The Heritage Foundation

BACKGROUNDER

UPDATED MAY 29, 2015 No. 3018 | MAY 21, 2015

Section 215 of the PATRIOT Act and Metadata Collection: Responsible Options for the Way Forward

James Jay Carafano, PhD, Charles D. Stimson, Steven P. Bucci, PhD, John G. Malcolm, and Paul Rosenzweig

Abstract

After the horrific attacks of September 11, 2001, the United States Congress passed the USA PATRIOT Act. Section 215 of the PATRIOT Act amended the Foreign Intelligence Surveillance Act of 1978 to allow U.S. intelligence to query telephone metadata. Section 215 expires at the end of May 2015, and policymakers are now faced with a daunting question: How do they protect Americans while respecting this nation's healthy distrust of government surveillance? Given ISIS and al-Qaeda's renewed determination to strike the American homeland, there are three major policy options that Congress should consider.

The Real and Growing Threat of Terrorism

Any debate about America's counterterrorism capabilities must be conducted in the context of the actual terrorist threat the U.S. faces. Since 9/11, The Heritage Foundation has tracked Islamist terrorist plots and attacks, which now, after the recent shooting in Garland, Texas, total 68.[1] This figure, however, does not consider foiled plots of which the public is unaware.

Recently, there has been a dramatic uptick in terrorism: The shooting in Garland is the sixth Islamist terrorist plot or attack in the past five months. Add to that number the surge of Americans seeking to support or join ISIS and al-Qaeda affiliates, and one fact becomes clear: The U.S. is facing the most concentrated period of terrorist activity in the homeland since 9/11.

Of course, it is no coincidence that this spike in terrorism parallels the spread of the Islamic State and other radical groups across Syria, Iraq, and other parts of the Middle East. More than 150 American passport holders have traveled to Syria, or attempted to

Key Points

- Since 9/11, The Heritage Foundation has tracked Islamist terrorist plots and attacks, which now, after the recent shooting in Garland, Texas, total 68.
- After the horrific attacks of September 11, 2001, the United States Congress passed the USA PATRIOT Act. The PATRIOT Act gave the intelligence community and counterterrorism investigators a number of lawful tools to detect and thwart future acts of international terrorism.
- Among other things, Section 215 of the PATRIOT Act substantially revised the Foreign Intelligence Surveillance Act of 1978 to allow U.S. intelligence to query telephone metadata.
- Section 215 expires at the end of May 2015, and policymakers now face a daunting question: How do they protect Americans while respecting this nation's healthy distrust of government surveillance?

This paper, in its entirety, can be found at **http://report.heritage.org/bg3018**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

travel there, to join the fighting, along with more than 20,000 fighters from more than 90 countries.[2] Many of these individuals with American passports are believed to have joined ISIS or the Nusra Front, an affiliate of al-Qaeda in Syria.

Both the Nusra Front and ISIS espouse an anti-Western Islamist ideology that calls for terrorist attacks against the United States. For example, in July 2012, the leader of ISIS, self-proclaimed caliph Abu Bakr Baghdadi, threatened to launch attacks against the U.S. homeland. Baghdadi warned Americans, "You will soon witness how attacks will resound in the heart of your land, because our war with you has now started."[3] Toward this end, al-Qaeda formed a unit of veteran terrorists to recruit some of the Western foreign fighters in Syria and train them to conduct terrorist attacks in their home countries. This unit, dubbed the Khorasan group by U.S. officials, is embedded in the Nusra Front and is particularly interested in recruiting fighters who hold American passports.[4]

These terrorist organizations have undertaken a significant effort to reach out to individuals across the world in order to radicalize and recruit them. In recent testimony before the Senate Appropriations Committee, FBI Director James Comey stated that:

> The threats posed by foreign fighters, including those recruited from the U.S., traveling to join the Islamic State of Iraq and the Levant (ISIL) and from homegrown violent extremists are extremely dynamic. These threats remain the biggest priorities and challenges for the FBI, the U.S. Intelligence Community, and our foreign, state, and local partners. ISIL is relentless and ruthless in its pursuits to terrorize individuals in Syria and Iraq, including Westerners. We are concerned about the possibility of individuals in the U.S. being radicalized and recruited via the Internet and social media to join ISIL in Syria and Iraq and then return to the U.S. to commit terrorist acts. ISIL's widespread reach through the Internet and social media is most concerning as the group has proven dangerously competent at employing such tools for its nefarious strategy.[5]

In the past several weeks, Director Comey has increased the intensity of his warnings, stating that "hundreds, maybe thousands" of individuals across the U.S. are being contacted by ISIS to attack the U.S. homeland.[6]

Secretary of Homeland Security Jeh Johnson has echoed these warnings, saying that lone-wolf terrorists inspired by ISIS could strike at any moment."[7] The 2015 Worldwide Threat Assessment of the U.S. Intelligence Community states that:

> Attacks by lone actors are among the most difficult to warn about because they offer few or no signatures.

