any body of records not retained indefinitely that could conceivably be relevant to an investigation. This should be especially troubling given that the same "relevance" language appears in the statutes authorizing National Security Letters, which do not require advance judicial approval.

The FISC's justification of the telephony metadata program has been extensively criticized on both constitutional and statutory grounds in a recent paper

by Professor Laura Donohue, and that critique largely applies, mutatis mutandis, to the e-mail metadata program. In the latter case, however, even if we accept the government's strained reliance on *Smith v. Maryland* and the increasingly untenable legal fiction that it is unreasonable for Americans to expect any privacy in records of their communications held by third parties, there is an additional complication: It would appear, though redactions make it hard to be certain, that metadata about e-mail communications was obtained not from e-mail providers themselves, but from Internet Service Providers that do not normally retain such information in business records or, indeed, need to process it as an incident to the provision of service. Relative to the ISP, e-mail metadata—which is not *necessarily* knowingly disclosed to or retained by any third party, at least in the case of communications between entities that maintain their own mail servers—could reasonably be considered just another form of content. Again, due to redactions in the published opinions, it is unclear how adequately the FISC dealt with this technical feature of Internet communications.

Though the FISC did attempt to impose restrictions designed to protect the privacy of innocent Americans, these were "continuously violated" over a period of years, while the Court was repeatedly misinformed about the technical details of the collection program's operation. As the FISC noted in another recently disclosed opinion, this is one of at least three instances in as many years in which the government had "disclosed a substantial misrepresentation regarding the scope of a major collection program." In the case of the 215 telephony metadata program, the Court found that as a result of these misrepresentations, the rules imposed by the

FISC had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall regime… has never functioned effectively."

The third such known instance, involving overcollection of domestic communications under the FISA Amendments Act's §702 authority, did at least occur under a provision clearly intended for large-scale collection. Here, the problem was that if a single e-mail triggered the NSA"s automatic filters while a user was downloading his inbox, the entire stream — including totally domestic messages — could be captured. As the FISC observed, even if this were a relatively rare occurrence, the massive scale of NSA interception meant the agency could be vacuuming up some 56,000 wholly domestic emails annually. This approach, the court drily concluded, was "deficient on statutory and constitutional grounds."

In light of the massive scale of this collection, that the American communications are deemed to be acquired "incidentally," and the U.S. communicants are not intentionally "targeted," provides little comfort. The general warrants deplored by our Founders, which inspired the Fourth Amendment, were similarly not "targeted" at any particular U.S. person—but that was accurately seen, not as some kind of safeguard, but as the essential problem.

Concerns on this score should be compounded by diclosures that NSA databases can then be queried for selectors associated with U.S. persons. Another recent report informs us that the "intelligence purposes" for which the collected data might be used include compiling derogatory information about the embarrassing online sexual habits of "radicalizers"—apparently including, in at least

one case, a U.S. person—who are engaged in Internet speech hostile to the United States, but not directly linked to violent groups.

Finally, the broad claims of intelligence necessity upon which the FISC relied in authorizing the program appear not to have withstood scrutiny—and this program, at least, was discontinued in 2011, though it remains unclear how broadly components of the intelligence community continue to collect Internet metadata under other programs or authorities.

Similar claims about the necessity of the telephony program have not fared much better. From initial claims that dozens of "terrorist events" were "disrupted" by that program *along with* PRISM surveillance, it has become clear that in only a single material support case did the 215 program provide a unique or essential lead, and in an amicus brief filed in support of an ACLU lawsuit, several senators with access to the classified details argue that there is "no evidence that the bulk collection of Americans' phone records has provided any intelligence of value that could not have been gathered through less intrusive means." Indeed, even as the FBI has repeatedly reassured the FISC of the value of this program, an exchange reported in Garret Graff's book *The Threat Matrix* quotes former FBI director Robert Mueller describing what appears to be the 215 telephony program as a "useless time suck."

This is a continuation of a pattern we have seen on numerous occasions over the past decade. Shortly after the terrorist attacks on September 11, 2001, President George W. Bush authorized the National Security Agency to conduct broad

telephone and Internet surveillance outside the procedures of the Foreign Intelligence Surveillance Act—a program that would eventually come to be known as STELLAR WIND. When one component of that program, involving warrantless telephone wiretapping, was discovered and—eventually—disclosed by reporters for *The New York Times*, the administration insisted on its effectiveness and vital importance. Former NSA director Michael Hayden claimed that it had "been successful in detecting and preventing attacks inside the United States." Vice President Dick Cheney went still further, asserting that the program had "saved thousands of lives."

