TEXTS: UNITED STATES NATIONAL SECURITY AGENCY

Compiled by Rozina Ali

Editor's Note: On June 5, 2013, Britain's Guardian *newspaper began publishing reports revealing the scale of domestic surveillance by the U.S. National Security Agency. On June 9, the newspaper revealed that the "whistleblower" behind the revelations was an NSA contractor, Edward Snowden.*

Statement by James R. Clapper, Director of National Intelligence, on Recent Unauthorized Disclosures of Classified Information, Washington, DC (June 6, 2013)
Source: Office of the Director of National Intelligence

The highest priority of the Intelligence Community is to work within the constraints of law to collect, analyze and understand information related to potential threats to our national security.

The unauthorized disclosure of a top secret U.S. court document threatens potentially long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation.

The article omits key information regarding how a classified intelligence collection program is used to prevent terrorist attacks and the numerous safeguards that protect privacy and civil liberties.

I believe it is important for the American people to understand the limits of this targeted counterterrorism program and the principles that govern its use. In order to provide a more thorough understanding of the program, I have directed that certain information related to the "business records" provision of the Foreign Intelligence Surveillance Act be declassified and immediately released to the public.

The following important facts explain the purpose and limitations of the program:

—The judicial order that was disclosed in the press is used to support a sensitive intelligence collection operation, on which members of Congress have been fully and repeatedly briefed. The classified program has been authorized by all three branches of the Government.

—Although this program has been properly classified, the leak of one order, without any context, has created a misleading impression of how it operates. Accordingly, we have determined to declassify certain limited information about this program.

—The program does not allow the Government to listen in on anyone's phone calls. The information acquired does not include the content of any communications or the identity of any subscriber. The only type of information acquired under the Court's order is telephony metadata, such as telephone numbers dialed and length of calls.

—The collection is broad in scope because more narrow collection would limit our ability to screen for and identify terrorism-related communications. Acquiring this information allows us to make connections related to terrorist activities over time. The FISA Court specifically approved this method of collection as lawful, subject to stringent restrictions.

—The information acquired has been part of an overall strategy to protect the nation from terrorist threats to the United States, as it may assist counterterrorism personnel to discover whether known or suspected terrorists have been in contact with other persons who may be engaged in terrorist activities.

—There is a robust legal regime in place governing all activities conducted pursuant to the Foreign Intelligence Surveillance Act, which ensures that those activities comply with the Constitution and laws and appropriately protect privacy and civil

liberties. The program at issue here is conducted under authority granted by Congress and is authorized by the Foreign Intelligence Surveillance Court (FISC). By statute, the Court is empowered to determine the legality of the program.

—By order of the FISC, the Government is prohibited from indiscriminately sifting through the telephony metadata acquired under the program. All information that is acquired under this program is subject to strict, court-imposed restrictions on review and handling. The court only allows the data to be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization. Only specially cleared counterterrorism personnel specifically trained in the Court-approved procedures may even access the records.

—All information that is acquired under this order is subject to strict restrictions on handling and is overseen by the Department of Justice and the FISA Court. Only a very small fraction of the records are ever reviewed because the vast majority of the data is not responsive to any terrorism-related query.

—The Court reviews the program approximately every 90 days. DOJ conducts rigorous oversight of the handling of the data received to ensure the applicable restrictions are followed. In addition, DOJ and ODNI regularly review the program implementation to ensure it continues to comply with the law.

—The Patriot Act was signed into law in October 2001 and included authority to compel production of business records and other tangible things relevant to an authorized national security investigation with the approval of the FISC. This provision has subsequently been reauthorized over the course of two Administrations—in 2006 and in 2011. It has been an important investigative tool that has been used over the course of two Administrations, with the authorization and oversight of the FISC and the Congress.

Discussing programs like this publicly will have an impact on the behavior of our adversaries and make it more difficult for us to understand their intentions. Surveillance programs like this one are consistently subject to safeguards that are designed to strike the appropriate balance between national security interests and civil liberties and privacy concerns. I believe it is important to address the misleading impression left by the article and to reassure the American people that the Intelligence Community is committed to respecting the civil liberties and privacy of all American citizens.

Government Accountability Project Statement on Edward Snowden and National Security Agency Domestic Surveillance, Washington, DC (June 14, 2013)

Source: Government Accountability Project

Recently, the American public learned that the National Security Agency (NSA) has conducted, and continues to conduct, wholesale surveillance of U.S. citizens through a secretive data-mining program. The program collects the phone records, email exchanges and internet histories of tens of millions of Americans who would otherwise have no knowledge of the secret program were it not for the disclosures of recent whistleblowers. The latest of these whistleblowers to come forward is former Booz Allen Hamilton federal contractor employee Edward Snowden.

As the nation's leading whistleblower protection and advocacy organization, the Government Accountability Project (GAP) would like to be clear about its position on each of the following points that relate to these significant revelations:

I. Snowden is a whistleblower.
Snowden disclosed information about a secret program that he reasonably believed to be illegal. Consequently, he meets the legal definition of a whistleblower, despite statements to the contrary made by numerous government officials and security pundits. Sen. Rand Paul (R-KY), Sen. Mark Udall (R-CO), Rep. Loretta Sanchez (D-CA), Rep. Thomas Massie (R-KY), and Sen. Bernie Sanders (I-VT) have also expressed concern about the potential illegality of the secret program. Moreover, Rep. Jim Sensenbrenner (R-WI) who is one of the original authors of the Patriot Act, the oft-cited justification for this pervasive surveillance, has expressed similar misgiving.

II. Snowden is the subject of classic whistleblower retaliation.
Derogatory characterizations of Snowden's personal character by government officials do not negate his whistleblower status. On the contrary, such attacks are classic acts of predatory reprisal used against whistleblowers in the wake of their revelations.

Snowden's personal life, his motives and his whereabouts have all been called into question by government officials and pundits engaged in the reflexive response of institutional apologists. The guilty habitually seek to discredit the whistleblower by shifting the spotlight from the dissent to the dissenter. Historically, this pattern of abuse is clear from behavior toward whistleblowers Daniel Ellsberg, Mark Felt, Frank Serpico, Jeffrey Wigand, Jesselyn Radack and recent NSA whistleblower Tom Drake.

III. The issue is the message and not the messenger.
As a matter of course, whistleblowers are discredited, but what truly matters is the disclosure itself. Snowden's revelations have sparked a public debate about the balance between privacy and security—a debate that President Obama now claims to welcome. Until Snowden's disclosures, however, the government had suppressed the facts that would make any serious debate possible.

IV. Pervasive surveillance does not meet the standard for classified information.
Many have condemned Snowden for disclosing classified information, but documents are classified if they reveal sources or methods of intelligence-gathering used to protect the United States from its enemies. Domestic surveillance that is pervasive and secret is only a valid method of intelligence gathering if the country's enemies include most of its own population. Moreover, under the governing Executive Order it is not legal to classify documents in order to cover up possible misconduct.

V. The public has a constitutional right to know.
In a democracy, it is simply not acceptable to discover widespread government surveillance only after a whistleblower's revelations. Because of Snowden's disclosures we now know that Director of National Intelligence James Clapper deliberately misled the Senate Intelligence Committee when he stated on March 12, 2013 that the NSA did not purposefully collect *any* type of data from millions of Americans. Regardless of the justification for this policy, the public has a Constitutional right to know about these actions.

Unfortunately, the responsibility has fallen on whistleblowers to inform the public about critical policy issues—from warrantless wiretapping to torture. Whistleblowers remain the regulator of last resort.

VI. There is a clear history of reprisal against NSA whistleblowers.
By communicating with the press, Snowden used the safest channel available to him to inform the public of wrongdoing. Nonetheless, government officials have been critical of him for not using internal agency channels—the same channels that have repeatedly failed to protect whistleblowers from reprisal in the past. In many cases, the critics are the exact officials who acted to exclude national security employees and contractors from the Whistleblower Protection Enhancement Act of 2012.

Prior to Snowden's disclosures, NSA whistleblowers Tom Drake, William Binney and J. Kirk Wiebe, all clients of GAP, used internal mechanisms—including the NSA chain of command, Congressional committees, and the Department of Defense Inspector General—to report the massive waste and privacy violations of earlier incarnations of the NSA's data collection program. Ultimately, the use of these internal channels served only to expose Binney, Drake and Wiebe to years-long criminal investigations and even FBI raids on their homes. As one example, consider that Tom Drake was subjected to a professionally and financially devastating prosecution under the Espionage Act. Despite a case against him that ultimately collapsed, Drake was labeled an "enemy of the state" and his career ruined.

VII. We are witnessing the criminalization of whistleblowing.
During the last decade, the legal rights for whistleblowers have expanded for many federal workers and contractors, with the one exception of employees within the intelligence community. The rights of these employees have significantly contracted. The Obama administration has conducted an unprecedented campaign against national security whistleblowers, bringing more Espionage Act indictments than all previous administrations combined.

Moreover, at the behest of the House Intelligence Committee, strengthened whistleblower

protections for national security workers were *stripped* from major pieces of legislation such as the Whistleblower Protection Enhancement Act (for federal employees) and the National Defense Authorization Act of 2013 (for federal contractors). If those protections existed today, Snowden's disclosures would have stood a greater chance of being addressed effectively from within the organization.

The actions already taken against Snowden are a punitive continuation of what has become a "War on Whistleblowers." Through a series of retaliatory measures, the federal government targets federal employees who speak out against gross waste, illegality, or fraud, rather than prosecuting individuals engaged in high crimes and misdemeanors. So far as we know, not one person from the NSA has yet to suffer any consequences for ordering, justifying or participating in the NSA's domestic spying operation.

It is the opinion of GAP that recent events suggest the full might of the Department of Justice will be leveled at Snowden, including an indictment under the Espionage Act, while those who stretched their interpretation of the Patriot Act to encompass the private lives of millions of Americans will simply continue working.

VIII. In the surveillance state, the enemy is the whistleblower.

If every action has an opposite and equal reaction, the whistleblower is that reaction within the surveillance state. Dragnet electronic surveillance is a high-tech revival of tactics used to attack the civil rights movement and political enemies of the Nixon administration. Whistleblowers famously alerted the public to past government overreach, while helping to defend both national security and civil liberties.

In contrast, secrecy, retaliation and intimidation undermine our Constitutional rights and weaken our democratic processes more swiftly, more surely, and more corrosively than the acts of terror from which they purport to protect us.

"How the NSA's Surveillance Procedures Threaten Americans' Privacy," Statement by American Civil Liberties Union, New York (June 21, 2013)

Source: American Civil Liberties Union

Newly released documents confirm what critics have long suspected—that the National Security Agency, a component of the Defense Department, is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans' international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans' privacy are weak and riddled with exceptions.

The FISA Amendment Act signed into law by President Bush in 2008, expanded the government's authority to monitor Americans' electronic communications. Critics of the law feared the NSA would use the law to conduct broad surveillance of Americans' international communications and, in the process, capture an unknown quantity of purely domestic communications. Government officials contended that the law authorized surveillance of foreign nationals outside the United States—not of Americans—and that it included robust safeguards to protect Americans' privacy. Last year, in a successful effort to derail a constitutional challenge to the law, the Obama administration made these same claims to the U.S. Supreme Court.

Now the *Guardian* has published two previously secret documents that show how the FISA Amendments Act is being implemented. One document sets out the government's "targeting procedures"—the procedures it uses to determine whether it has the authority to acquire communications in the first place. The other sets out the government's "minimization procedures"—the procedures that govern the retention, analysis and dissemination of the communications it acquires. Both documents—the "Procedures"—have apparently been endorsed by the Foreign Intelligence Surveillance Court, which oversees government surveillance in some national security cases.

The Procedures are complex, but at least some of their flaws are clear.

1. The Procedures permit the NSA to monitor Americans' international communications in the course of surveillance targeted at foreigners abroad.

The NSA "is not listening to Americans' phone calls or monitoring their emails," the Chairman of the House Intelligence Committee recently said, and many other government officials, including the

president himself, have made similar assurances. But these statements are not true. While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans' communications with those foreign targets. Indeed, in advocating for the Act, government officials made clear that these "one-end-domestic" communications were the ones of most interest to them. The Procedures contemplate not only that the NSA will acquire Americans' international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans' communications that contain "foreign intelligence information" or evidence of a crime can be retained forever, and even communications that don't can be retained for as long as five years. Despite government officials' claims to the contrary, the NSA is building a growing database of Americans' international telephone calls and emails.

2. The Procedures allow the surveillance of Americans by failing to ensure that the NSA's surveillance targets are in fact foreigners outside the United States.

The Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the U.S. government sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts the government's premise, the Procedures fail to ensure that the NSA's surveillance targets are *in fact* foreigners outside the United States. This is because the Procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

3. The Procedures permit the government to conduct surveillance that has no real connection to the government's foreign intelligence interests.

One of the fundamental problems with the Act is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who aren't even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the Act allows the government to conduct surveillance only if one of its purposes is to gather "foreign intelligence information." That term, though, is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense and even "the foreign affairs of the United States." The Procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner's address book. In other words, the NSA seems to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA's surveillance.

4. The Procedures permit the NSA to collect international communications, including Americans' international communications, in bulk.

On its face, the Act permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the Act made clear that this was one of its principal purposes, and unsurprisingly, the Procedures give effect to that design. While they require the government to identify a "target" outside the country, once the target has been identified the Procedures permit the NSA to sweep up the communications of any foreigner who may be communicating "about" the target. The Procedures contemplate that the NSA will do this by "employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," by "target[ing] Internet links that terminate in a foreign country," or by identifying "the country code of the telephone number." However the NSA does it, the result is the same: millions of communications may be swept up, Americans' international communications among them.

5. The Procedures allow the NSA to retain even purely domestic communications.

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some

of the communications the NSA collects under the Act, then, will be purely domestic. (Notably, a 2009 *New York Times* article discusses an episode in which the NSA used the Act to engage in "significant and systemic" over collection of such domestic communications.) The Act should require the NSA to purge these communications from its databases, but it does not. The Procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime or encrypted information. Again, foreign intelligence information is defined exceedingly broadly. The result is that the NSA is steadily building a database of Americans' purely domestic calls and emails.

6. The Procedures allow the government to collect and retain communications protected by the attorney–client privilege.
The Procedures expressly contemplate that the NSA will collect attorney–client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the Procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The Procedures include a more restrictive rule for communications between attorneys and their clients who have been criminally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

7. The Procedures contemplate that the NSA will maintain "knowledge databases" containing sensitive information about Americans.
To determine whether a target is a foreigner abroad, the Procedures contemplate that the NSA will consult various NSA databases containing information collected by it and other agencies through signals intelligence, human intelligence, law enforcement and other means. These databases—referred to as "NSA content repositories" and "knowledge databases"—apparently house internet data, including metadata that reveals online activities, as well as telephone numbers and email addresses that the agency has reason to believe are being used by U.S. persons. The Procedures' reference to "Home Location Registers," which receive updates whenever a phone "moves into a new service area," suggests that the NSA also collects some form of location information about millions of Americans' cellphones. The Procedures do not say what limits apply to these databases or what safeguards, if any, are in place to protect Americans' constitutional rights.

8. The Procedures allow the NSA to retain encrypted communications indefinitely.
The Procedures permit the NSA to retain, forever, all communications—even purely domestic ones—that are encrypted. The use of encryption to protect data is a routine and sometimes legally required practice by financial organizations, health care providers, and real-time communications services (like Skype and Apple's FaceTime). Accordingly, the Procedures permit the NSA to retain huge volumes of Americans' most sensitive information.

Press Release, Office of United Nations Commissioner for Human Rights Navi Pillay, on Edward Snowden and Surveillance, Geneva (July 12, 2013)

Source: Office of the United Nations High Commissioner for Human Rights

GENEVA (12 July 2013) – The situation of Edward Snowden and alleged large-scale violations of the right of privacy by surveillance programs raise a number of important international human rights issues which need to be addressed, the UN High Commissioner for Human Rights, Navi Pillay, said on Friday.

"While concerns about national security and criminal activity may justify the exceptional and narrowly tailored use of surveillance programs, surveillance without adequate safeguards to protect the right to privacy actually risks impacting negatively on the enjoyment of human rights and fundamental freedoms," Pillay said.

"Both Article 12 of the Universal Declaration of Human rights and Article 17 of the International Covenant on Civil and Political rights state that no one shall be subjected to arbitrary interference with one's privacy, family, home or correspondence, and that everyone has the right to the protection of the law against such interference or attacks," said the High Commissioner.

"People need to be confident that their private communications are not being unduly scrutinized by the State," the High Commissioner noted.

"The right to privacy, the right to access to information and freedom of expression are closely linked. The public has the democratic right to take part in public affairs and this right cannot be effectively exercised by solely relying on authorized information," Pillay said.

"Snowden's case has shown the need to protect persons disclosing information on matters that have implications for human rights, as well as the importance of ensuring respect for the right to privacy," Pillay said.