1. David Inserra and James Phillips, "67 Islamist Terrorist Plots Since 9/11: Spike in Plots Inspired by Terrorist Groups, Unrest in Middle East," Heritage Foundation *Issue Brief* No. 4392, April 22, 2015, http://www.heritage.org/research/reports/2015/04/67-islamist-terrorist-plots-since-911-spike-in-plots-inspired-by-terrorist-groups-unrest-in-middle-east; Christine Mai-Duc, "SWAT Team Shot Muhammad Cartoon Event Gunmen, Police Chief Says," *The Los Angeles Times*, May 11, 2015, http://www.latimes.com/nation/nationnow/la-na-nn-muhammad-cartoon-shooting-memo-20150511-story.html (accessed May 13, 2015).
2. Nicholas J. Rasmussen, Director, National Counterterrorism Center, "Current Terrorist Threat to the United States," testimony before the Senate Select Committee on Intelligence, February 12, 2015, http://www.nctc.gov/docs/Current_Terrorist_Threat_to_the_United_States.pdf (accessed May 13, 2015).
3. James Phillips, "A Resurgent Al-Qaeda in Iraq Threatens U.S. Attack," The Daily Signal, July 26, 2012, http://dailysignal.com/2012/07/26/a-resurgent-al-qaeda-in-iraq-threatens-u-s-attack/.
4. James Phillips, "The Rise of Al-Qaeda's Khorasan Group: What It Means for U.S. National Security," Heritage Foundation *Issue Brief* No. 4281, October 6, 2014, http://www.heritage.org/research/reports/2014/10/the-rise-of-al-qaedas-khorasan-group-what-it-means-for-us-national-security.
5. James B. Comey, Director, Federal Bureau of Investigation, "Statement Before the Senate Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies," March 12, 2015, http://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2016 (accessed May 13, 2015).
6. Kevin Johnson, "FBI Director Says Islamic State Influence Growing in U.S.," *USA Today*, May 7, 2015, http://www.usatoday.com/story/news/nation/2015/05/07/isis-attacks-us/70945534/ (accessed May 13, 2015).
7. Elise Viebeck, "DHS Secretary: Lone Wolf Attackers Could 'Strike at Any Moment'," *The Hill*, May 10, 2015, http://thehill.com/homenews/sunday-talk-shows/241562-dhs-secretary-lone-wolf-attackers-could-strike-at-any-moment (accessed May 13, 2015).

Contributors

James Jay Carafano, PhD, *is Vice President for the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy and E. W. Richardson Fellow at The Heritage Foundation.*

Charles D. Stimson *is Manager of the National Security Law Program and Senior Legal Fellow in the Davis Institute.*

Steven P. Bucci, PhD, *is Director of the Douglas and Sarah Allison Center for Foreign and National Security Policy of the Davis Institute.*

John G. Malcolm *is Director of, and Ed Gilbertson and Sherry Lindberg Gilbertson Senior Legal Fellow in, the Edwin Meese III Center for Legal and Judicial Studies at The Heritage Foundation.*

Paul Rosenzweig *is a Visiting Fellow in the Allison Center.*

> If ISIL were to substantially increase the priority it places on attacking the West rather than fighting to maintain and expand territorial control, then the group's access to radicalized Westerners who have fought in Syria and Iraq would provide a pool of operatives who potentially have access to the United States and other Western countries.[8]

On the same note, the Director of the National Counterterrorism Center also stated in his testimony to the Senate Select Committee on Intelligence this February that there has been a recent "uptick in terror attacks in the West." This increase in attacks "underscores the threat of emboldened Homegrown Violent Extremists and, how the rapid succession of these attacks may motivate some to attempt to replicate these tactics with little-to-no warning."[9]

These statements and assessments, together with the explicit and public statements of intent by multiple terrorist groups and the recent surge in terrorist plots and attacks against the U.S. homeland, demonstrate that the threat of terrorism is on the rise. Fortunately, the U.S. has improved its ability to foil these attacks, largely due to intelligence capabilities that include but are not limited to the bulk telephone metadata program under Section 215 of the PATRIOT Act.

Signals Intelligence and Section 215

For decades, the United States has relied on robust signals intelligence to gather critical information related to the enemy. During World War I, World War II, the Korean War, the Vietnam War, and the Cold War, this country has depended on the technical capabilities of our national security agencies and the Department of Defense to intercept suspected enemy communications. As technology improved, so did the capabilities of the U.S. government to intercept suspected or known enemy communications. For the most part, the communications the United States was most interested in happened overseas and were gathered without a warrant.