Yet when the intelligence community's Inspectors General finally published an unclassified report on the program, they noted that the officials they interviewed "had difficulty citing specific instances where [the program] had directly contributed to counterterrorism successes." As one senior CIA official told NSA historian Matthew Aid: "We spent a ton on the program but got back very little in the way of solid returns. I don't think it was worth the money."

Fusion centers, massively funded by the Department of Homeland Security over the past decade, were repeatedly hailed by intelligence officials as a "vital, proven tool" and a "centerpiece of our counterterrorism strategy." It was only last year that an extensive, bipartisan Senate investigation concluded that they had in fact produced no useful counterterror intelligence, and indeed risked violating the Privacy Act by generating reports of citizens' First Amendment protected activities.

I am not, I wish to stress, claiming that intelligence officials deliberately mislead either Congress or the FISC about the importance of these programs. But the employees of every government agency naturally tend to believe that their programs and authorities serve an essential public purpose, and that internal assessment should not be uncritically accepted—especially when the authorities in question impinge on Americans' privacy and civil liberties.

It has become increasingly clear that the FISA court, conceived as a body charged with assessing and authorizing specific targeting decisions, is ill equipped in its current form to evaluate broad *programs* of surveillance and data collection. Greater transparency, and some form of adversarial process in cases where the FISC considers novel legal and technological questions, may remedy the problem somewhat, but it would be better still to require the intelligence agencies to seek specific congressional authorization for collection on that scale, limiting the existing authorities to collection with a specific nexus to a suspected foreign agent—a limitation the Senate already unanimously approved back in 2005.

I note in closing that we have been assured the violations of existing rules limiting surveillance require no further constraint because, for the most part, they have not been determined to be "willful" or "intentional." I do not find this reassuring for several reasons.

First, in any system of oversight, inadvertent violations are more likely to be discovered than willful abuses, precisely because inadvertent violators take no steps to evade detection. We know from our own history that when intelligence agencies

engaged in clearly illegal political surveillance throughout the 1960s, they took elaborate steps to evade the more anemic oversight structures in place prior to the passage of FISA, avoiding the creation of any official record of abuses. In one case discussed by historian Athan Theoharis, for instance, a member of Congress made repeated improper requests for access to FBI files on specific individuals. In each case, the request was met with a formal letter of denial—hand-delivered by an agent carrying the requested files in a briefcase. We should not expect bad actors in the future to be less ingenious.

Second, the history of intelligence abuses uncovered by the Church Committee in the 1970s *sometimes* involved wholly illegal surveillance unconnected to any legitimate intelligence purpose. Often, however, information obtained through surveillance that had some colorable intelligence justification in its inception was later—sometimes years later—misused for political purposes.

Third, and relatedly, the sheer volume of modern collection makes intentional abuse vastly harder to definitively prove. Whatever excuses might have been offered for the extensive campaign of surveillance, slander, and harassment directed at Martin Luther King and other political activists and dissidents, nobody could plausibly claim that the telephones and offices of the Southern Christian Leadership Conference had been wiretapped *inadvertently* or *incidentally*. Against the background of bulk collection, however, it is likely to be far more difficult to distinguish between deliberate abuse and a well-intentioned data query that happens to return information about innocent Americans—one reason that, at the

very minimum, Congress should require judicial approval before selectors pertaining to Americans can be used to query foreign intelligence databases.

Again, I do not mean to claim that we have reason to believe abuses of the type revealed by the Church Committee are now occurring, or have occurred in the past decade. It is entirely plausible they have not. We must recognize, however, that we have constructed—not through any one particular authority, but by the cumulative expansion of interconnected intelligence powers—an architecture of surveillance vastly more potent than anything those responsible for COINTELPRO or Operation SHAMROCK could have conceived. When even inadvertent misuse of that architecture can go undetected by overseers for years at a time, it seems unwise to wait for evidence of malice before imposing commonsensical limits on the programs that are demonstrably vital to national security—and eliminating entirely those whose value remains largely theoretical.