"National legal systems must ensure that there are adequate avenues for individuals disclosing violations of human rights to express their concern without fear of reprisals," she added.

As stated by the former UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, "reliable factual information about serious human rights violations by an intelligence agency is most likely to come from within the agency itself. In these cases, the public interest in disclosure outweighs the public interest in non-disclosure. Such whistleblowers should firstly be protected from legal reprisals and disciplinary action when disclosing unauthorized information."

The UN Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms contains important provisions for the protection of the right to defend human rights. Those who reveal information that they reasonably believe to indicate the commission of human rights violations are entitled to such protection.

"Without prejudging the validity of any asylum claim by Snowden, I appeal to all States to respect the internationally guaranteed right to seek asylum, in accordance with Article 14 of the Universal Declaration and Article 1 of the UN Convention relating to the status of Refugees, and to make any such determination in accordance with their international legal obligations," Pillay said.

Testimony of Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union Foundation, and Laura W. Murphy, Director, Washington Legislative Office American Civil Liberties Union, before the House Committee on the Judiciary Oversight Hearing on the Administration's Use of FISA Authorities (July 17, 2013)

Source: American Civil Liberties Union

On behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide, thank you for inviting the ACLU to testify before the Committee.

Over the last six weeks it has become clear that the National Security Agency (NSA) is engaged in far-reaching, intrusive, and unlawful surveillance of Americans' telephone calls and electronic communications. That the NSA is engaged in this surveillance is the result of many factors. The Foreign Intelligence Surveillance Act (FISA) affords the government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and scope of the government's surveillance activities. Structural features of the Foreign Intelligence Surveillance Court (FISC) have prevented that court from serving as an effective guardian of individual rights. And the ordinary federal courts have improperly used procedural doctrines to place the NSA's activities beyond the reach of the Constitution.

To say that the NSA's activities present a grave danger to American democracy is no overstatement. Thirty-seven years ago, after conducting a comprehensive investigation into the intelligence abuses of the previous decades, the Church Committee warned that inadequate regulations on government surveillance "threaten[ed] to undermine our democratic society and fundamentally alter its nature." This warning should have even more resonance today, because in recent decades the NSA's resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more powerful.

Because the problem Congress confronts today has many roots, there is no single solution to it. It is crucial, however, that Congress take certain steps immediately. It should amend relevant provisions of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans'

communications. It should require the publication of past and future FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should ensure that the public has access to basic information, including statistical information, about the government's use of new surveillance authorities. It should also hold additional hearings to consider further amendments to FISA—including amendments to make FISC proceedings more transparent.

I. Metadata surveillance under Section 215 of the Patriot Act

On June 5, 2013, the *Guardian* disclosed a previously secret FISC order that compels a Verizon subsidiary, Verizon Business Network Services (VBNS), to supply the government with records relating to every phone call placed on its network between April 25, 2013 and July 19, 2013.[1] The order directs VBNS to produce to the NSA "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating its customers' calls, including those "wholly within the United States."[2] As many have noted, the order is breathtaking in its scope. It is as if the government had seized every American's address book—with annotations detailing which contacts she spoke to, when she spoke with them, for how long, and (possibly) from which locations.

News reports since the disclosure of the VBNS order indicate that the mass acquisition of Americans' call details extends beyond customers of VBNS, encompassing subscribers of the country's three largest phone companies: Verizon, AT&T, and Sprint.[3] Members of the congressional intelligence committees have confirmed that the order issued to VBNS is part of a broader program under which the government has been collecting the telephone records of essentially all Americans for at least seven years.[4]

a. The metadata program is not authorized by statute

The metadata program has been implemented under Section 215 of the Patriot Act—sometimes referred to as FISA's "business records" provision—but this provision does not permit the government to track all Americans' phone calls, let alone over a period of seven years.

As originally enacted in 1998, FISA's business records provision permitted the FBI to compel the production of certain business records in foreign intelligence or international terrorism investigations by making an application to the FISC. *See* 50 U.S.C. §§ 1861-62 (2000 ed.). Only four types of records could be sought under the statute: records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities. 50 U.S.C. § 1862 (2000 ed.). Moreover, the FISC could issue an order only if the application contained "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power." *Id.*

The business records power was considerably expanded by the Patriot Act.[5] Section 215 of that Act, now codified in 50 U.S.C. § 1861, permitted the FBI to make an application to the FISC for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities… 50 U.S.C. § 1861(a)(1) (emphasis added).

No longer limited to four discrete categories of business records, the new law authorized the FBI to seek the production of "any tangible things." *Id.* It also authorized the FBI to obtain orders without demonstrating reason to believe that the target was a foreign power or agent of a foreign power. Instead, it permitted the government to obtain orders where tangible things were "sought for" an authorized investigation. P.L. 107-56, § 215. This language was further amended by the USA PATRIOT Improvement and Reauthorization Act of 2005, P.L. 109-177, § 106(b). Under the current version of the business records provision, the FBI must provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant*" to a foreign intelligence, international terrorism, or espionage investigation. 50 U.S.C. § 1861(b)(2)(A) (emphasis added).[6]

While the Patriot Act considerably expanded the government's surveillance authority, Section 215 does not authorize the metadata program. First, whatever "relevance" might allow, it does not permit the government to cast a seven-year dragnet over the records of every phone call made or received by any American. Indeed, to say that Section 215 authorizes this surveillance is to deprive the word "relevance" of any meaning. The government's theory appears to be that some

of the information swept up in the dragnet might become relevant to "an authorized investigation" at some point in the future. The statute, however, does not permit the government to collect information on this basis. *Cf.* Jim Sensenbrenner, "This Abuse of the Patriot Act Must End," *Guardian,* June 9, 2013, http://bit.ly/18iDA3x ("[B]ased on the scope of the released order, both the administration and the FISA court are relying on an unbounded interpretation of the act that Congress never intended."). The statute requires the government to show a connection between the records it seeks and some specific, existing investigation.

Indeed, the changes that Congress made to the statute in 2006 were meant to ensure that the government did not exploit ambiguity in the statute's language to justify the collection of sensitive information not actually connected to some authorized investigation. As Senator Jon Kyl put it in 2006, "We all know the term 'relevance.' It is a term that every court uses. The relevance standard is exactly the standard employed for the issuance of discovery orders in civil litigation, grand jury subpoenas in a criminal investigation."[7]

As Congress recognized in 2006, relevance is a familiar standard in our legal system. It has never been afforded the limitless scope that the executive branch is affording it now. Indeed, in the past, courts have carefully policed the outer perimeter of "relevance" to ensure that demands for information are not unbounded fishing expeditions. *See, e.g., In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973) ("What is more troubling is the matter of relevance. The [grand jury] subpoena requires production of all documents contained in the files, without any attempt to define classes of potentially relevant documents or any limitations as to subject matter or time period.").[8] The information collected by the government under the metadata program goes far beyond anything a court has ever allowed under the rubric of "relevance."[9]

b. The metadata program is unconstitutional

President Obama and intelligence officials have been at pains to emphasize that the government is collecting metadata, not content. The suggestion that metadata is somehow beyond the reach of the Constitution, however, is not correct. For Fourth Amendment purposes, the crucial question is not whether the government is collecting content or metadata but whether it is invading reasonable expectations of privacy. In the case of bulk collection of Americans' phone records, it clearly is.

The Supreme Court's recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012), is instructive. In that case, a unanimous Court held that long-term surveillance of an individual's location constituted a search under the Fourth Amendment. The Justices reached this conclusion for different reasons, but at least five Justices were of the view that the surveillance infringed on a reasonable expectation of privacy. Justice Sotomayor observed that tracking an individual's movements over an extended period allows the government to generate a "precise, comprehensive record" that reflects "a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* (Sotomayor, J., concurring).

The same can be said of the tracking now taking place under Section 215. Call records can reveal personal relationships, medical issues, and political and religious affiliations. Internet metadata may be even more revealing, allowing the government to learn which websites a person visits, precisely which articles she reads, whom she corresponds with, and whom *those* people correspond with.

The long-term surveillance of metadata constitutes a search for the same reasons that the long-term surveillance of location was found to constitute a search in *Jones*. In fact, the surveillance held unconstitutional in *Jones* was narrower and shallower than the surveillance now taking place under Section 215. The location tracking in *Jones* was meant to further a specific criminal investigation into a specific crime, and the government collected information about one person's location over a period of less than a month. What the government has implemented under Section 215 is an indiscriminate program that has already swept up the communications of millions of people over a period of seven years.

Some have defended the metadata program by reference to the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which upheld the installation of a pen register in a criminal investigation. The pen register in *Smith*, however, was very primitive—it tracked the numbers being dialed, but it didn't indicate which calls were completed, let alone the duration of the calls. Moreover, the surveillance was directed at a single criminal suspect over a period of less than two days. The police were not casting a net over the whole country.

Another argument that has been offered in defense of the metadata program is that, though

the NSA collects an immense amount of information, it examines only a tiny fraction of it. But the Fourth Amendment is triggered by the *collection* of information, not simply by the querying of it. The NSA cannot insulate this program from Fourth Amendment scrutiny simply by promising that Americans' private information will be safe in its hands. The Fourth Amendment exists to prevent the government from acquiring Americans' private papers and communications in the first place.

Because the metadata program vacuums up sensitive information about associational and expressive activity, it is also unconstitutional under the First Amendment. The Supreme Court has recognized that the government's surveillance and investigatory activities have an acute potential to stifle association and expression protected by the First Amendment. *See, e.g., United States v. U.S. District Court*, 407 U.S. 297 (1972). As a result of this danger, courts have subjected investigatory practices to "exacting scrutiny" where they substantially burden First Amendment rights. *See, e.g., Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation); *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102-03 (2d Cir. 1985) (grand jury subpoena). The metadata program cannot survive this scrutiny. This is particularly so because all available evidence suggests that the program is far broader than necessary to achieve the government's legitimate goals. *See, e.g.*, Press Release, "Wyden, Udall Question the Value and Efficacy of Phone Records Collection in Stopping Attacks," June 7, 2013, http://1.usa.gov/19Q1Ng1 ("As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.").

c. Congress should amend Section 215 to prohibit suspicionless, dragnet collection of "tangible things"

As explained above, the metadata program is neither authorized by statute nor constitutional. As the government and FISC have apparently found to the contrary, however, the best way for Congress to protect Americans' privacy is to narrow the statute's scope. The ACLU urges Congress to amend Section 215 to provide that the government may compel the production of records under the provision only where there is a close connection between the records sought and a foreign power or agent of a foreign power. Several bipartisan bills now in the House and Senate should be considered by this Committee and Congress at large. The LIBERT-E Act, H.R. 2399, 113th Cong. (2013), sponsored by Ranking Member Conyers, Rep. Justin Amash, and forty others, would tighten the relevance requirement, mandating that the government supply "specific and articulable facts showing that there are reasonable grounds to believe that the tangible things sought are relevant and material," and that the records sought "pertain only to an individual that is the subject of such investigation." A bill sponsored by Senators Udall and Wyden would similarly tighten the required connection between the government's demand for records and a foreign power or agent of a foreign power. Congress could also consider simply restoring some of the language that was deleted by the Patriot Act—in particular, the language that required the government to show "specific and articulable facts giving reason to believe that the person to whom the records pertain[ed] [was] a foreign power or an agent of a foreign power."

II. Electronic surveillance under Section 702 of FISA

The metadata program is only one part of the NSA's domestic surveillance activities. Recent disclosures show that the NSA is also engaged in large-scale monitoring of Americans' electronic communications under Section 702 of FISA, which codifies the FISA Amendments Act of 2008.[10] Under this program, labeled "PRISM" in NSA documents, the government collects emails, audio and video chats, photographs, and other internet traffic from nine major service providers—Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.[11] The Director of National Intelligence has acknowledged the existence of the PRISM program but stated that it involves surveillance of foreigners outside the United States.[12] This is misleading. The PRISM program involves the collection of Americans' communications, both international and domestic, and for reasons explained below, the program is unconstitutional.

a. Section 702 is unconstitutional

President Bush signed the FISA Amendments Act into law on July 10, 2008.[13] While leaving FISA in place for purely domestic communications, the FISA Amendments Act revolutionized the FISA

regime by permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans' international communications. Under the FISA Amendments Act, the Attorney General and Director of National Intelligence ("DNI") can "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. 1881a(a). The government is prohibited from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," *Id.*§ 1881a(b)(1), but an acquisition authorized under the FISA Amendments Act may nonetheless sweep up the international communications of U.S. citizens and residents.

Before authorizing surveillance under Section 702—or, in some circumstances, within seven days of authorizing such surveillance—the Attorney General and the DNI must submit to the FISA Court an application for an order (hereinafter, a "mass acquisition order"). *Id.*§ 1881a(a), (c)(2). A mass acquisition order is a kind of blank check, which once obtained permits—without further judicial authorization—whatever surveillance the government may choose to engage in, within broadly drawn parameters, for a period of up to one year.

To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISA Court "a written certification and any supporting affidavit" attesting that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "targeting procedures" reasonably designed to ensure that the acquisition is "limited to targeting persons reasonably believed to be located outside the United States," and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States." *Id.*§ 1881a(g)(2)(A)(i).

The certification and supporting affidavit must also attest that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "minimization procedures" that meet the requirements of 50 U.S.C. § 1801(h) or § 1821(4).

Finally, the certification and supporting affidavit must attest that the Attorney General has adopted "guidelines" to ensure compliance with the limitations set out in § 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose of the acquisition is to obtain foreign intelligence information." *Id.*§ 1881a(g)(2)(A)(iii)–(vii).

Importantly, Section 702 does not require the government to demonstrate to the FISA Court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government's certification is not required to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed. *Id.* § 1881a(g)(4).

Nor does Section 702 place meaningful limits on the government's retention, analysis, and dissemination of information that relates to U.S. citizens and residents. The Act requires the government to adopt "minimization procedures," *Id.*§ 1881a, that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons," *Id.*§§ 1801(h)(1), 1821(4)(A). The Act does not, however, prescribe specific minimization procedures. Moreover, the FISA Amendments Act specifically allows the government to retain and disseminate information—including information relating to U.S. citizens and residents—if the government concludes that it is "foreign intelligence information." *Id.*§ 1881a(e) (referring to *Id.*§§ 1801(h)(1), 1821(4)(A)). The phrase "foreign intelligence information" is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs. *Id.*§ 1801(e).

As the FISA Court has itself acknowledged, its role in authorizing and supervising surveillance under the FISA Amendments Act is "narrowly circumscribed."[14] The judiciary's traditional role under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its role under the FISA Amendments Act is to issue advisory opinions blessing in advance broad parameters and targeting procedures, under which the government is then free to conduct surveillance for up to one year. Under Section 702, the FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and

does not closely supervise the implementation of the government's targeting or minimization procedures. In short, the role that the FISA Court plays under the FISA Amendments Act bears no resemblance to the role that it has traditionally played under FISA.

The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702.[15] The statute's defects include:

Section 702 allows the government to collect Americans' international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored.

Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court whom it intends to target or which facilities it intends to monitor, and without making any showing to the court—or even making an internal executive determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, Section 702 allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the FISA Amendments Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications *en masse*. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

Section 702 allows the government to conduct intrusive surveillance without meaningful judicial oversight.

Under Section 702, the government is authorized to conduct intrusive surveillance without meaningful judicial oversight. The FISA Court does not review individualized surveillance applications. It does not consider whether the government's surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government why it is initiating any particular surveillance program. The FISA Court's role is limited to reviewing the government's "targeting" and "minimization" procedures. And even with respect to the procedures, the FISA court's role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time.

Section 702 places no meaningful limits on the government's retention and dissemination of information relating to U.S. citizens and residents.

As a result of the FISA Amendments Act, thousands or even millions of U.S. citizens and residents will find their international telephone and email communications swept up in surveillance that is "targeted" at people abroad. Yet the law fails to place any meaningful limitations on the government's retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt "minimization" procedures—procedures that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." However, these minimization procedures must accommodate the government's need "to obtain, produce, and disseminate foreign intelligence information." In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is "foreign intelligence information." Because "foreign intelligence information" is defined broadly (as discussed below), this is an exception that swallows the rule.

Section 702 does not limit government surveillance to communications relating to terrorism.

The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather "foreign intelligence information." There are multiple problems with this. First, under the new law the "foreign intelligence" requirement applies to entire surveillance

programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase "foreign intelligence information" has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the "foreign affairs of the United States." Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and email that relates to the foreign affairs of the U.S.

b. The NSA's "targeting" and "minimization" procedures do not mitigate the statute's constitutional deficiencies.

Since the FISA Amendments Act was enacted in 2008, the government's principal defense of the law has been that "targeting" and "minimization" procedures supply sufficient protection for Americans' privacy. Because the procedures were secret, the government's assertion was impossible to evaluate. Now that the procedures have been published, however,[16] it is plain that the assertion is false. Indeed, the procedures confirm what critics have long suspected—that the NSA is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans' international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans' privacy are weak and riddled with exceptions.

