AMERICAN CONSTITUTIONALISM
VOLUME II: RIGHTS AND LIBERTIES
Howard Gillman • Mark A. Graber • Keith E. Whittington

Supplementary Material

Chapter 11: The Contemporary Era—Criminal Justice

House Hearings on Disclosure of NSA Intelligence Gathering (2013)[1]

On May 20, 2013, Edward Snowden, an employee of the private contractor Booz Allen Hamilton working at the National Security Agency (NSA), flew to Hong Kong with four laptop computers loaded with classified information describing the structure and operation of the NSA's electronic intelligence gathering activities. He soon leaked that information to a British newspaper, which published a series of stories on the NSA's access to data on electronic communication held by a variety of American telecommunications and Internet companies. The Obama Administration claimed this surveillance was constitutional and legal. The PATRIOT Act and the Foreign Intelligence Surveillance Act (FISA) provided statutory authority for the collection of information about phone calls and other electronic communication ("metadata") and for accessing the content of phone calls and e-mails of foreigners located outside the United States. Section 702 of FISA allowed the government to obtain the content of phone calls and e-mails of persons outside the United States. Section 215 of the PATRIOT Act allowed the government to obtain access of electronic metadata. Senator Obama had been critical of the PATRIOT Act and the Bush administration's intelligence activities. In the aftermath of the leaks, President Obama defended the NSA as striking the "right balance" between privacy and security. Heemphasizing that the intelligence agency was receiving proper oversight from the executive, legislative, and judicial branches.

Congressional reaction to the leaks was mixed. Members of Congress took to the floor to denounce both the leaks and the NSA. Representative Ted Poe (Republican, Texas) asked rhetorically, "Do you think the government spooks are drunk on power, and it's time for Congress to intervene to prevent the invasion of privacy by government against the citizens?" Representative Alan Grayson (Democrat, Florida) argued, "I don't understand why anyone would think that it's somehow okay for the Department of Defense to get every single one of our call records regardless of who we are, regardless of whether we are innocent or guilty of anything. . . . We are not North Koreans. We don't live in Nazi Germany."[2] Congressional committees held public hearings that aired explanations of the programs and offered opportunities to administration officials to defend the programs against charges that they had unduly infringed on the privacy rights of Americans.

Is there a reasonable expectation of privacy for the list of phone numbers from which you received calls? Is there a difference between the government creating a database of the records of all phone calls received in the United States and accessing the specific list of phone calls received by an individual person? If the government could demonstrate that assembling and using such a database has been useful in preventing terrorist attacks within the United States, would that justify this intelligence gathering? Should there be restrictions on surveillance of non-U.S. citizens or residents who are located outside the United States? Is executive reporting to select congressional committees whose members have security clearance sufficient to provide legislative oversight of

[1] *Disclosure of NSA Programs: Hearings before the House Select Intelligence Committee*, U.S. House of Representatives, 113th Cong., 1st Sess. (2013).

[2] U.S. House of Representatives, *Cong. Record*, 113th Cong., 1st Sess. (June 11, 2013): H3261; *Cong. Record* (June 14, 2013): H3640.

intelligence-gathering activities? Should the general public be made aware of what databases the NSA is assembling and how electronic searches of records are conducted?

REPRESENTATIVE MIKE ROGERS (Republican, Michigan)

. . . .

The committee has been extensively briefed on these efforts over a regular basis as a part of our ongoing oversight responsibility over the 16 elements of the intelligence community and the national intelligence program.

In order to fully understand the intelligence collection programs most of these briefings and hearings have taken place in classified settings. Nonetheless, the collection efforts under the business records provision in Section 702 of the Foreign Intelligence Surveillance Act are legal, court-approved and subject to an extensive oversight regime.

. . . .

The public trusts the government to protect the country from another 9/11-type attack, but that trust can start to wane when they are faced with inaccuracies, half-truths, and outright lies about the way the intelligence programs are being run.

One of the more damaging aspects of selectively leaking incomplete information is that it paints an inaccurate picture and fosters distrust in our government.

. . . .

It is critically important to protect sources and methods so we aren't giving the enemy our play book.

It is also important, however, to be able to talk about how these programs help protect us so they can continue to be reauthorized. And then we highlight the protections and oversight of which these programs operate under.

. . . .

REPRESENTATIVE C. A. RUPPERSBERGER (Democrat, Maryland)

. . . .

. . . . NSA is in my district. I have an occasion to communicate, and a lot of the people who go to work to protect our country, who work hard every day, are concerned that the public think they're doing something wrong. And that's not the case at all.