The NSA's procedures permit it to monitor Americans' international communications in the course of surveillance targeted at foreigners abroad.

While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans' communications with those foreign targets. The recently disclosed procedures contemplate not only that the NSA will acquire Americans' international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans' communications that contain "foreign intelligence information" or evidence of a crime can be retained forever, and even communications that don't can be retained for as long as five years. Despite government officials' claims to the contrary, the NSA is building a growing database of Americans' international telephone calls and emails.

The NSA's procedures allow the surveillance of Americans by failing to ensure that its surveillance targets are in fact foreigners outside the United States.

The FISA Amendments Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the NSA sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts this premise, the NSA's procedures fail to ensure that its surveillance targets are *in fact* foreigners outside the United States. This is because the procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

The NSA's procedures permit the government to conduct surveillance that has no real connection to the government's foreign intelligence interests.

One of the fundamental problems with Section 702 is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who are not even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the FISA Amendments Act allows the government to conduct surveillance only if one of its purposes is to gather "foreign intelligence information." As noted above, however, that term is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even "the foreign affairs of the United States." The NSA's procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another

is whether it is listed in a foreigner's address book. In other words, the NSA appears to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA's surveillance.

The NSA's procedures permit the NSA to collect international communications, including Americans' international communications, in bulk.

On its face, Section 702 permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the FISA Amendments Act made clear that this was one of its principal purposes, and unsurprisingly, the procedures give effect to that design. While they require the government to identify a "target" outside the country, once the target has been identified the procedures permit the NSA to sweep up the communications of any foreigner who may be communicating "about" the target. The Procedures contemplate that the NSA will do this by "employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," by "target[ing] Internet links that terminate in a foreign country," or by identifying "the country code of the telephone number." However the NSA does it, the result is the same: millions of communications may be swept up, Americans' international communications among them.

The NSA's procedures allow the NSA to retain even purely domestic communications.

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some of the communications the NSA collects under the Act, then, will be purely domestic.[17] The Act should require the NSA to purge these communications from its databases, but it does not. The procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime, or encrypted information. Again, foreign intelligence information is defined exceedingly broadly.

The NSA's procedures allow the government to collect and retain communications protected by the attorney-client privilege.

The procedures expressly contemplate that the NSA will collect attorney-client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The procedures include a more restrictive rule for communications between attorneys and their clients who have been criminally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

c. Congress should amend Section 702 to prohibit suspicionless, dragnet collection of Americans' communications.

For the reasons discussed above, the ACLU believes that the FISA Amendments Act is unconstitutional on its face. There are many ways, however, that Congress could provide meaningful protection for privacy while preserving the statute's broad outline. One bill introduced by Senator Wyden during the reauthorization debate last fall would have prohibited the government from searching through information collected under the FISA Amendments Act for the communications of specific, known U.S. persons. Bills submitted during the debate leading up to the passage of the FISA Amendments Act in 2008 would have banned dragnet collection in the first instance or required the government to return to the FISC before searching communications obtained through the FISA Amendments Act for information about U.S. persons. Congress should examine these proposals again and make amendments to the Act that would provide greater protection for individual privacy and mitigate the chilling effect on rights protected by the First Amendment.

III. Excessive secrecy surrounds the government's use of FISA authorities.

Amendments to FISA since 2001 have substantially expanded the government's surveillance authorities, but the public lacks crucial information about the way these authorities have been implemented. Rank-and-file members of

Congress and the public have learned more about domestic surveillance in the last two months than in the last several decades combined. While the Judiciary and Intelligence Committees have received some information in classified format, only members of the Senate Select Committee on Intelligence, party leadership, and a handful of Judiciary Committee members have staff with clearance high enough to access the information and advise their principals. Although the Inspectors General and others file regular reports with the Committees of jurisdiction, these reports do not include even basic information such how many Americans' communications are swept up in these programs, or how and when Americans' information is accessed and used.

Nor does the public have access to the FISC decisions that assess the meaning, scope, and constitutionality of the surveillance laws. Aggregate statistics alone would not allow the public to understand the reach of the government's surveillance powers; as we have seen with Section 215, one application may encompass millions of individual records. Public access to the FISA Court's substantive legal reasoning is essential. Without it, some of the government's most far-reaching policies will lack democratic legitimacy. Instead, the public will be dependent on the discretionary disclosures of executive branch officials—disclosures that have sometimes been self-serving and misleading in the past.[18] Needless to say, it may be impossible to release FISC opinions without redacting passages concerning the NSA's sources and methods. The release of redacted opinions, however, would be far better than the release of nothing at all.

Congress should require the release of FISC opinions concerning the scope, meaning, or constitutionality of FISA, including opinions relating to Section 215 and Section 702. Administration officials have said there are over a dozen such opinions, some close to one hundred pages long.[19] Executive officials testified before Congress several years ago that declassification review was already underway,[20] and President Obama directed the DNI to revisit that process in the last few weeks. If the administration refuses to release these opinions, Congress should consider legislation compelling their release. Possible vehicles include the LIBERT-E Act, cited above, or the Ending Secret Law Act, H.R. 2475, 113th Cong. (2013), a bipartisan bill sponsored by Rep. Adam Schiff, Todd Rokita, and sixteen other members of the House.

Congress should also require the release of information about the type and volume of information that is obtained under dragnet surveillance programs. The leaked Verizon order confirms that the government is using Section 215 to collect telephony metadata about every phone call made by VBNS subscribers in the United States. That the government is using Section 215 for this purpose raises the question of what other "tangible things" the government may be collecting through similar dragnets. For reasons discussed above, the ACLU believes that these dragnets are unauthorized by the statute as well as unconstitutional. Whatever their legality, however, the public has a right to know, at least in general terms, what kinds of information the government is collecting about innocent Americans, and on what scale.

IV. Summary of recommendations

As discussed above, the ACLU urges Congress to:

—Amend Section 215 of the Patriot Act and Section 702 of FISA to prohibit suspicionless, "dragnet" monitoring or tracking of Americans' communications.

—Require the publication of past and future FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws.

—Require the publication of information about the type and volume of information that the government obtains under dragnet surveillance programs.

—Hold additional hearings to consider further amendments to FISA—including amendments to make FISC proceedings more transparent.

Thank you for this opportunity to present the ACLU's views.

1 See Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily", *Guardian*, June 5, 2013, http://bit.ly/13jsdlb.

2 Secondary Order, *In Re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs.*, Inc. d/b/a Verizon Bus. Servs., No. BR 13-80 at 2 (FISA Ct. Apr. 25, 2013), available at http://bit.ly/11FY393.

3 See Siobhan Gorman et al., "U.S. Collects Vast Data Trove," *Wall St. J.,* June 7, 2013, http://on.wsj.com/11uD0ue ("The arrangement

with Verizon, AT&T and Sprint, the country's three largest phone companies, means that every time the majority of Americans make a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation, according to people familiar with the matter. . . . AT&T has 107.3 million wireless customers and 31.2 million landline customers. Verizon has 98.9 million wireless customers and 22.2 million landline customers while Sprint has 55 million customers in total."); Siobhan Gorman & Jennifer Valentino-DeVries, "Government Is Tracking Verizon Customers' Records," *Wall St. J.*, June 6, 2013, http://on.wsj.com/13mLm7c.

In the days following the *Guardian*'s disclosure of the Verizon order, officials revealed other details about the government's surveillance under Section 215. See James R. Clapper, DNI Statement on Recent Unauthorized Disclosures of Classified Information, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13jwuFc. The DNI stated, for example, that "the [FISC] only allows the data to be queried when there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization."

4 Dan Roberts & Spencer Ackerman, "Senator Feinstein: NSA Phone Call Data Collection in Place 'Since 2006'," *Guardian*, June 6, 2013, http://bit.ly/13rfxdu; *id.* (Senator Saxby Chambliss: "This has been going on for seven years.").

5 For ease of reference, this testimony uses "business records provision" to refer to the current version of the law as well as to earlier versions, even though the current version of the law allows the FBI to compel the production of much more than business records, as discussed below.

6 Records are presumptively relevant if they pertain to (1) a foreign power or an agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. This relaxed standard is a significant departure from the original threshold, which, as noted above, required an individualized inquiry.

7 Jennifer Valentino-Devries & Siobhan Gorman, "Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering," *Wall St. J.*, July 8, 2013, http://on.wsj.com/13x8QKU.

8 *See also Hale v. Henkel*, 201 U.S. 43, 76-77 (1906).

9 The metadata program also violates Section 215 because the statute does not authorize the prospective acquisition of business records. The text of the statute contemplates "release" of "tangible things" that can be "fairly identified," and "allow[s] a reasonable time" for providers to "assemble" those things. 50 U.S.C. § 1861(c)(1)-(2). These terms suggest that Section 215 reaches only business records already in existence.

10 Barton Gellman & Laura Poitras, "U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program," *Wash. Post*, June 7, 2013, http://wapo.st/1888aNr.

11 While news reports have generally described PRISM as an NSA "program," the publicly available documents leave open the possibility that PRISM is instead the name of the NSA database in which content collected from these providers is stored.

12 James R. Clapper, DNI Statement on Activities Authorized Under Section 702 of FISA, Office of the Director of National Intelligence (June 6, 2013), http://1.usa.gov/13JJdBE; see also James R. Clapper, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013), http://1.usa.gov/10YY4tp.

13 A description of electronic surveillance prior to the passage of the FISA Amendments Act, including the warrantless wiretapping program authorized by President Bush beginning in 2001, is available in Mr. Jaffer's earlier testimony to the Committee. *See* The FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security, H. Comm. on the Judiciary, 112th Cong. (May 31, 2012) (written testimony of Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union Foundation), *available at* http://bit.ly/14Q61Bs.

14 In *re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted) *available at* http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf.

15 The ACLU raised many of these defects in a constitutional challenge to the FISA Amendments Act filed just hours after the Act was signed into law in 2008. The case, *Amnesty v. Clapper*, was filed on behalf of a broad coalition of attorneys and human rights, labor, legal and media organizations whose work requires them to engage in sensitive and sometimes privileged telephone and email communications with individuals located outside the United States. In a 5-4 ruling handed down on February 26, 2013, the Supreme Court held that the ACLU's plaintiffs did not have standing to challenge the constitutionality of the Act because they could not show, at the outset, that their communications had been monitored by the government. *See Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013). The Court did not reach the merits of plaintiffs' constitutional challenge.

16 See Glenn Greenwald & James Ball, "The Top Secret Rules that Allow NSA to Use US Data Without a Warrant," *Guardian*, June 20, 2013, http://bit.ly/105qb9B.

17 Notably, a 2009 *New York Times* article discusses an episode in which the NSA used the Act to engage in "significant and systemic" overcollection of such domestic communications. Eric Lichtblau & James Risen, "Officials Say U.S. Wiretaps Exceeded Law," *N.Y. Times*, April 15, 2009, http://nyti.ms/16AIq5O.

18 See, e.g., Glenn Kessler, "James Clapper's 'Least Untruthful' Statement to the Senate," *Wash. Post*, June 12, 2013, http://wapo.st/170VVSu.

19 See Eric Lichtblau, In Secret, Court Vastly Broadens Powers of N.S.A., *N.Y. Times*, July 6, 2013, http://nyti.ms/12beiA3.

20 Prehearing Questions for Lisa O. Monaco Upon Her Nomination to be the Assistant Attorney General for National Security, Sen. Select Comm. on Intelligence, 112th Cong., at 12-13, available at http://bit.ly/10V5Ion.

Privacy, Technology, and National Security: An Overview of Intelligence Collection by Robert S. Litt, Office of the Director of National Intelligence General Counsel; Remarks prepared for delivery to the Brookings Institution, Washington, DC

(July 19, 2013)

Source: Office of the Director of National Intelligence

I. Introduction

I wish that I was here in happier times for the Intelligence Community. The last several weeks have seen a series of reckless disclosures of classified information about intelligence activities. These disclosures threaten to cause long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our Nation. And because the disclosures were made by people who did not fully understand what they were talking about, they were sensationalized and led to mistaken and misleading impressions. I hope to be able to correct some of these misimpressions today.

My speech today is prompted by disclosures about two programs that collect valuable foreign intelligence that has protected our Nation and its allies: the bulk collection of telephony metadata, and the so-called "PRISM" program. Some people claim that these disclosures were a form of "whistleblowing." But let's be clear. These programs are not illegal. They are authorized by Congress and are carefully overseen by the Congressional intelligence and judiciary committees. They are conducted with the approval of the Foreign Intelligence Surveillance Court and under its supervision. And they are subject to extensive, court-ordered oversight by the Executive Branch. In short, all three branches of Government knew about these programs, approved them, and helped to ensure that they complied with the law. Only time will tell the full extent of the damage caused by the unlawful disclosures of these lawful programs.

Nevertheless, I fully appreciate that it's not enough for us simply to assert that our activities are consistent with the letter of the law. Our Government's activities must always reflect and reinforce our core democratic values. Those of us who work in the intelligence profession share these values, including the importance of privacy. But security and privacy are not zero-sum. We have an obligation to give full meaning to both: to protect security while at the same time protecting privacy and other constitutional rights. But although our values are enduring, the manner in which our activities reflect those values must necessarily adapt to changing societal expectations and norms. Thus, the Intelligence Community continually evaluates and improves the safeguards we have in place to protect privacy, while at the same time ensuring that we can carry out our mission of protecting national security.

So I'd like to do three things today. First, I'd like to discuss very briefly the laws that govern intelligence collection activities. Second, I want to talk about the effect of changing technology, and the corresponding need to adapt how we protect privacy, on those collection activities. And third, I want to bring these two strands together, to talk about how some of these laws play out in practice—how we structure the Intelligence Community's collection activities under FISA to respond to these changes in a way that remains faithful to our democratic values.

II. Legal Framework

Let me begin by discussing in general terms the legal framework that governs intelligence collection activities. And it is a bedrock concept that those activities are bound by the rule of law. This is a topic that has been well addressed by others, including the general counsels of the CIA and NSA, so I will make this brief. We begin, of course, with the Constitution. Article II makes the President the Commander in Chief and gives him extensive responsibility for the conduct of foreign affairs. The ability to collect foreign intelligence derives from that constitutional source. The First Amendment protects freedom of speech. And the Fourth Amendment prohibits unreasonable searches and seizures.

I want to make a few points about the Fourth Amendment. First, under established Supreme Court rulings a person has no legally recognized expectation of privacy in information that he or she gives to a third party. So obtaining those records from the third party is not a search as to that person. I'll return to this point in a moment. Second, the Fourth Amendment doesn't apply to foreigners outside of the United States. Third, the Supreme Court has said that the "reasonableness" of a warrantless search depends on balancing the "intrusion on the individual's Fourth Amendment interests against" the search's "promotion of legitimate Governmental interests."

In addition to the Constitution, a variety of statutes govern our collection activities. First, the National Security Act and a number of laws relating to specific agencies, such as the CIA Act and the NSA Act, limit what agencies can do, so that, for example, the CIA cannot engage in domestic law enforcement. We are also governed by laws such as the Electronic Communications Privacy Act, the Privacy Act and, in particular, the Foreign Intelligence Surveillance Act, or FISA. FISA was passed by Congress in 1978 and significantly amended in 2001 and 2008. It regulates electronic surveillance and certain other activities carried out for foreign intelligence purposes. I'll have much more to say about FISA later.

A final important source of legal restrictions is Executive Order 12333. This order provides additional limits on what intelligence agencies can do, defining each agency's authorities and responsibilities. In particular, Section 2.3 of EO 12333 provides that elements of the Intelligence Community "are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures…approved by the Attorney General…after consultation with" the Director of National Intelligence. These procedures must be consistent with the agencies' authorities. They must also establish strict limits on collecting, retaining or disseminating information about U.S. persons, unless that information is actually of foreign intelligence value, or in certain other limited circumstances spelled out in the order, such as to protect against a threat to life. These so-called "U.S. person rules" are basic to the operation of the Intelligence Community. They are among the first things that our employees are trained in, and they are at the core of our institutional culture.

It's not surprising that our legal regime provides special rules for activities directed at U.S. persons. So far as I know, every nation recognizes legal distinctions between citizens and non-citizens. But as I hope to make clear, our intelligence collection procedures also provide protection for the privacy rights of non-citizens.

III. Impact of Changing Societal Norms

Let me turn now to the impact of changing technology on privacy. Prior to the end of the nineteenth century there was little discussion about a "right to privacy." In the absence of mass media, photography and other technologies of the industrial age, the most serious invasions of privacy were the result of gossip or Peeping Toms. Indeed, in the 1890 article that first articulated the idea of a legal right to privacy, Louis Brandeis and Samuel Warren explicitly grounded that idea on changing technologies:

> *Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for*

securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-top."

Today, as a result of the way digital technology has developed, each of us shares massive amounts of information about ourselves with third parties. Sometimes this is obvious, as when we post pictures on social media or transmit our credit card numbers to buy products online. Other times it is less obvious, as when telephone companies store records listing every call we make. All in all, there's little doubt that the amount of data that each of us provides to strangers every day would astonish Brandeis and Warren—let alone Jefferson and Madison.

And this leads me to what I consider to be the key question. Why is it that people are willing to expose large quantities of information to private parties but don't want the Government to have the same information? Why, for example, don't we care if the telephone company keeps records of all of our phone calls on its servers, but we feel very differently about the prospect of the same information being on NSA servers? This does not seem to me to be a difficult question: we care because of what the Government could do with the information.

Unlike a phone company, the Government has the power to audit our tax returns, to prosecute and imprison us, to grant or deny licenses to do business, and many other things. And there is an entirely understandable concern that the Government may abuse this power. I don't mean to say that private companies don't have a lot of power over us. Indeed, the growth of corporate privacy policies, and the strong public reaction to the inadvertent release or commercial use of personal information, reinforces my belief that our primary privacy concern today is less with who has information than with what they do with it. But there is no question that the Government, because of its powers, is properly viewed in a different light.

On the other hand, just as consumers around the world make extensive use of modern technology, so too do potentially hostile foreign governments and foreign terrorist organizations. Indeed, we know that terrorists and weapons proliferators are using global information networks to conduct research, to communicate and to plan attacks. Information that can help us identify and prevent terrorist attacks or other threats to our security is often hiding in plain sight among the vast amounts of information flowing around the globe. New technology means that the Intelligence Community must continue to find new ways to locate and analyze foreign intelligence. We need to be able to do more than connect the dots when we happen to find them; we need to be able to find the right dots in the first place.

One approach to protecting privacy would be to limit the Intelligence Community to a targeted, focused query looking for specific information about an identified individual based on probable cause. But from the national security perspective, that would not be sufficient. The business of foreign intelligence has always been fundamentally different from the business of criminal investigation. Rather than attempting to solve crimes that have happened already, we are trying to find out what is going to happen before it happens. We may have only fragmentary information about someone who is plotting a terrorist attack, and need to find him and stop him. We may get information that is useless to us without a store of data to match it against, such as when we get the telephone number of a terrorist and want to find out who he has been in touch with. Or we may learn about a plot that we were previously unaware of, causing us to revisit old information and find connections that we didn't notice before—and that we would never know about if we hadn't collected the information and kept it for some period of time. We worry all the time about what we are missing in our daily effort to protect the Nation and our allies.

So on the one hand there are vast amounts of data that contains intelligence needed to protect us not only from terrorism, but from cyber attacks, weapons of mass destruction, and good old-fashioned espionage. And on the other hand, giving the Intelligence Community access to this data has obvious privacy implications. We achieve both security and privacy protection in this context in large part by a framework that establishes appropriate controls on what the Government can do with the information it lawfully collects, and appropriate oversight to ensure that it respects those controls. The protections depend on such factors as the type of information we collect, where we collect it, the scope of the collection, and the use the Government intends to make of

the information. In this way we can allow the Intelligence Community to acquire necessary foreign intelligence, while providing privacy protections that take account of modern technology.

IV. FISA Collection

In showing that this approach is in fact the way our system deals with intelligence collection, I'll use FISA as an example for a couple of reasons. First, because FISA is an important mechanism through which Congress has legislated in the area of foreign intelligence collection. Second, because it covers a wide range of activities, and involves all three sources of law I mentioned earlier: constitutional, statutory and executive. And third, because several previously classified examples of what we do under FISA have recently been declassified, and I know people want to hear more about them.

I don't mean to suggest that FISA is the only way we collect foreign intelligence. But it's important to know that, by virtue of Executive Order 12333, all of the collection activities of our intelligence agencies have to be directed at the acquisition of foreign intelligence or counterintelligence. Our intelligence priorities are set annually through an interagency process. The leaders of our Nation tell the Intelligence Community what information they need in the service of the Nation, its citizens and its interests, and we collect information in support of those priorities.

I want to emphasize that the United States, as a democratic nation, takes seriously this requirement that collection activities have a valid foreign intelligence purpose. We do not use our foreign intelligence collection capabilities to steal the trade secrets of foreign companies in order to give American companies a competitive advantage. We do not indiscriminately sweep up and store the contents of the communications of Americans, or of the citizenry of any country.

We do not use our intelligence collection for the purpose of repressing the citizens of any country because of their political, religious or other beliefs. We collect metadata—information about communications—more broadly than we collect the actual content of communications, because it is less intrusive than collecting content and in fact can provide us information that helps us more narrowly focus our collection of content on appropriate targets. But it simply is not true that the United States Government is listening to everything said by every citizen of any country.

Let me turn now to FISA. I'm going to talk about three provisions of that law: traditional FISA orders, the FISA business records provision, and Section 702. These provisions impose limits on what kind of information can be collected and how it can be collected, require procedures restricting what we can do with the information we collect and how long we can keep it, and impose oversight to ensure that the rules are followed. This sets up a coherent regime in which protections are afforded at the front end, when information is collected; in the middle, when information is reviewed and used; and at the back end, through oversight, all working together to protect both national security and privacy. The rules vary depending on factors such as the type of information being collected (and in particular whether or not we are collecting the content of communications), the nature of the person or persons being targeted, and how narrowly or broadly focused the collection is. They aren't identical in every respect to the rules that apply to criminal investigations, but I hope to persuade you that they are reasonable and appropriate in the very different context of foreign intelligence.

So let's begin by talking about traditional FISA collection. Prior to the passage of FISA in 1978, the collection of foreign intelligence was essentially unregulated by statutory law. It was viewed as a core function of the Executive Branch. In fact, when the criminal wiretap provisions were originally enacted, Congress expressly provided that they did not "limit the constitutional power of the President . . . to obtain foreign intelligence information . . . deemed essential to the national security of the United States." However, ten years later, as a result of abuses revealed by the Church and Pike Committees, Congress imposed a judicial check on some aspects of electronic surveillance for foreign intelligence purposes. This is what is now codified in Title I of FISA, sometimes referred to as "traditional FISA."

FISA established a special court, the Foreign Intelligence Surveillance Court, to hear applications by the Government to conduct electronic surveillance for foreign intelligence purposes. Because traditional FISA surveillance involves acquiring the content of communications, it is intrusive, implicating recognized privacy interests; and because it can be directed at individuals inside the United States, including American citizens, it implicates the Fourth Amendment. In FISA, Congress required that to get a "traditional" FISA

electronic surveillance order, the Government must establish probable cause to believe that the target of surveillance is a foreign power or an agent of a foreign power, a probable cause standard derived from the standard used for wiretaps in criminal cases. And if the target is a U.S. person, he or she cannot be deemed an agent of a foreign power based solely on activity protected by the First Amendment—you cannot be the subject of surveillance merely because of what you believe or think.

Moreover, by law the use of information collected under traditional FISA must be subject to minimization procedures, a concept that is key throughout FISA. Minimization procedures are procedures, approved by the FISA Court, that must be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning un-consenting United States persons consistent with the need of the United States to obtain, produce and disseminate foreign intelligence information." For example, they generally prohibit disseminating the identity of a U.S. person unless the identity itself is necessary to understand the foreign intelligence or is evidence of a crime. The reference to the purpose and technique of the particular surveillance is important. Minimization procedures can and do differ depending on the purpose of the surveillance and the technique used to implement it. These tailored minimization procedures are an important way in which we provide appropriate protections for privacy.

So let me explain in general terms how traditional FISA surveillance works in practice. Let's say that the FBI suspects someone inside the United States of being a spy, or a terrorist, and they want to conduct electronic surveillance. While there are some exceptions spelled out in the law, such as in the case of an emergency, as a general rule they have to present an application to the FISA Court establishing probable cause to believe that the person is an agent of a foreign power, according to the statutory definition. That application, by the way, is reviewed at several levels within both the FBI and Department of Justice before it is submitted to the Court. Now, the target may have a conversation with a U.S. person that has nothing to do with the foreign intelligence purpose of the surveillance, such as talking to a neighbor about a dinner party.

Under the minimization procedures, an analyst who listens to a conversation involving a U.S. person that has no foreign intelligence value cannot generally share it or disseminate it unless it is evidence of a crime. Even if a conversation has foreign intelligence value—let's say a terrorist is talking to a confederate—that information may only be disseminated to someone with an appropriate need to know the information pursuant to his or her mission.

In other words, electronic surveillance under FISA's Title I implicates the well-recognized privacy interest in the contents of communications, and is subject to corresponding protections for that privacy interest—in terms of the requirements that it be narrowly targeted and that it have a substantial factual basis approved by the Court, and in terms of the limitations imposed on use of the information.

Now let me turn to the second activity, the collection of business records. After FISA was passed, it became apparent that it left some significant gaps in our intelligence collection authority. In particular, while the Government had the power in a criminal investigation to compel the production of records with a grand jury subpoena, it lacked similar authority in a foreign intelligence investigation. So a provision was added in 1998 to provide such authority, and was amended by Section 215 of the USA-PATRIOT Act passed shortly after 9/11. This provision, which is generally referred to as "Section 215," allows us to apply to the FISA Court for an order requiring production of documents or other tangible things when they are relevant to an authorized national security investigation. Records can be produced only if they are the type of records that could be obtained pursuant to a grand jury subpoena or other court process—in other words, where there is no statutory or other protection that would prevent use of a grand jury subpoena. In some respects this process is more restrictive than a grand jury subpoena. A grand jury subpoena is issued by a prosecutor without any prior judicial review, whereas under the FISA business records provision we have to get court approval. Moreover, as with traditional FISA, records obtained pursuant to the FISA business records provision are subject to court-approved minimization procedures that limit the retention and dissemination of information about U.S. persons—another requirement that does not apply to grand jury subpoenas.

Now, of course, the FISA business records provision has been in the news because of one particular use of that provision. The FISA Court

has repeatedly approved orders directing several telecommunications companies to produce certain categories of telephone metadata, such as the number calling, the number being called, and the date, time and duration of the call. It's important to emphasize that under this program we do not get the content of any conversation; we do not get the identity of any party to the conversation; and we do not get any cell site or GPS locational information.

The limited scope of what we collect has important legal consequences. As I mentioned earlier, the Supreme Court has held that if you have voluntarily provided this kind of information to third parties, you have no reasonable expectation of privacy in that information. All of the metadata we get under this program is information that the telecommunications companies obtain and keep for their own business purposes. As a result, the Government can get this information without a warrant, consistent with the Fourth Amendment.

Nonetheless, I recognize that there is a difference between getting metadata about one telephone number and getting it in bulk. From a legal point of view, Section 215 only allows us to get records if they are "relevant" to a national security investigation, and from a privacy perspective people worry that, for example, the government could apply data mining techniques to a bulk data set and learn new personal facts about them—even though the underlying set of records is not subject to a reasonable expectation of privacy for Fourth Amendment purposes.

On the other hand, this information is clearly useful from an intelligence perspective: It can help identify links between terrorists overseas and their potential confederates in the United States. It's important to understand the problem this program was intended to solve. Many will recall that one of the criticisms made by the 9/11 Commission was that we were unable to find the connection between a hijacker who was in California and an al-Qaida safe house in Yemen. Although NSA had collected the conversations from the Yemen safe house, they had no way to determine that the person at the other end of the conversation was in the United States, and hence to identify the homeland connection. This collection program is designed to help us find those connections.

In order to do so, however, we need to be able to access the records of telephone calls, possibly going back many years. However, telephone companies have no legal obligation to keep this kind of information, and they generally destroy it after a period of time determined solely by their own business purposes. And the different telephone companies have separate datasets in different formats, which makes analysis of possible terrorist calls involving several providers considerably slower and more cumbersome. That could be a significant problem in a fast-moving investigation where speed and agility are critical, such as the plot to bomb the New York City subways in 2009.

The way we fill this intelligence gap while protecting privacy illustrates the analytical approach I outlined earlier. From a subscriber's point of view, as I said before, the difference between a telephone company keeping records of his phone calls and the Intelligence Community keeping the same information is what the Government could do with the records. That's an entirely legitimate concern. We deal with it by limiting what the Intelligence Community is allowed do with the information we get under this program—limitations that are approved by the FISA Court:

—First, we put this information in secure databases.
—Second, the only intelligence purpose for which this information can be used is counterterrorism.
—Third, we allow only a limited number of specially trained analysts to search these databases.
—Fourth, even those trained analysts are allowed to search the database only when they have a reasonable and articulable suspicion that a particular telephone number is associated with particular foreign terrorist organizations that have been identified to the Court. The basis for that suspicion has to be documented in writing and approved by a supervisor.
—Fifth, they're allowed to use this information only in a limited way, to map a network of telephone numbers calling other telephone numbers.
—Sixth, because the database contains only metadata, even if the analyst finds a previously unknown telephone number that warrants further investigation, all she can do is disseminate the telephone number. She doesn't even know whose number it is. Any further investigation of that number has to be done pursuant to other lawful means, and in particular, any collection of the contents of communications would have to be done using another valid legal authority, such as a traditional FISA.
—Finally, the information is destroyed after five years.

The net result is that although we collect large volumes of metadata under this program, we only look at a tiny fraction of it, and only for a carefully circumscribed purpose—to help us find links between foreign terrorists and people in the United States. The collection has to be broad to be operationally effective, but it is limited to non-content data that has a low privacy value and is not protected by the Fourth Amendment. It doesn't even identify any individual. Only the narrowest, most important use of this data is permitted; other uses are prohibited. In this way, we protect both privacy and national security.

Some have questioned how collection of a large volume of telephone metadata could comply with the statutory requirement that business records obtained pursuant to Section 215 be "relevant to an authorized investigation." While the Government is working to determine what additional information about the program can be declassified and disclosed, including the actual court papers, I can give a broad summary of the legal basis. First, remember that the "authorized investigation" is an intelligence investigation, not a criminal one. The statute requires that an authorized investigation be conducted in accordance with guidelines approved by the Attorney General, and those guidelines allow the FBI to conduct an investigation into a foreign terrorist entity if there is an "articulable factual basis…that reasonably indicates that the [entity] may have engaged in… international terrorism or other threat to the national security," or may be planning or supporting such conduct. In other words, we can investigate an organization, not merely an individual or a particular act, if there is a factual basis to believe the organization is involved in terrorism. And in this case, the Government's applications to collect the telephony metadata have identified the particular terrorist entities that are the subject of the investigations.

Second, the standard of "relevance" required by this statute is not the standard that we think of in a civil or criminal trial under the rules of evidence. The courts have recognized in other contexts that "relevance" can be an extremely broad standard. For example, in the grand jury context, the Supreme Court has held that a grand jury subpoena is proper unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation." And in civil discovery, relevance is "construed broadly to encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case."

In each of these contexts, the meaning of "relevance" is sufficiently broad to allow for subpoenas or requests that encompass large volumes of records in order to locate within them a smaller subset of material that will be directly pertinent to or actually be used in furtherance of the investigation or proceedings. In other words, the requester is not limited to obtaining only those records that actually are potentially incriminating or pertinent to establishing liability, because to identify such records, it is often necessary to collect a much broader set of the records that might potentially bear fruit by leading to specific material that could bear on the issue.

When it passed the business records provision, Congress made clear that it had in mind such broad concepts of relevance. The telephony metadata collection program meets this relevance standard because, as I explained earlier, the effectiveness of the queries allowed under the strict limitations imposed by the court—the queries based on "reasonable and articulable suspicion"—depends on collecting and maintaining the data from which the narrowly focused queries can be made. As in the grand jury and civil discovery contexts, the concept of "relevance" is broad enough to allow for the collection of information beyond that which ultimately turns out to be important to a terrorist-related investigation. While the scope of the collection at issue here is broader than typically might be acquired through a grand jury subpoena or civil discovery request, the basic principle is similar: the information is relevant because you need to have the broader set of records in order to identify within them the information that is actually important to a terrorism investigation. And the reasonableness of this method of collection is reinforced by all of the stringent limitations imposed by the Court to ensure that the data is used only for the approved purpose.

I want to repeat that the conclusion that the bulk metadata collection is authorized under Section 215 is not that of the Intelligence Community alone. Applications to obtain this data have been repeatedly approved by numerous judges of the FISA Court, each of whom has determined that the application complies with all legal requirements. And Congress reauthorized Section 215 in 2011, after the Intelligence and Judiciary Committees of

both Houses had been briefed on the program, and after information describing the program had been made available to all Members. In short, all three branches of Government have determined that this collection is lawful and reasonable—in large part because of the substantial protections we provide for the privacy of every person whose telephone number is collected.

The third program I want to talk about is Section 702, part of the FISA Amendments Act of 2008. Again, a little history is in order. Generally speaking, as I said before, Title I of FISA, or traditional FISA, governs electronic surveillance conducted within the United States for foreign intelligence purposes. When FISA was first passed in 1978, Congress did not intend it to regulate the targeting of foreigners outside of the United States for foreign intelligence purposes.