. . . .

We're here today because of the brazen disclosure of critical classified information that keeps our country safe. . . . The terrorists now know many of our sources and methods.

. . . .

To be clear, the National Security Agency is prohibited from listening in on phone calls of Americans without proper, court-approved legal authorities.

We live in a country of laws. These laws are strictly followed and layered with oversight from three branches of government. . . .

. . . .

. . . . In fact, these [laws] have been instrumental in helping to prevent dozens of terrorist attacks, many on U.S. soil.

. . . .

We need to change our systems and practices, and employ the latest in technology that would alert superiors when a worker tries to download and remove this type of information. We need to seal this crack in the system.

. . . .

GENERAL KEITH ALEXANDER, Director of the National Security Agency

. . . .

The events of September 11, 2001 occurred, in part, because of a failure on the part of our government to connect [the] dots. . . .

Section 215 of [the PATRIOT Act] . . . helps the government close [the] gap by enabling the detection of telephone contact between terrorists overseas and operatives within the United States. . . . [I]f we had had Section 215 in place prior to 9/11, we may have known that the 9/11 hijacker Mihdhar was located in San Diego and communicating with a known Al Qaida safe house in Yemen.

. . . .

I believe we have achieved the security and relative safety in a way that does not compromise the privacy and civil liberties of our citizens. We would like to make three fundamental points. First, these programs are critical to the intelligence community's ability to protect our nation and our allies' security. . . .

Second, these programs are limited, focused, and subject to rigorous oversight. . . .

Third, the disciplined operation of these programs protects the privacy and civil liberties of the American people. . . .

DEPUTY ATTORNEY GENERAL JAMES M. COLE, U.S. Department of Justice

. . . .

. . . . This is not a program that's off the books, that's been hidden away. This is part of what government puts together and discusses. Statutes are passed. It is overseen by three branches of our government. . . . The process of oversight occurs before, during, and after the process that we're talking about today.

. . . .

. . . . First of all, it's metadata. These are phone records. . . . We do not get the identity of any of the parties to this phone call. . . . We don't get any cell site or location information. . . . And, most importantly . . . , we don't get any content under this.

. . . . [T]he way it works is, there is an application that is made by the FBI under the statute to the FISA court. We call it the FISC. They ask for and receive permission under the FISC . . . to get records that are relevant to a national security investigation. And they must demonstrate to the FISC that it will be operated under the guidelines that are set forth by the attorney general. . . .

. . . . [I]t is quite explicitly limited to things that you could get with a grand jury subpoena, those kinds of records. Now, it's important to know that prosecutors issue grand jury subpoenas all the time and do not need any involvement of a court or anybody else to do so.

Under this program, we need to get permission from the court to issue this ahead of time. . . .

. . . . [W]e have to re-up and renew these orders every 90 days in order to do this. Now, there are strict controls over what we can do under the order. . . . There're restrictions on who can access it. . . .

In order to access [the collected records], there needs to be a finding that there is a responsible suspicion . . . that the person whose phone records you want to query is involved with some sort of terrorist organizations. . . . So there has to be independent evidence . . . that the person you're targeting is involved. . . .

If that person is a United States citizen, or a lawful permanent resident, you have to have something more than just their own speeches. . . .

Now, one of the things to keep in mind is under the law, the Fourth Amendment does not apply to these records . . . because people don't have a reasonable expectation of privacy in who they called and when they called. . . . [*Smith v. Maryland* (1979)]

. . . .

We also provide the Intelligence and Judiciary Committees with any significant interpretations that the court makes of the [statute]. If they make a ruling that is significant or issue an order that is significant in its interpretation, we provide those, as well as the applications made for those orders, to the Intelligence and to the Judiciary Committee.

And every 30 days, we are filing with the FISC a report that describes how we implement this program. . . .

At least once every 90 days and sometimes more frequently, the Department of Justice, the Office of the Director of National Intelligence, and the NSA meet to assess NSA's compliance with all of these requirements that are contained in the court order. Separately, the Department of Justice meets with the inspector general for the National Security Agency and assesses the NSA's compliance on a regular basis.

Finally, there is by statute reporting of certain information to Congress in semiannual reports that we make on top of the periodic reports we make if there's a compliance incident. . . .

Now, the 702 statute under the FISA Amendments Act is different. Under this, we do get content, but there's a big difference. You are only allowed . . . to target for this purpose non-U.S. persons who are located outside of the United States. So if you have a U.S. permanent resident who's in Madrid, Spain, we can't target them under 702. Or if you have a non-U.S. person who's in Cleveland, Ohio, we cannot target them under 702. . . .