This kind of surveillance was generally carved out of coverage under FISA by the way Congress defined "electronic surveillance." Most international communications in 1978 took place via satellite, so Congress excluded international radio communications from the definition of electronic surveillance covered by FISA, even when the radio waves were intercepted in the United States, unless the target of the collection was a U.S. person in the United States.

Over time, that technology-based differentiation fell apart. By the early twenty-first century, most international communications travelled over fiber optic cables and thus were no longer "radio communications" outside of FISA's reach. At the same time there was a dramatic increase in the use of the Internet for communications purposes, including by terrorists. As a result, Congress original intention was frustrated; we were increasingly forced to go to the FISA Court to get individual warrants to conduct electronic surveillance of foreigners overseas for foreign intelligence purposes.

After 9/11, this burden began to degrade our ability to collect the communications of foreign terrorists. Section 702 created a new, more streamlined procedure to accomplish this surveillance. So Section 702 was not, as some have called it, a "defanging" of the FISA Court's traditional authority. Rather, it extended the FISA Court's oversight to a kind of surveillance that Congress had originally placed outside of that oversight: the surveillance, for foreign intelligence purposes, of foreigners overseas. This American regime imposing judicial supervision of a kind of foreign intelligence collection directed at citizens of other countries is a unique limitation that, so far as I am aware, goes beyond what other countries require of their intelligence services when they collect against persons who are not their own citizens.

The privacy and constitutional interests implicated by this program fall between traditional FISA and metadata collection. On the one hand we are collecting the full content of communications; on the other hand we are not collecting information in bulk and we are only targeting non-U.S. persons for valid foreign intelligence purposes. And the information involved is unquestionably of great importance for national security: collection under Section 702 is one of the most valuable sources of foreign intelligence we have. Again, the statutory scheme, and the means by which we implement it, are designed to allow us to collect this intelligence, while providing appropriate protections for privacy. Collection under Section 702 does not require individual judicial orders authorizing collection against each target. Instead, the FISA Court approves annual certifications submitted by the Attorney General and the Director of National Intelligence that identify categories of foreign intelligence that may be collected, subject to Court-approved "targeting" procedures and "minimization" procedures.

The targeting procedures are designed to ensure that we target someone only if we have a valid foreign intelligence purpose; that we target only non-U.S. persons reasonably believed to be outside of the United States; that we do not intercept wholly domestic communications; and that we do not target any person outside the United States as a "back door" means of targeting someone inside the United States. The procedures must be reviewed by the Court to ensure that they are consistent with the statute and the Fourth Amendment. In other words, the targeting procedures are a way of minimizing the privacy impact of this collection both as to Americans and as to non-Americans by limiting the collection to its intended purpose.

The concept of minimization procedures should be familiar to you by now: they are the procedures that limit the retention and dissemination of information about U.S. persons. We may incidentally acquire the communications of Americans even though we are not targeting them, for example if they talk to non-U.S. persons outside of the United States who are properly targeted for foreign intelligence collection. Some of these

communications may be pertinent; some may not be. But the incidental acquisition of non-pertinent information is not unique to Section 702. It is common whenever you lawfully collect information, whether it's by a criminal wiretap (where the target's conversations with his friends or family may be intercepted) or when we seize a terrorist's computer or address book, either of which is likely to contain non-pertinent information. In passing Section 702, Congress recognized this reality and required us to establish procedures to minimize the impact of this incidental collection on privacy.

How does Section 702 work in practice? As of today, there are certifications for several different categories of foreign intelligence information. Let's say that the Intelligence Community gets information that a terrorist is using a particular email address. NSA analysts look at available data to assess whether that email address would be a valid target under the statute—whether the email address belongs to someone who is not a U.S. person, whether the person with the email address is outside the United States, and whether targeting that email address is likely to lead to the collection of foreign intelligence relevant to one of the certifications. Only if all three requirements of the statute are met, and validated by supervisors, will the email address be approved for targeting. We don't randomly target email addresses or collect all foreign individuals' emails under Section 702; we target specific accounts because we are looking for foreign intelligence information. And even after a target is approved, the court approved procedures require NSA to continue to verify that its targeting decision is valid based on any new information.

Any communications that we collect under Section 702 are placed in secure databases, again with limited access. Trained analysts are allowed to use this data for legitimate foreign intelligence purposes, but the minimization procedures require that if they review a communication that they determine involves a U.S. person or information about a U.S. person, and they further determine that it has no intelligence value and is not evidence of a crime, it must be destroyed. In any case, conversations that are not relevant are destroyed after a maximum of five years. So under Section 702, we have a regime that involves judicial approval of procedures that are designed to narrow the focus of the surveillance and limit its impact on privacy. I've outlined three different collection programs, under different provisions of FISA, which all reflect the framework I described. In each case, we protect privacy by a multi-layered system of controls on what we collect and how we use what we collect, controls that are based on the nature and intrusiveness of the collection, but that take into account the ways in which that collection can be useful to protect national security. But we don't simply set out a bunch of rules and trust people to follow them. There are substantial safeguards in place that help ensure that the rules are followed.

These safeguards operate at several levels. The first is technological. The same technological revolution that has enabled this kind of intelligence collection and made it so valuable also allows us to place relatively stringent controls on it. For one thing, intelligence agencies can work with providers so that they provide the information we are allowed to acquire under the relevant order, and not additional information. Second, we have secure databases to hold this data, to which only trained personnel have access. Finally, modern information security techniques allow us to create an audit trail tracking who uses these databases and how, so that we have a record that can enable us to identify any possible misuse. And I want to emphasize that there's no indication so far that anyone has defeated those technological controls and improperly gained access to the databases containing people's communications. Documents such as the leaked secondary order are kept on other NSA databases that do not contain this kind of information, to which many more NSA personnel have access.

We don't rely solely on technology. NSA has an internal compliance officer, whose job includes developing processes that all NSA personnel must follow to ensure that NSA is complying with the law. In addition, decisions about what telephone numbers we use as a basis for searching the telephone metadata are reviewed first within NSA, and then by the Department of Justice. Decisions about targeting under Section 702 are reviewed first within NSA, and then by the Department of Justice and by my agency, the Office of the Director of National Intelligence, which has a dedicated Civil Liberties Protection Officer who actively oversees these programs. For Title I collection, the Department of Justice regularly conducts reviews to ensure that information collected is used and disseminated in accordance with the court-approved minimization procedures. Finally, independent Inspectors General also review the operation of these programs. The point is not that these

individuals are perfect; it's that as you have more and more people from more and more organizations overseeing the operation of the programs, it becomes less and less likely that unintentional errors will go unnoticed or that anyone will be able to misuse the information.

But wait, there's more. In addition to this oversight by the Executive Branch, there is considerable oversight by both the FISA Court and the Congress. As I've said, the FISA Court has to review and approve the procedures by which we collect intelligence under FISA, to ensure that those procedures comply with the statute and the Fourth Amendment. In addition, any compliance matter, large or small, has to be reported to the Court. Improperly collected information generally must be deleted, subject only to some exceptions set out in the Court's orders, and corrective measures are taken and reported to the Court until it is satisfied.

And I want to correct the erroneous claim that the FISA Court is a rubber stamp. Some people assume that because the FISA Court approves almost every application, it does not give these applications careful scrutiny. In fact the exact opposite is true. The judges and their professional staff review every application carefully, and often ask extensive and probing questions, seek additional information, or request changes, before the application is ultimately approved. Yes, the Court approves the great majority of applications at the end of this process, but before it does so, its questions and comments ensure that the application complies with the law.

Finally, there is the Congress. By law, we are required to keep the Intelligence and Judiciary Committees informed about these programs, including detailed reports about their operation and compliance matters. We regularly engage with them and discuss these authorities, as we did this week, to provide them information to further their oversight responsibilities. For example, when Congress reauthorized Section 215 in 2009 and 2011 and Section 702 in 2012, information was made available to every member of Congress, by briefings and written material, describing these programs in detail.

In short, the procedures by which we implement collection under FISA are a sensible means of accounting for the changing nature of privacy in the information age. They allow the Intelligence Community to collect information that is important to protect our Nation and its allies, while protecting privacy by imposing appropriate limits on the use of that information. Much is collected, but access, analysis and dissemination are subject to stringent controls and oversight. This same approach—making the extent and nature of controls over the use of information vary depending on the nature and sensitivity of the collection—is applied throughout our intelligence collection.

And make no mistake, our intelligence collection has helped to protect our Nation from a variety of threats—and not only our Nation, but the rest of the world. We have robust intelligence relationships with many other countries. These relationships go in both directions, but it is important to understand that we cannot use foreign intelligence to get around the limitations in our laws, and we assume that our other countries similarly expect their intelligence services to operate in compliance with their own laws. By working closely with other countries, we have helped ensure our common security. For example, while many of the details remain classified, we have provided the Congress a list of fifty-four cases in which the bulk metadata and Section 702 authorities have given us information that helped us understand potential terrorist activity and even disrupt it, from potential bomb attacks to material support for foreign terrorist organizations. Forty-one of these cases involved threats in other countries, including twenty-five in Europe. We were able to alert officials in these countries to these events, and help them fulfill their mission of protecting their nations, because of these capabilities.

I believe that our approach to achieving both security and privacy is effective and appropriate. It has been reviewed and approved by all three branches of Government as consistent with the law and the Constitution. It is not the only way we could regulate intelligence collection, however. Even before the recent disclosures, the President said that we welcomed a discussion about privacy and national security, and we are working to declassify more information about our activities to inform that discussion. In addition, the Privacy and Civil Liberties Oversight Board—an independent body charged by law with overseeing our counterterrorism activities—has announced that it intends to provide the President and Congress a public report on the Section 215 and 702 programs, including the collection of bulk metadata. The Board met recently with the President, who welcomed their review and committed to providing them access to

all materials they will need to fulfill their oversight and advisory functions. We look forward to working with the Board on this important project.

This discussion can, and should, have taken place without the recent disclosures, which have brought into public view the details of sensitive operations that were previously discussed on a classified basis with the Congress and in particular with the committees that were set up precisely to oversee intelligence operations. The level of detail in the current public debate certainly reflects a departure from the historic understanding that the sensitive nature of intelligence operations demanded a more limited discussion. Whether or not the value of the exposure of these details outweighs the cost to national security is now a moot point. As the debate about our surveillance programs goes forward, I hope that my remarks today have helped provide an appreciation of the efforts that have been made—and will continue to be made—to ensure that our intelligence activities comply with our laws and reflect our values.

Thank you.

Remarks prepared for delivery by Senator Ron Wyden to the Center for American Progress Event on National Security Agency Surveillance, Washington, DC

(July 23, 2013)

Source: Office of Senator Ron Wyden

Thank you for having me this morning. The Center for American Progress and the noted privacy hawk John Podesta have long been pursuing thoughtful intelligence policy. Since opening your doors in 2003 you have been making the case that security and liberty are not mutually exclusive, and your work is well known in my office and throughout Washington.

When the Patriot Act was last reauthorized, I stood on the floor of the United States Senate and said, "I want to deliver a warning this afternoon. When the American people find out how their government has interpreted the Patriot Act, they are going to be stunned and they are going to be angry." From my position on the Senate Intelligence Committee, I had seen government activities conducted under the umbrella of the Patriot Act that I knew would astonish most Americans.

At the time, Senate rules about classified information barred me from giving any specifics of what I'd seen except to describe it as Secret Law, a secret interpretation of the Patriot Act, issued by a secret court, that authorizes secret surveillance programs that I and colleagues think go far beyond the intent of the statute.

If that is not enough to give you pause, then consider that not only were the existence of and the legal justification for these programs kept completely secret from the American people; senior officials from across the government were making statements to the public about domestic surveillance that were clearly misleading and at times simply false. Senator Mark Udall and I tried again and again to get the executive branch to be straight with the public, but under the classification rules observed by the Senate we are not even allowed to tap the truth out in Morse code and we tried just about everything else we could think of to warn the American people.

But as I've said before, one way or another the truth always wins out. Last month, disclosures made by an NSA contractor lit the surveillance world on fire. Several provisions of secret law were no longer secret and the American people were finally able to see some of the things I've been raising the alarm about for years. And when they did, boy were they stunned, and boy are they angry.

You hear it in the lunchrooms, town hall meetings and senior citizen centers. The latest polling, the well-respected Quinnipiac poll, found that a plurality of people said the government is overreaching and encroaching too much on Americans' civil liberties. That's a huge swing from what that same survey said just a couple years ago, and that number is trending upward. As more information about sweeping government surveillance of law-abiding Americans is made public and the American people can discuss its impacts, I believe more Americans will speak out. They're going to say, in America, you don't have to settle for one priority or the other: laws can be written to protect both privacy and security, and laws should never be secret.

After 9/11, when 3,000 Americans were murdered by terrorists, there was a consensus that our government needed to take decisive action. At a time of understandable panic, Congress gave the government new surveillance authorities, but attached an expiration date to these authorities so that they could be deliberated more carefully once the immediate emergency had passed. Yet in the decade since, that law has been extended several

times with no public discussion about how the law has actually been interpreted.

The result: the creation of an always expanding, omnipresent surveillance state that hour by hour chips needlessly away at the liberties and freedoms our Founders established for us, without the benefit of actually making us any safer.

So, today I'm going to deliver another warning: If we do not seize this unique moment in our constitutional history to reform our surveillance laws and practices, we will all live to regret it. I'll have more to say about the consequences of the omnipresent surveillance state, but as you listen to this talk, ponder that most of us have a computer in our pocket that potentially can be used to track and monitor us 24/7.

The combination of increasingly advanced technology with a breakdown in the checks and balances that limit government action could lead us to a surveillance state that cannot be reversed.

At this point, a little bit of history might be helpful. I joined the Senate Intelligence Committee in January 2001, just before 9/11. Like most senators I voted for the original Patriot Act, in part, because I was reassured that it had an expiration date that would force Congress to come back and consider these authorities more carefully when the immediate crisis had passed. As time went on, from my view on the Intelligence Committee there were developments that seemed farther and farther removed from the ideals of our Founding Fathers. This started not long after 9/11, with a Pentagon program called Total Information Awareness, which was essentially an effort to develop an ultra large scale domestic data mining system. Troubled by this effort, and its not- exactly modest logo of an all-seeing eye on the universe, I worked with a number of senators to shut it down. Unfortunately, this was hardly the last domestic surveillance overreach. In fact, the NSA's infamous warrantless wiretapping program was already up and running at that point, though I, and most members of the Intelligence Committee didn't learn about it until a few years later. This was part of a pattern of withholding information from Congress that persisted throughout the Bush administration. I joined the Intelligence Committee in 2001, but I learned about the warrantless wiretapping program when you read about it in the *New York Times* in late 2005.

The Bush administration spent most of 2006 attempting to defend the warrantless wiretapping program. Once again, when the truth came out, it produced a surge of public pressure and the Bush administration announced that they would submit to oversight from Congress and the Foreign Intelligence Surveillance Court, also known as the FISA Court.

Unfortunately, because the FISA Court's rulings are secret, most Americans had no idea that the Court was prepared to issue incredibly broad rulings, permitting the massive surveillance that finally made headlines last month.

It's now a matter of public record that the bulk phone records program has been operating since at least 2007. It's not a coincidence that a handful of senators have been working since then to find ways to alert the public about what has been going on. Months and years went into trying to find ways to raise public awareness about secret surveillance authorities within the confines of classification rules.

I and several of my colleagues have made it our mission to end the use of secret law.

When Oregonians hear the words secret law, they have come up to me and asked, "Ron, how can the law be secret? When you guys pass laws that's a public deal. I'm going to look them up online." In response, I tell Oregonians that there are effectively two Patriot Acts; the first is the one that they can read on their laptop in Medford or Portland, analyze and understand. Then there's the real Patriot Act; the secret interpretation of the law that the government is actually relying upon. The secret rulings of the Foreign Intelligence Surveillance Court have interpreted the Patriot Act, as well as section 702 of the FISA statute, in some surprising ways, and these rulings are kept entirely secret from the public. These rulings can be astoundingly broad. The one that authorizes the bulk collection of phone records is as broad as any I have ever seen.

This reliance of government agencies on a secret body of law has real consequences. Most Americans don't expect to know the details about ongoing sensitive military and intelligence activities, but as voters they absolutely have a need and a right to know what their government thinks it is permitted to do, so that they can ratify or reject decisions that elected officials make on their behalf. To put it another way, Americans recognize that intelligence agencies will sometimes need to conduct secret operations, but they don't think those agencies should be relying on secret law.

Now, some argue that keeping the meaning of surveillance laws secret is necessary, because it makes it easier to gather intelligence on terrorist groups and other foreign powers. If you follow this logic, when Congress passed the original Foreign Intelligence Surveillance Act back in the 1970s, they could have found a way to make the whole thing secret, so that Soviet agents wouldn't know what the FBI's surveillance authorities were. But that's not the way you do it in America.

It is a fundamental principle of American democracy that laws should not be public only when it is convenient for government officials to make them public. They should be public all the time, open to review by adversarial courts, and subject to change by an accountable legislature guided by an informed public. If Americans are not able to learn how their government is interpreting and executing the law then we have effectively eliminated the most important bulwark of our democracy. That's why, even at the height of the Cold War, when the argument for absolute secrecy was at its zenith, Congress chose to make US surveillance laws public.

Without public laws, and public court rulings interpreting those laws, it is impossible to have informed public debate. And when the American people are in the dark, they can't make fully informed decisions about who should represent them, or protest policies that they disagree with. These are fundamentals. It's Civics 101. And secret law violates those basic principles. It has no place in America.

Now let's turn to the secret court the Foreign Intelligence Surveillance Court, the one virtually no one had heard of two months ago and now the public asks me about at the barber.

When the FISA court was created as part of the 1978 FISA law its work was pretty routine. It was assigned to review government applications for wiretaps and decide whether the government was able to show probable cause. Sounds like the garden variety function of district court judges across America. In fact, their role was so much like a district court that the judges who make up the FISA Court are all current federal district court judges.

After 9/11, Congress passed the Patriot Act and the FISA Amendments Act. This gave the government broad new surveillance powers that didn't much resemble anything in either the criminal law enforcement world or the original FISA law. The FISA Court got the job of interpreting these new, unparalleled authorities of the Patriot Act and FISA Amendments Act. They chose to issue binding secret rulings that interpreted the law and the Constitution in the startling way that has come to light in the last six weeks. They were to issue the decision that the Patriot Act could be used for dragnet, bulk surveillance of law abiding Americans.

Outside the names of the FISA court judges, virtually everything else is secret about the court. Their rulings are secret, which makes challenging them in an appeals court almost impossible. Their proceedings are secret too, but I can tell you that they are almost always one sided. The government lawyers walk in and lay out an argument for why the government should be allowed to do something, and the Court decides based solely on the judge's assessment of the government's arguments.

That's not unusual if a court is considering a routine warrant request, but it's very unusual if a court is doing major legal or constitutional analysis. I know of absolutely no other court in this country that strays so far from the adversarial process that has been part of our system for centuries.

It may also surprise you to know that when President Obama came to office, his administration agreed with me that these rulings needed to be made public. In the summer of 2009 I received a written commitment from the Justice Department and the Office of the Director of National Intelligence that a process would be created to start redacting and declassifying FISA Court opinions, so that the American people could have some idea of what the government believes the law allows it to do. In the last four years exactly zero opinions have been released.

Now that we know a bit about secret law and the court that created it, let's talk about how it has diminished the rights of every American man, woman and child.

Despite the efforts of the intelligence community leadership to downplay the privacy impact of the Patriot Act collection, the bulk collection of phone records significantly impacts the privacy of millions of law abiding Americans. If you know who someone called, when they called, where they called from, and how long they talked, you lay bare the personal lives of law abiding Americans to the scrutiny of government bureaucrats and outside contractors.

This is particularly true if you're vacuuming up cell phone location data, essentially turning every American's cell phone into a tracking device. We are told this is not happening today, but

intelligence officials have told the press that they currently have the legal authority to collect Americans' location information in bulk.

Especially troubling is the fact that there is nothing in the Patriot Act that limits this sweeping bulk collection to phone records. The government can use the Patriot Act's business records authority to collect, collate and retain all sorts of sensitive information, including medical records, financial records, or credit card purchases. They could use this authority to develop a database of gun owners or readers of books and magazines deemed subversive. This means that the government's authority to collect information on law abiding American citizens is essentially limitless. If it is a record held by a business, membership organization, doctor, or school, or any other third party, it could be subject to bulk collection under the Patriot Act.

Authorities this broad give the national security bureaucracy the power to scrutinize the personal lives of every law abiding American. Allowing that to continue is a grave error that demonstrates a willful ignorance of human nature. Moreover, it demonstrates a complete disregard for the responsibilities entrusted to us by the Founding Fathers to maintain robust checks and balances on the power of any arm of the government.

That obviously raises some very serious questions. What happens to our government, our civil liberties and our basic democracy if the surveillance state is allowed to grow unchecked?

As we have seen in recent days, the intelligence leadership is determined to hold on to this authority. Merging the ability to conduct surveillance that reveals every aspect of a person's life with the ability to conjure up the legal authority to execute that surveillance, and finally, removing any accountable judicial oversight, creates the opportunity for unprecedented influence over our system of government.

Without additional protections in the law, every single one of us in this room may be and can be tracked and monitored anywhere we are at any time. The piece of technology we consider vital to the conduct of our everyday personal and professional life happens to be a combination phone bug, listening device, location tracker, and hidden camera. There isn't an American alive who would consent to being required to carry any one of those items and so we must reject the idea that the government may use its powers to arbitrarily bypass that consent.

Today, government officials are openly telling the press that they have the authority to effectively turn Americans' smart phones and cell phones into location-enabled homing beacons. Compounding the problem is the fact that the case law is unsettled on cell phone tracking and the leaders of the intelligence community have consistently been unwilling to state what the rights of law-abiding people are on this issue. Without adequate protections built into the law there's no way that Americans can ever be sure that the government isn't going to interpret its authorities more and more broadly, year after year, until the idea of a telescreen monitoring your every move turns from dystopia to reality.

Some would say that could never happen because there is secret oversight and secret courts that guard against it. But the fact of the matter is that senior policymakers and federal judges have deferred again and again to the intelligence agencies to decide what surveillance authorities they need. For those who believe executive branch officials will voluntarily interpret their surveillance authorities with restraint, I believe it is more likely that I will achieve my lifelong dream of playing in the NBA.

But seriously, when James Madison was attempting to persuade Americans that the Constitution contained sufficient protections against any politician or bureaucrat seizing more power than that granted to them by the people, he did not just ask his fellow Americans to trust him. He carefully laid out the protections contained in the Constitution and how the people could ensure they were not breached. We are failing our constituents, we are failing our founders, and we are failing every brave man and woman who fought to protect American democracy if we are willing, today, to just trust any individual or any agency with power greater than the checked and limited authority that serves as a firewall against tyranny.

Now I want to spend a few minutes talking about those who make up the intelligence community and day in and day out work to protect us all.

Let me be clear: I have found the men and women who work at our nation's intelligence agencies to be hardworking, dedicated professionals. They are genuine patriots who make real sacrifices to serve their country. They should be able to do their jobs secure in the knowledge that there is public support for everything that they are doing. Unfortunately, that can't happen when senior officials from across the government

mislead the public about the government's surveillance authorities.

And let's be clear: the public was not just kept in the dark about the Patriot Act and other secret authorities. The public was actively misled. I've pointed out several instances in the past where senior officials have made misleading statements to the public and to Congress about the types of surveillance they are conducting on the American people, and I'll recap some of the most significant examples.

For years, senior Justice Department officials have told Congress and the public that the Patriot Act's business record authority which is the authority that is used to collect the phone records of millions of ordinary Americans is "analogous to a grand jury subpoena." This statement is exceptionally misleading it strains the word "analogous" well beyond the breaking point. It's certainly true that both authorities can be used to collect a wide variety of records, but the Patriot Act has been secretly interpreted to permit ongoing bulk collection, and this makes that authority very, very different from regular grand jury subpoena authority. Any lawyers in here? After the speech is over come up and tell me if you've ever seen a grand jury subpoena that allowed the government on an ongoing basis to collect the records of millions of ordinary Americans. The fact is that no one has seen a subpoena like that is because there aren't any. This incredibly misleading analogy has been made by more than one official on more than one occasion and often as part of testimony to Congress. The official who served for years as the Justice Department's top authority on criminal surveillance law recently told the Wall Street Journal that if a federal attorney "served a grand jury subpoena for such a broad class of records in a criminal investigation, he or she would be laughed out of court."

Defenders of this deception have said that members of Congress have the ability to get the full story of what the government is doing on a classified basis, so they shouldn't complain when officials make misleading public statements, even in congressional hearings. That is an absurd argument. Sure, members of Congress COULD get the full story in a classified setting, but that does not excuse the practice of half truths and misleading statements being made on the public record. When did it become all right for government officials' public statements and private statements to differ so fundamentally? The answer is that it is not all right, and it is indicative of a much larger culture of misinformation that goes beyond the congressional hearing room and into the public conversation writ large.

For example, last spring the Director of the National Security Agency spoke over at the American Enterprise Institute, where he said publicly that "we don't hold data on U.S. citizens." That statement sounds reassuring, but of course the American people now know that it is false. In fact, it's one of the most false statements ever made about domestic surveillance. Later that same year, at the annual hackers' conference known as DefCon, the same NSA Director said that the government does not collect "dossiers" on millions of Americans. Now I've served on the Intelligence Committee for a dozen years and I didn't know what "dossiers" meant in this context. I do know that Americans not familiar with the classified details would probably hear that statement and think that there was no bulk collection of the personal information of hundreds of millions of Americans taking place.

After the Director of the NSA made this statement in public, Senator Udall and I wrote to the Director asking for a clarification. In our letter we asked whether the NSA collects any type of data at all on millions or hundreds of millions of Americans. Even though the Director of the NSA was the one who had raised this issue publicly, intelligence officials declined to give us a straight answer.

A few months ago, I made the judgment that I would not be responsibly carrying out my oversight powers if I didn't press intelligence officials to clarify what the NSA Director told the public about data collection. So I decided it was necessary to put the question to the Director of National Intelligence. And I had my staff send the question over a day in advance so that he would be prepared to answer. The Director unfortunately said that the answer was no, the NSA does not knowingly collect data on millions of Americans, which is obviously not correct. After the hearing, I had my staff call the Director's office on a secure line and urge them to correct the record. Disappointingly, his office decided to let this inaccurate statement stand. My staff made it clear that this was wrong and that it was unacceptable to leave the American public misled. I continued to warn the public about the problem of secret surveillance law over the following weeks, until the June disclosures.

Even after those disclosures, there has been an effort by officials to exaggerate the effectiveness of the bulk phone records collection program by

conflating it with the collection of Internet communications under section 702 of the FISA statute. This collection, which involves the PRISM computer system, has produced some information of real value. I will note that last summer I was able to get the executive branch to declassify the fact that the FISA Court has ruled on at least one occasion that this collection violated the Fourth Amendment in a way that affected an undisclosed number of Americans. And the Court also said that the government has violated the spirit of the law as well. So, I think section 702 clearly needs stronger protections for the privacy of law-abiding Americans, and I think these protections could be added without losing the value of this collection. But I won't deny that this value exists. Meanwhile, I have not seen any indication that the bulk phone records program yielded any unique intelligence that was not also available to the government through less intrusive means. When government officials refer to these programs collectively, and say that "these programs" provided unique intelligence without pointing out that one program is doing all the work and the other is basically just along for the ride, in my judgment that is also a misleading statement.

And there have also been a number of misleading and inaccurate statements made about section 702 collection as well. Last month, Senator Udall and I wrote to the NSA Director to point out that the NSA's official fact sheet contained some misleading information and a significant inaccuracy that made protections for Americans' privacy sound much stronger than they actually are. The next day that fact sheet was taken down from the front page of the NSA website. Would the misleading fact sheet still be up there if Senator Udall and I hadn't pushed to take it down? Given what it took to correct the misleading statements of the Director of National Intelligence and the National Security Agency that may well be the case.

So having walked you through how secret law, interpreted by a secret court, authorized secret surveillance, the obvious question is what is next? "Ron, what are you going to do about it?"

A few weeks ago more than a quarter of the U.S. Senate wrote to the Director of National Intelligence demanding public answers to additional questions about the use of the government's surveillance authorities. It's been two months since the disclosures by Mr. Snowden, and the signers of this letter including key members of the senate leadership and committee chairs with decades of experience have made it clear they are not going to accept more stonewalling or misleading statements.

Patriot Act reform legislation has also been introduced. The centerpiece of this effort would require that the government show a demonstrated link to terrorism or espionage before collecting Americans' personal information.

Senators have also proposed legislation that would ensure that the legal analysis of secret court opinions interpreting surveillance law is declassified in a responsible manner. And I am collaborating with colleagues to develop other reforms that will bring openness, accountability, and the benefits of an adversarial process to the anachronistic operations of the most secretive court in America.

And most importantly, I and my colleagues are working to keep the public debate alive. We have exposed misleading statements. We are holding officials accountable. And we are showing that liberty and security are not incompatible.

The fact is, the side of transparency and openness is starting to put some points on the board.

As many of you are now aware, the NSA also had a bulk email records program that was similar to the bulk phone records program. This program operated under section 214 of the Patriot Act, which is known as the "pen register" provision, until fairly recently. My Intelligence Committee colleague Senator Udall and I were very concerned about this program's impact on Americans' civil liberties and privacy rights, and we spent a significant portion of 2011 pressing intelligence officials to provide evidence of its effectiveness. It turned out that they were unable to do so, and that statements that had been made about this program to both Congress and the FISA Court had significantly exaggerated the program's effectiveness. The program was shut down that same year. So that was a big win for everyone who cares about Americans' privacy and civil liberties, even though Senator Udall and I weren't able to tell anyone about it until just a few weeks ago.

More recently, when the annual Intelligence Authorization bill was going through the Intelligence Committee late last year it included a few provisions that were meant to stop intelligence leaks but that would have been disastrous to the news media's ability to report on foreign policy and national security. Among other things, it would have restricted the ability of former government officials to talk to the press, even about unclassified foreign policy matters. And it would

have prohibited intelligence agencies from making anyone outside of a few high-level officials available for background briefings, even on unclassified matters. These provisions were intended to stop leaks, but it's clear to me that they would have significantly encroached upon the First Amendment, and led to a less informed public debate on foreign policy and national security matters.

These anti-leaks provisions went through the committee process in secret, and the bill was agreed to by a vote of 141 (I'll let you all guess who that nay vote was). The bill then made its way to the Senate floor and a public debate. Once the bill became public, of course, it was promptly eviscerated by media and free speech advocates, who saw it as a terrible idea. I put a hold on the bill so that it could not be quickly passed without the discussion it deserved and within weeks, all of the anti-leaks provisions were removed.

A few months later, my colleagues and I were finally able to get the official Justice Department opinions laying out what the government believes the rules are for the targeted killings of Americans. You probably know this as the "drones" issue. These documents on killing Americans weren't even being shared with members of Congress on a classified basis, let alone with the American people. You may have heard me say this before, but I believe every American has the right to know when their government thinks it is allowed to kill them. My colleagues and I fought publicly and privately to get these documents, used whatever procedural opportunities were available, and eventually got the documents we had demanded. Since then we've been looking them over and working out a strategy that would allow for the pertinent portions of these documents to be made public. I don't take a backseat to anybody when it comes to protecting genuinely sensitive national security information, and I think most Americans expect that government agencies will sometimes conduct secret operations. But those agencies should never rely on secret law or authorities granted by secret courts.

We find ourselves at a truly unique time in our Constitutional history. The growth of digital technology, dramatic changes in the nature of warfare and the definition of a battlefield, and novel courts that run counter to everything the Founding Fathers imagined, make for a combustible mix. At this point in the speech I would usually conclude with the quote from Ben Franklin about giving up liberty for security and not deserving either, but I thought a different Founding Father might be more fitting today. James Madison, the father of our constitution, said that the accumulation of executive, judicial and legislative powers in the hands of any faction is the very definition of tyranny. He then went on to assure the nation that the Constitution protected us from that fate. So, my question to you is: by allowing the executive to secretly follow a secret interpretation of the law under the supervision of a secret, non-adversarial court and occasional secret congressional hearings, how close are we coming to James Madison's "very definition of tyranny"? I believe we are allowing our country to drift a lot closer than we should, and if we don't take this opportunity to change course now, we will all live to regret it.

Remarks by President Barack Obama in a Press Conference on National Security Agency Surveillance, Washington, DC

(August 9, 2013)
Source: The White House

Over the past few weeks, I've been talking about what I believe should be our number-one priority as a country—building a better bargain for the middle class and for Americans who want to work their way into the middle class. At the same time, I'm focused on my number-one responsibility as Commander-in-Chief, and that's keeping the American people safe. And in recent days, we've been reminded once again about the threats to our nation.

As I said at the National Defense University back in May, in meeting those threats we have to strike the right balance between protecting our security and preserving our freedoms. And as part of this rebalancing, I called for a review of our surveillance programs. Unfortunately, rather than an orderly and lawful process to debate these issues and come up with appropriate reforms, repeated leaks of classified information have initiated the debate in a very passionate, but not always fully informed way.

Now, keep in mind that as a senator, I expressed a healthy skepticism about these programs, and as President, I've taken steps to make sure they have strong oversight by all three branches of government and clear safeguards to prevent abuse and protect the rights of the American people. But given the history of abuse by governments, it's right to ask questions about surveillance—particularly as technology is reshaping every aspect of our lives.

I'm also mindful of how these issues are viewed overseas, because American leadership around the world depends upon the example of American democracy and American openness—because what makes us different from other countries is not simply our ability to secure our nation, it's the way we do it—with open debate and democratic process.