. . . . The FISC gives a certificate that allows this targeting to be done for a year period. It then has to be renewed. . . . [and similar reporting and oversight processes are followed for FISA].

. . . .

[A report recently found that] the U.S. is more transparent about its [intelligence gathering] procedures, requires more due process protections in its investigations that involve national security, terrorism and foreign intelligence [than our partner countries, including those in the European Union].

. . . .

REPRESENTATIVE JANICE SCHAKOWSKY (Democrat, Illinois)

. . . . [W]ill you release these [FISA] court opinions with the necessary redactions, of course? And if not, why?

ROBERT LITT, General Counsel, National Security Agency

As you may know, we have been working for some time on trying to declassify opinions of the FISA court. It's been a very difficult task, because like most legal opinions, you have facts intermingled with legal discussion. And the facts frequently involve classified information, sensitive sources and methods. And what we've been discovering is that when you remove all of the information that needs to be classified, you're left with something that looks like Swiss cheese, and is not really very comprehensible. . . .

REPRESENTATIVE JAMES HIMES (Democrat, Connecticut)

. . . . [The programs that Snowden revealed] trouble me because of the breadth and the scope of the information collected. They trouble me because I think this is historically unprecedented in the extent of the data that is being collected on potentially all American citizens. . . . We know that when a capability exists, there's potential for abuse. . . .

. . . . And one of the things that I'm concerned about is that [Snowden] . . . had access to some of the most sensitive information that we have. . . . Could have accessed phone numbers and—though we spent a lot of time on the fact that you don't get names, we all know that with a phone number and Google, you can get a name pretty quickly.

He could have chosen to make a point about Congressman Himes making 2:00 am phone calls out of a bar in Washington. . . . Or anything really. Information that we hold to be private.

. . . .

DEPUTY ATTORNEY GENERAL JAMES M. COLE, U.S. Department of Justice

I think some of it is a matter for the United States Congress to decide as policy matters. . . . Certainly the courts have looked at this and determined that under the statutes we have, there is a relevance requirement, and they're not just saying out of whole cloth you're allowed to gather these things. . . . And they're only saying that you can gather this volume under these circumstances, under these restrictions, with these controls. . . . [T]he acquisition comes together with the restriction on access.

. . . .

GENERAL KEITH ALEXANDER, Director of the National Security Agency

. . . . So your question is, could somebody get your phone number and see that you were at a bar last night? The answer is no. Because first in our system, somebody would have had to approve, and there's only 22 people that can approve, a reasonable articulable suspicion on a phone number. . . . Only those phone numbers that are approved could then be queried. And so you have to have one of those 22 break a law [to approve access a congressman's phone number]. Then you have to have somebody go in and break the law [by actually accessing the phone number]. And the system is 100 percent auditable, so it will be caught.

. . . . And then that person would be found by the [FISA] court to be in violation of a court order, and that's much more serious. We have never had that happen.

. . . .

REPRESENTATIVE MICHELE BACHMANN (Republican, Minnesota)

[D]oes the federal government have a database with video data in it tracking the whereabouts of the American people?

DEPUTY DIRECTOR SEAN JOYCE, Federal Bureau of Investigation

The FBI does not have such a database, nor am I aware of one.

REPRESENTATIVE MICHELE BACHMANN (Republican, Minnesota)

[D]oes the American government have a database that has the GPS location whereabouts of Americans . . . ?

DEPUTY DIRECTOR CHRIS INGLIS, National Security Agency

NSA does not hold such a database.

REPRESENTATIVE MICHELE BACHMANN (Republican, Minnesota)

Does the NSA have a database that you maintain that holds the content of Americans' phone calls? . . .

GENERAL KEITH ALEXANDER, Director of the National Security Agency

We're not allowed to do that, nor do we do that, unless we have a court order to do that. And it would be only in specific cases and almost always that would be an FBI lead, not ours.

. . . .

DEPUTY ATTORNEY GENERAL JAMES M. COLE, U.S. Department of Justice

. . . . [I]f you're looking for a needle in the haystack, you have to get the haystack first. And that's why we have the ability under the court order to acquire—and the key word here is acquire—all that data.

We don't get to use all of that data necessarily. That is the next step, which is to have to be able to determine that there is reasonable, articulable suspicion to use that data.

So if we want to find that there is a phone number that we believe is connected with terrorist organizations and terrorist activity, we need to have the rest of the haystack, all the other numbers, to find out which ones it was in contact with.

. . . .