In other words, it's not enough for me, as President, to have confidence in these programs. The American people need to have confidence in them as well. And that's why, over the last few weeks, I've consulted members of Congress who come at this issue from many different perspectives. I've asked the Privacy and Civil Liberties Oversight Board to review where our counterterrorism efforts and our values come into tension, and I directed my national security team to be more transparent and to pursue reforms of our laws and practices.

And so, today, I'd like to discuss four specific steps—not all inclusive, but some specific steps that we're going to be taking very shortly to move the debate forward.

First, I will work with Congress to pursue appropriate reforms to Section 215 of the Patriot Act—the program that collects telephone records. As I've said, this program is an important tool in our effort to disrupt terrorist plots. And it does not allow the government to listen to any phone calls without a warrant. But given the scale of this program, I understand the concerns of those who would worry that it could be subject to abuse. So after having a dialogue with members of Congress and civil libertarians, I believe that there are steps we can take to give the American people additional confidence that there are additional safeguards against abuse.

For instance, we can take steps to put in place greater oversight, greater transparency, and constraints on the use of this authority. So I look forward to working with Congress to meet those objectives.

Second, I'll work with Congress to improve the public's confidence in the oversight conducted by the Foreign Intelligence Surveillance Court, known as the FISC. The FISC was created by Congress to provide judicial review of certain intelligence activities so that a federal judge must find that our actions are consistent with the Constitution. However, to build greater confidence, I think we should consider some additional changes to the FISC.

One of the concerns that people raise is that a judge reviewing a request from the government to conduct programmatic surveillance only hears one side of the story—may tilt it too far in favor of security, may not pay enough attention to liberty. And while I've got confidence in the court and I think they've done a fine job, I think we can provide greater assurances that the court is looking at these issues from both perspectives—security and privacy.

So, specifically, we can take steps to make sure civil liberties concerns have an independent voice in appropriate cases by ensuring that the government's position is challenged by an adversary.

Number three, we can, and must, be more transparent. So I've directed the intelligence community to make public as much information about these programs as possible. We've already declassified unprecedented information about the NSA, but we can go further. So at my direction, the Department of Justice will make public the legal rationale for the government's collection activities under Section 215 of the Patriot Act. The NSA is taking steps to put in place a full-time civil liberties and privacy officer, and released information that details its mission, authorities, and oversight. And finally, the intelligence community is creating a website that will serve as a hub for further transparency, and this will give Americans and the world the ability to learn more about what our intelligence community does and what it doesn't do, how it carries out its mission, and why it does so.

Fourth, we're forming a high-level group of outside experts to review our entire intelligence and communications technologies. We need new thinking for a new era. We now have to unravel terrorist plots by finding a needle in the haystack of global telecommunications. And meanwhile, technology has given governments—including our own—unprecedented capability to monitor communications.

So I am tasking this independent group to step back and review our capabilities—particularly our surveillance technologies. And they'll consider how we can maintain the trust of the people, how we can make sure that there absolutely is no abuse in terms of how these surveillance technologies are used, ask how surveillance impacts our foreign policy—particularly in an age when more and more information is becoming public. And they will provide an interim report in sixty days and a final report by the end of this year, so that we can move forward with a better understanding of how these programs impact our security, our privacy and our foreign policy.

So all these steps are designed to ensure that the American people can trust that our efforts are in line with our interests and our values. And to others around the world, I want to make clear once again that America is not interested in spying on ordinary people. Our intelligence is focused, above all, on finding the information that's necessary to protect our people, and—in many cases—protect our allies.

It's true we have significant capabilities. What's also true is we show a restraint that many governments around the world don't even think to do, refuse to show—and that includes, by the way, some of America's most vocal critics. We shouldn't forget the difference between the ability of our government to collect information online under strict guidelines and for narrow purposes, and the willingness of some other governments to throw their own citizens in prison for what they say online.

And let me close with one additional thought. The men and women of our intelligence community work every single day to keep us safe because they love this country and believe in our values. They're patriots. And I believe that those who have lawfully raised their voices on behalf of privacy and civil liberties are also patriots who love our country and want it to live up to our highest ideals. So this is how we're going to resolve our differences in the United States—through vigorous public debate, guided by our Constitution, with reverence for our history as a nation of laws, and with respect for the facts.

Statement by the National Security Agency on Missions, Authorities, Oversight and Partnerships, Washington, DC

(August 9, 2013)
Source: National Security Agency

"That's why, in the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are. That means reviewing the authorities of law enforcement, so we can intercept new types of communication, but also build in privacy protections to prevent abuse."
—President Obama, May 23, 2013

In his May 2013 address at the National Defense University, the President made clear that we, as a Government, need to review the surveillance authorities used by our law enforcement and intelligence community professionals so that we can collect information needed to keep us safe and ensure that we are undertaking the right kinds of privacy protections to prevent abuse. In the wake of recent unauthorized disclosures about some of our key intelligence collection programs, President Obama has directed that as much information as possible be made public, while mindful of the need to protect sources, methods and national security. Acting under the guidance, the Administration has provided enhanced transparency on, and engaged in robust public discussion about, key intelligence collection programs undertaken by the National Security Agency (NSA). This is important not only to foster the kind of debate the President has called for, but to correct inaccuracies that have appeared in the media and elsewhere. This document is a step in that process, and is aimed at providing a succinct description of NSA's mission, authorities, oversight and partnerships.

Prologue

After the al-Qa'ida attacks on the World Trade Center and the Pentagon, the 9/11 Commission found that the U.S. Government had failed to identify and connect the many "dots" of information that would have uncovered the planning and preparation for those attacks. We now know that 9/11 hijacker Khalid al-Midhar, who was on board American Airlines flight 77 that crashed into the Pentagon, resided in California for the first six months of 2000. While NSA had intercepted some of Midhar's conversations with persons in an al-Qa'ida safe house in Yemen during that period, NSA did not have the U.S. phone number or any indication that the phone Midhar was using was located in San Diego. NSA did not have the tools or the database to search to identify these connections and share them with the FBI. Several programs were developed to address the U.S. Government's need to connect the dots of information available to the intelligence community and to strengthen the coordination between foreign intelligence and domestic law enforcement agencies.

Background

NSA is an element of the U.S. intelligence community charged with collecting and reporting intelligence for foreign intelligence and counterintelligence purposes. NSA performs this mission by engaging in the collection of "signals intelligence," which, quite literally, is the production of foreign

intelligence through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire, or other electromagnetic means. Every intelligence activity NSA undertakes is necessarily constrained to these central foreign intelligence and counterintelligence purposes. NSA's challenge in an increasingly interconnected world—a world where our adversaries make use of the same communications systems and services as Americans and our allies—is to find and report on the communications of foreign intelligence value while respecting privacy and civil liberties. We do not need to sacrifice civil liberties for the sake of national security—both are integral to who we are as Americans. NSA can and will continue to conduct its operations in a manner that respects both. We strive to achieve this through a system that is carefully designed to be consistent with *authorities* and *controls* and enabled by capabilities that allow us to *collect, analyze* and *report* intelligence needed to protect national security.

NSA Mission

NSA's mission is to help protect national security by providing policy makers and military commanders with the intelligence information they need to do their jobs. NSA's priorities are driven by externally developed and validated intelligence requirements, provided to NSA by the President, his national security team, and their staffs through the National Intelligence Priorities Framework.

NSA Collection Authorities

NSA's collection authorities stem from two key sources: Executive Order 12333 and the Foreign Intelligence Surveillance Act of 1978 (FISA).

Executive Order 12333

Executive Order 12333 is the foundational authority by which NSA collects, retains, analyzes and disseminates foreign signals intelligence information. The principal application of this authority is the collection of communications by foreign persons that occur wholly outside the United States. To the extent a person located outside the United States communicates with someone inside the United States or someone inside the United States communicates with a person located outside the United States those communications could also be collected. Collection pursuant to EO 12333 is conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA. Intelligence activities conducted under this authority are carried out in accordance with minimization procedures established by the Secretary of Defense and approved by the Attorney General.

To undertake collections authorized by EO 12333, NSA uses a variety of methodologies. Regardless of the specific authority or collection source, NSA applies the process described below:

1. NSA identifies foreign entities (persons or organizations) that have information responsive to an identified foreign intelligence requirement. For instance, NSA works to identify individuals who may belong to a terrorist network.
2. NSA develops the "network" with which that person or organization's information is shared or the command and control structure through which it flows. In other words, if NSA is tracking a specific terrorist, NSA will endeavor to determine who that person is in contact with, and who he is taking direction from.
3. NSA identifies how the foreign entities communicate (radio, email, telephony, etc.)
4. NSA then identifies the telecommunications infrastructure used to transmit those communications.
5. NSA identifies vulnerabilities in the methods of communication used to transmit them.
6. NSA matches its collection to those vulnerabilities, or develops new capabilities to acquire communications of interest if needed.

This process will often involve the collection of communications metadata—data that helps NSA understand where to find valid foreign intelligence information needed to protect U.S. national security interests in a large and complicated global network. For instance, the collection of overseas communications metadata associated with telephone calls—such as the telephone numbers, and time and duration of calls—allows NSA to map communications between terrorists and their associates. This strategy helps ensure that NSA's collection of communications content is more precisely focused on only those targets necessary to respond to identified foreign intelligence requirements.

NSA uses EO 12333 authority to collect foreign intelligence from communications systems around the world. Due to the fragility of these sources, providing any significant detail outside of classified channels is damaging to national security. Nonetheless, every type of collection undergoes a strict

oversight and compliance process internal to NSA that is conducted by entities within NSA other than those responsible for the actual collection.

FISA Collection

FISA regulates certain types of foreign intelligence collection including certain collection that occurs with compelled assistance from U.S. telecommunications companies. Given the techniques that NSA must employ when conducting NSA's foreign intelligence mission, NSA quite properly relies on FISA authorizations to acquire significant foreign intelligence information and will work with the FBI and other agencies to connect the dots between foreign-based actors and their activities in the U.S. The FISA Court plays an important role in helping to ensure that signals intelligence collection governed by FISA is conducted in conformity with the requirements of the statute. All three branches of the U.S. Government have responsibilities for programs conducted under FISA, and a key role of the FISA Court is to ensure that activities conducted pursuant to FISA authorizations are consistent with the statute, as well as the U.S. Constitution, including the Fourth Amendment.

FISA Section 702

Under Section 702 of the FISA, NSA is authorized to target non-U.S. persons who are reasonably believed to be located outside the United States. The principal application of this authority is in the collection of communications by foreign persons that utilize U.S. communications service providers. The United States is a principal hub in the world's telecommunications system and FISA is designed to allow the U.S. Government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans. In general, Section 702 authorizes the Attorney General and Director of National Intelligence to make and submit to the FISA Court written certifications for the purpose of acquiring foreign intelligence information. Upon the issuance of an order by the FISA Court approving such a certification and the use of targeting and minimization procedures, the Attorney General and Director of National Intelligence may jointly authorize for up to one year the targeting of non-United States persons reasonably believed to be located overseas to acquire foreign intelligence information. The collection is acquired through compelled assistance from relevant electronic communications service providers.

NSA provides specific identifiers (for example, email addresses, telephone numbers) used by non-U.S. persons overseas who the government believes possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification. Once approved, those identifiers are used to select communications for acquisition. Service providers are compelled to assist NSA in acquiring the communications associated with those identifiers.

For a variety of reasons, including technical ones, the communications of U.S. persons are sometimes incidentally acquired in targeting the foreign entities. For example, a U.S. person might be courtesy copied on an email to or from a legitimate foreign target, or a person in the U.S. might be in contact with a known terrorist target. In those cases, minimization procedures adopted by the Attorney General in consultation with the Director of National Intelligence and approved by the Foreign Intelligence Surveillance Court are used to protect the privacy of the U.S. person. These minimization procedures control the acquisition, retention and dissemination of any U.S. person information incidentally acquired during operations conducted pursuant to Section 702.

The collection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification and disruption of terrorist threats to the U.S. and around the world. One notable example is the Najibullah Zazi case. In early September 2009, while monitoring the activities of al Qaeda terrorists in Pakistan, NSA noted contact from an individual in the U.S. that the FBI subsequently identified as Colorado-based Najibullah Zazi. The U.S. Intelligence Community, including the FBI and NSA, worked in concert to determine his relationship with al Qaeda, as well as identify any foreign or domestic terrorist links. The FBI tracked Zazi as he traveled to New York to meet with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and his co-conspirators were subsequently arrested. Zazi pled guilty to conspiring to bomb the New York City subway system. The FAA Section 702 collection against foreign terrorists was critical to the discovery and disruption of this threat to the U.S.

FISA (Title I)

NSA relies on Title I of FISA to conduct electronic surveillance of foreign powers or their agents, to include members of international terrorist

organizations. Except for certain narrow exceptions specified in FISA, a specific court order from the Foreign Intelligence Surveillance Court based on a showing of probable cause is required for this type of collection.

Collection of U.S. Person Data

There are three additional FISA authorities that NSA relies on, after gaining court approval, that involve the acquisition of communications, or information about communications, of U.S. persons for foreign intelligence purposes on which additional focus is appropriate. These are the Business Records FISA provision in Section 501 (also known by its section numbering within the PATRIOT Act as Section 215) and Sections 704 and 705(b) of the FISA.

Business Records FISA, Section 215

Under NSA's Business Records FISA program (or BR FISA), first approved by the Foreign Intelligence Surveillance Court (FISC) in 2006 and subsequently reauthorized during two different Administrations, four different Congresses, and by fourteen federal judges, specified U.S. telecommunications providers are compelled by court order to provide NSA with information about telephone calls to, from, or within the U.S. The information is known as metadata, and consists of information such as the called and calling telephone numbers and the date, time, and duration of the call—but no user identification, content, or cell site locational data. The purpose of this particular collection is to identify the U.S. nexus of a foreign terrorist threat to the homeland.

The Government cannot conduct substantive queries of the bulk records for any purpose other than counterterrorism. Under the FISC orders authorizing the collection, authorized queries may only begin with an "identifier," such as a telephone number, that is associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court. An identifier used to commence a query of the data is referred to as a "seed." Specifically, under Court-approved rules applicable to the program, there must be a "reasonable, articulable suspicion" that a seed identifier used to query the data for foreign intelligence purposes is associated with a particular foreign terrorist organization. When the seed identifier is reasonably believed to be used by a U.S. person, the suspicion of an association with a particular foreign terrorist organization cannot be based solely on activities protected by the First Amendment. The "reasonable, articulable suspicion" requirement protects against the indiscriminate querying of the collected data. Technical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier.

The BR FISA program is used in cases where there is believed to be a threat to the homeland. Of the fifty-four terrorism events recently discussed in public, thirteen of them had a homeland nexus, and in twelve of those cases, BR FISA played a role. Every search into the BR FISA database is auditable and all three branches of our government exercise oversight over NSA's use of this authority.

FISA Sections 704 and 705(b)

FISA Section 704 authorizes the targeting of a U.S. person outside the U.S. for foreign intelligence purposes if there is probable cause to believe the U.S. person is a foreign power or is an officer, employee, or agent of a foreign power. This requires a specific, individual court order by the Foreign Intelligence Surveillance Court. The collection must be conducted using techniques not otherwise regulated by FISA.

Section 705(b) permits the Attorney General to approve similar collection against a U.S. person who is already the subject of a FISA court order obtained pursuant to Section 105 or 304 of FISA. The probable cause standard has, in these cases, already been met through the FISA court order process.

The Essential Role of Corporate Communications Providers

Under all FISA and FAA programs, the government compels one or more providers to assist NSA with the collection of information responsive to the foreign intelligence need. The government employs cover names to describe its collection by source. Some that have been revealed in the press recently include FAIRVIEW, BLARNEY, OAKSTAR, and LITHIUM. While some have tried to characterize the involvement of such providers as separate programs, that is not accurate. The role of providers compelled to provide assistance by the FISC is identified separately by the Government as a specific facet of the lawful collection activity.

The Essential Role of Foreign Partners

NSA partners with well over thirty different nations in order to conduct its foreign

intelligence mission. In every case, NSA does not and will not use a relationship with a foreign intelligence service to ask that service to do what NSA is itself prohibited by law from doing. These partnerships are an important part of the U.S. and allied defense against terrorists, cyber threat actors, and others who threaten our individual and collective security. Both parties to these relationships benefit.

One of the most successful sets of international partnerships for signals intelligence is the coalition that NSA developed to support U.S. and allied troops in Iraq and Afghanistan. The combined efforts of as many as fourteen nations provided signals intelligence support that saved U.S. and allied lives by helping to identify and neutralize extremist threats across the breadth of both battlefields. The senior U.S. commander in Iraq credited signals intelligence with being a prime reason for the significant progress made by U.S. troops in the 2008 surge, directly enabling the removal of almost 4,000 insurgents from the battlefield.

The Oversight and Compliance Framework

NSA has an internal oversight and compliance framework to provide assurance that NSA's activities—its people, its technology and its operations—act consistently with the law and with NSA and U.S. intelligence community policies and procedures. This framework is overseen by multiple organizations external to NSA, including the Director of National Intelligence, the Attorney General, the Congress, and for activities regulated by FISA, the Foreign Intelligence Surveillance Court.

NSA has had different minimization procedures for different types of collection for decades. Among other things, NSA's minimization procedures, to include procedures implemented by United States Signals Intelligence Directive No. SP0018 (USSID 18), provide detailed instructions to NSA personnel on how to handle incidentally acquired U.S. person information. The minimization procedures reflect the reality that U.S. communications flow over the same communications channels that foreign intelligence targets use, and that foreign intelligence targets often discuss information concerning U.S. persons, such as U.S. persons who may be the intended victims of a planned terrorist attack. Minimization procedures direct NSA on the proper way to treat information at all stages of the foreign intelligence process in order to protect U.S. persons' privacy interests.

In 2009 NSA stood up a formal Director of Compliance position, affirmed by Congress in the FY2010 Intelligence Authorization Bill, which monitors verifiable consistency with laws and policies designed to protect U.S. person information during the conduct of NSA's mission. The program managed by the Director of Compliance builds on a number of previous efforts at NSA, and leverages best practices from the professional compliance community in industry and elsewhere in the government. Compliance at NSA is overseen internally by the NSA Inspector General and is also overseen by a number of organizations external to NSA, including the Department of Justice, the Office of the Director of National Intelligence, and the Assistant Secretary of Defense for Intelligence Oversight, the Congress, and the Foreign Intelligence Surveillance Court.

In addition to NSA's compliance safeguards, NSA personnel are obliged to report when they believe NSA is not, or may not be, acting consistently with law, policy, or procedure. This self reporting is part of the culture and fabric of NSA. If NSA is not acting in accordance with law, policy, or procedure, NSA will report through its internal and external intelligence oversight channels, conduct reviews to understand the root cause, and make appropriate adjustments to constantly improve.

Extract of Speech by Brazilian President Dilma Rousseff to the 68th Session of the United National General Assembly, New York (September 24, 2013)

Source: Permanent Mission of Brazil to the United Nations

Ambassador John Ashe, president of the 68th session of the United Nations General Assembly, Mr. Ban Ki-moon, Secretary-General of the United Nations, Heads of State and Government, Ladies and Gentlemen.

Allow me initially to express my satisfaction in having a renowned representative of Antigua and Barbuda—a country that is part of the Caribbean, which is so cherished in Brazil and in our region—to conduct the work of this session of the General Assembly.

You can count, Excellency, on the permanent support of my Government.

Allow me also, at the beginning of my intervention, to express the repudiation of the Brazilian Government and people to the terrorist attack that

took place in Nairobi. I express our condolences and our solidarity to the families of the victims, the people and the Government of Kenya.

Terrorism, wherever it may occur and regardless of its origin, will always deserve our unequivocal condemnation and our firm resolve to fight against it. We will never give way to barbarity.

Mr. President, I would like to bring to the consideration of delegations a matter of great importance and gravity.

Recent revelations concerning the activities of a global network of electronic espionage have caused indignation and repudiation in public opinion around the world.

In Brazil, the situation was even more serious, as it emerged that we were targeted by this intrusion. Personal data of citizens was intercepted indiscriminately. Corporate information—often of high economic and even strategic value—was at the center of espionage activity. Also, Brazilian diplomatic missions, among them the Permanent Mission to the United Nations and the Office of the President of the Republic itself, had their communications intercepted.

Tampering in such a manner in the affairs of other countries is a breach of International Law and is an affront to the principles that must guide the relations among them, especially among friendly nations. A sovereign nation can never establish itself to the detriment of another sovereign nation. The right to safety of citizens of one country can never be guaranteed by violating fundamental human rights of citizens of another country. The arguments that the illegal interception of information and data aims at protecting nations against terrorism cannot be sustained.

Brazil, Mr. President, knows how to protect itself. We reject, fight and do not harbor terrorist groups.

We are a democratic country surrounded by nations that are democratic, pacific and respectful of International Law. We have lived in peace with our neighbors for more than 140 years.

As many other Latin Americans, I fought against authoritarianism and censorship, and I cannot but defend, in an uncompromising fashion, the right to privacy of individuals and the sovereignty of my country. In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy. In the absence of the respect for sovereignty, there is no basis for the relationship among Nations.

We face, Mr. President, a situation of grave violation of human rights and of civil liberties; of invasion and capture of confidential information concerning corporate activities, and especially of disrespect to national sovereignty.

We expressed to the Government of the United States our disapproval, and demanded explanations, apologies and guarantees that such procedures will never be repeated.

Friendly governments and societies that seek to build a true strategic partnership, as in our case, cannot allow recurring illegal actions to take place as if they were normal. They are unacceptable.

Brazil, Mr. President, will redouble its efforts to adopt legislation, technologies and mechanisms to protect us from the illegal interception of communications and data.

My Government will do everything within its reach to defend the human rights of all Brazilians and to protect the fruits borne from the ingenuity of our workers and our companies.

The problem, however, goes beyond a bilateral relationship. It affects the international community itself and demands a response from it. Information and telecommunication technologies cannot be the new battlefield between States. Time is ripe to create the conditions to prevent cyberspace from being used as a weapon of war, through espionage, sabotage, and attacks against systems and infrastructure of other countries.

The United Nations must play a leading role in the effort to regulate the conduct of States with regard to these technologies.

For this reason, Brazil will present proposals for the establishment of a civilian multilateral framework for the governance and use of the Internet and to ensure the effective protection of data that travels through the web.

We need to create multilateral mechanisms for the worldwide network that are capable of ensuring principles such as:

1. Freedom of expression, privacy of the individual and respect for human rights.
2. Open, multilateral and democratic governance, carried out with transparency by stimulating collective creativity and the participation of society, Governments and the private sector.
3. Universality that ensures the social and human development and the construction of inclusive and non-discriminatory societies.
4. Cultural diversity, without the imposition of beliefs, customs and values.
5. Neutrality of the network, guided only by

technical and ethical criteria, rendering it inadmissible to restrict it for political, commercial, religious or any other purposes.

Harnessing the full potential of the Internet requires, therefore, responsible regulation, which ensures at the same time freedom of expression, security and respect for human rights.

Opening Statement of General Keith B. Alexander, Director, National Security Agency, to the Senate Committee on the Judiciary, Washington, DC (October 2, 2013)

Source: United States Senate Committee on the Judiciary

Chairman Leahy, Ranking Member Grassley, distinguished members of the Committee, thank you for the opportunity to provide opening remarks.

I am privileged today to represent the work of the dedicated professionals at the National Security Agency who employ the authorities provided by Congress, the federal courts and the Executive Branch to help protect the nation and protect our civil liberties and privacy.

If we are to have an honest debate about how NSA conducts its business, we need to step away from sensationalized headlines and focus on facts.

Our mission is to defend the nation and to protect our civil liberties and privacy. Ben Wittes from the Brookings Institution said about the media leaks and specifically about these two FISA programs: "shameful as it is that these documents were leaked, they actually should give the public great confidence in both NSA's internal oversight mechanisms and in the executive and judicial oversight mechanisms outside the Agency. They show no evidence of any intentional spying on Americans or abuse of civil liberties. They show a low rate of the sort of errors any complex system of technical collection will inevitably yield. They show robust compliance procedures on the part of the NSA. And they show an earnest, ongoing dialogue with the FISA court over the parameters of the Agency's legal authority and a commitment both to keeping the court informed of activities and to complying with its judgments on their legality."

Today I'd like to present facts to specifically address:

—Who we are in terms of both our mission and our people;

—What we do: adapt to technology and the threat; take direction from political leadership; operate strictly within the law and consistent with explicit intelligence priorities; and ensure compliance with all constraints imposed by our authorities and internal procedures;

—What we have accomplished specifically for our country with the tools we have been authorized; and

—Where do we go from here?

Who We Are—Our Mission

NSA is a foreign intelligence agency with two missions:

—We collect foreign intelligence of national security interest and

—We protect certain sensitive information and U.S. networks.

—All this while protecting our civil liberties.

NSA contributes to the security of our nation, its armed forces, and our allies. NSA accomplishes this mission, while protecting civil liberties and privacy—because the constitution we are sworn to protect and defend makes no allowances to trade one for the other. NSA operates squarely within the authorities granted by the president, congress and the courts.

Who We Are—Our People

I'm proud of what NSA does and more proud of our people:

—National Security Agency employees take an oath to protect and defend the constitution of the United States of America.

—They have devoted themselves to protecting our nation.

—Just like you, they will never forget the moment terrorists killed 2,996 Americans in New York, Pennsylvania and the Pentagon.

—They witnessed the first responders' efforts to save lives. They saw the military shift to a wartime footing. They committed themselves to ensuring that another 9/11 would not happen and our deployed forces would return home safely.

—In fact, they deploy with our armed forces into areas of hostility. More than 6,000 deployed in support of operations in Iraq, Afghanistan and CT. Twenty-two paid the ultimate sacrifice since 9/11; sadly adding to a list of NSA/CSS personnel numbering over 170 killed in the line of duty since

NSA's formation in 1952. Theirs is a noble cause.
—NSA prides itself on its highly skilled workforce.
—We are the largest employer of mathematicians in the U.S. (1,013).
—966 PhDs and 4,374 computer scientists.
—Linguists in more than 120 languages.
—More patents than any other Intelligence Community agency and most businesses.
—They are also Americans and they take their privacy and civil liberties seriously.

What We Do—Adapt to Technology and the Threat

Today's telecommunications system is literally one of the most complex systems ever devised by mankind. The fact that over 2.5 billion people all connect and communicate across a common infrastructure is a tribute to the ingenuity of mankind. The stark reality is that terrorists, criminals and adversaries make use of the same infrastructure.

Terrorists and other foreign adversaries hide in the same global network, use the same communications networks as everyone else, and take advantage of familiar services: Gmail, Facebook, Twitter, etc. Technology has made it easy for them.

We must develop and apply the best analytic tools to succeed at our mission; finding the communications of adversaries while protecting those of innocent people, regardless of their nationality.

What We Do—Take Direction from Political Leadership (NIPF)

NSA's direction comes from national security needs, as defined by the nation's senior leaders.

NSA does not decide what topics to collect and analyze. NSA's collection and analysis is driven by the national intelligence priorities framework and received in formal tasking.

We do understand that electronic surveillance capabilities are powerful tools in the hands of the state. That's why we have extensive mandatory internal training, automated checks, and an extensive regime of both internal and external oversight.

What We Do—Use Lawful Programs and Tools to Do Our Mission

The authorities we have been granted and the capabilities we have developed help keep our nation safe. Since 9/11 we have disrupted terrorist attacks at home and abroad using capabilities informed by the lessons of 9/11. The Business Records FISA program, NSA's implementation of Section 215 of the PATRIOT Act, focuses on defending the homeland by linking the foreign and domestic threats.

Section 702 of FISA focuses on acquiring foreign intelligence, including critical information concerning international terrorist organizations, by targeting non-U.S. persons who are reasonably believed to be located outside the United States. NSA also operates under other sections of the FISA statute in accordance with the law's provisions (such as Title 1 and Section 704).

It is important to remember that in order to target a U.S. person anywhere in the world under the FISA statute, we are required to obtain a court order based on a probable cause showing that the prospective target of the surveillance is a foreign power or agent of a foreign power.

NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order (EO) 12333.

As I have said before, these authorities and capabilities are powerful; we take this responsibility seriously.

What We Do—Ensure Compliance

We stood up a Director of Compliance in 2009 and repeatedly train our entire workforce in privacy protections and the proper use of capabilities.

We do make mistakes. The vast majority of compliance incidents reflect the challenge of implementing very specific rules in the context of ever-changing technology. Compliance incidents, with very rare exception, are unintentional and reflect the sort of errors that will occur in any complex system of technical activity.

The press claimed evidence of "thousands of privacy violations." This is false and misleading. According to NSA's independent Inspector General, there have been only twelve substantiated cases of willful violation over ten years – essentially one per year from a population of NSA/CSS personnel numbering in the tens of thousands. But the relatively small number of cases does not excuse any infraction of the rules. We took action in every case referring several to the Department of Justice for potential prosecution; appropriate disciplinary action was taken in others.

We hold ourselves accountable every day. Most of these cases involved improper tasking or querying regarding foreign persons in foreign places. I am not aware of any intentional or willful violations of the FISA statute, which is designed to

be most protective of the privacy interests of U.S. persons. Of the 2,776 incidents noted in the press from one of our leaked annual compliance reports, about 75% are not violations of approved procedures at all but rather NSA's detection of valid foreign targets that travel to the U.S. and a record that NSA stopped collecting, in accordance with the rules (roamers).

Let me also start to clear the air on actual compliance incidents. The vast majority of the actual compliance incidents involve foreign locations and foreign activities, as our activities are regulated by specific rules wherever they occur. For the smaller number that did involve a U.S. person, a typical incident involves a person overseas involved with a foreign organization who is subsequently determined to be a U.S. person. All initial indications and research before collection point the other way, but NSA constantly re-evaluates indications.

NSA detects and corrects and—in most cases—does so before any information is even obtained, used, or shared outside of NSA. Despite the difference, between willful and not, we treat incidents the same: we detect, we address, we remediate—including removing or purging information from our databases in accordance with the rules. And we report. We hold ourselves accountable and keep others informed so they can do the same.

On NSA's compliance regime Ben Wittes said at last Thursday's Intelligence Committee hearing: "but one thing we have learned an enormous amount about is the compliance procedures that NSA uses. They are remarkable. They are detailed. They produce data streams that are extremely telling—and, to my mind, deeply reassuring."(September 26)

We welcome an ongoing discussion about how the public can, going forward, have increased information about NSA's compliance program and its compliance posture, much the same way all three branches of the government have today. From our perspective, additional measures that will increase the public's confidence in these authorities and our use of them can and should be open for discussion.

What We have Accomplished for Our Country

NSA's existing authorities and programs have helped "connect the dots," working with the broader Intelligence Community and homeland and domestic security organizations, for the good of the nation and its people.

NSA's programs have contributed to understanding and disrupting fifty-four terror related events: twenty-five in Europe, eleven in Asia, five in Africa, and thirteen related to the homeland. This was no accident nor coincidence. These were direct results of a dedicated workforce, appropriate policy, and well-scoped authorities created in the wake of 9/11 to make sure 9/11 never happened again.

This is not the case in other countries. In the week ending September 23 there were 972 terror-related deaths in Kenya, Pakistan, Afghanistan, Syria, Yemen and Iraq. [Kenya, 62; Pakistan, 75; Afghanistan, 18; Syria, 504; Yemen, 50; and Iraq, 263]. Another 1,030 were injured in the same countries.

We need these types of programs to protect against having these types of statistics on our soil. NSA's global system is optimized for today's technology on a global network. Our analytic tools are effective at finding terrorist communications in time to make a difference. This global system and analytic tools are also what we need for cybersecurity. This is how we see in cyberspace, identify threats there, and defend networks.

Reforms

On August 9 the President laid out some specific steps to increase the confidence of the American people in our foreign intelligence collection programs.

We are always looking for ways to better protect privacy and security. We have improved over time our ability to reconcile our technology with our operations and with the rules and authorities. We will continue to do so as we go forward and strive to improve how we protect the American people—their privacy and security.

Regarding NSA's telephone metadata program, policy makers across the Executive and Legislative Branches will ultimately decide whether we want to sustain or dispense with a tool designed to detect terrorist plots across the seam between foreign and domestic domains. Different implementations of the program can address the need, but each should be scored against several key attributes:

—Privacy: privacy and civil liberties are protected.
—Agility: queries can be made in a timely manner so that, in the most urgent cases, results can support disruption of imminent terrorist plots.
—Duration: terrorist planning can extend for years, so the metadata repository must extend back for some period of time in order to discover terrorist plans and disrupt plots.

—Breadth: repository of metadata is comprehensive enough to ensure query responses can indicate with high confidence any connections a terrorist-associated number may have to other persons who may be engaged in terrorist activities. As you consider changes in metadata storage location, length of storage, who approves query terms and the number of hops, we must preserve these foundational attributes of BR FISA.

Similarly as you entertain reforms to the FISC, operational and practical considerations must be weighed so that there are no inherent delays; emergency provisions are maintained; and any reform to the FISC structure is respectful of the nature of classified information.

Conclusion

NSA looks forward to supporting the discussion of reforms. Whatever changes are made, we will exercise our authorities dutifully, just as we have always done.

The leaks of classified NSA and partner information will change how we operate and what people know about us. However, the leaks will not change the ethos of the NSA workforce, which is dedicated to finding and reporting the vital intelligence our customers need to keep the nation safe, in a manner that is fully compliant with the laws and rules that authorize and limit NSA's activities and sustain the privacy protections that we as a nation enjoy.

I look forward to answering your questions.