In the 1970s, after the Supreme Court decision in *United States v. U.S. District Court* (also known as "the Keith case")[10] and the findings of the Senate's so-called Church Committee, the Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA), which established a special court in Washington to review government requests for orders allowing for electronic surveillance.[11]

Pre-dating the PATRIOT Act, the FISA allowed the Director of the FBI to obtain orders from the Foreign Intelligence Surveillance Court (FISC) authorizing common carriers to provide the government certain business records for the purpose of foreign intelligence and international terrorism investigations. In order to obtain such an order, the government had to prove the existence of "specific and articulable facts giving reason to believe that the person to whom the records pertain [wa]s a foreign power or an agent of a foreign power."

8. James R. Clapper, Director of National Intelligence, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee," February 26, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (accessed May 13, 2015).
9. Rasmussen, "Current Terrorist Threat to the United States."
10. 407 U.S. 297 (1972).
11. Pub. L. 95-511, 92 Stat. 1783, 50 U.S.C. ch. 36, §§ 1801, et seq. Establishment of the FISA court is provided for in Section 103 of FISA, 50 U.S.C. § 1803.

After the horrific attacks of September 11, 2001, the United States Congress passed the USA PATRIOT Act. The PATRIOT Act gave the intelligence community and counterterrorism investigators a number of lawful tools to detect and thwart future acts of international terrorism.

Among other things, Section 215 of the PATRIOT Act substantially revised the FISA to provide for the production not only of "business records," but also of "any tangible things" and to eliminate the restrictions on the types of businesses such orders can reach. The current version of the FISA as amended by Section 215 allows the Director of the FBI to "make an application for an order requiring the production of any tangible thing...for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."

Under the FISA as amended by Section 215 of the PATRIOT Act, the government—pursuant to an order from the FISC—has been collecting telephone metadata information in bulk since at least May 2006. The court orders to be produced "all call-detail records or 'telephony metadata' created by" United States telecommunications providers "including comprehensive communications routing information, including but not limited to" date and time of call, number called, and duration of call.

Once the government has reasonable, articulable suspicion that a particular phone number is associated with a foreign terrorist organization, that seed number is searched across the government's metadata. The search results yield phone numbers, and the metadata associated with them, which have been in contact with the seed—a step known as the first "hop." Until recently, the National Security Agency (NSA) has been conducting three hops from the original seed number and analyzing the resulting data.

The FISA as amended by Section 215 requires the Attorney General of the United States to adopt "specific minimization procedures governing the retention and dissemination by the [government] of [information] received."[12] Those procedures include storing the metadata in a secure network, accessing the metadata only pursuant to a FISC court order, not disseminating query results outside of the NSA except under certain circumstances, and providing proper training and technical controls to relevant NSA personnel. The 215 bulk telephony metadata program does not collect, analyze, or listen to the content of telephone calls.

The original order, which was good for 90 days, has been renewed 41 times since May 2006. The information is provided on a daily basis to the NSA, where it is kept for five years.

On June 5, 2013, the English newspaper *The Guardian* published a copy of the FISC order that had been leaked illegally by former government contractor Edward Snowden, exposing the telephone metadata program. That leak and subsequent leaks by Snowden that were published by *The Guardian* and *The Washington Post* set in motion a frenzy of debate and discussion, nationally and internationally, about the efficacy of and need for gathering such data, as well as its implications for the privacy interests of American citizens.

Following the Snowden disclosures and after the Obama Administration established the Privacy and Civil Liberties Oversight Board (PCLOB) and the President's Review Group, the NSA limited its inquiries to two hops and required that a FISC judge find that the reasonable articulable suspicion standard has been satisfied before a seed can be queried. Both limitations were approved by a FISC order dated February 5, 2015.

The American Civil Liberties Union subsequently sued the government, arguing that Section 215 was unconstitutional and that the statute did not authorize the bulk collection of telephone metadata. On May 7, 2015, the Court of Appeals for the Second Circuit held that Section 215 did not authorize the bulk telephone metadata program and that the program exceeded the scope of what Congress had authorized. The court declined to address the constitutional issue.[13]

Section 215 expires at the end of May 2015.

12. 50 U.S.C. § 1861(g)(1).

13. The opinion, written by Judge Gerard E. Lynch, contains an excellent summary of the evolution of the PATRIOT Act as it relates to Section 215, telephone metadata in general, and the history of Section 215 since the Edward Snowden disclosures. *American Civil Liberties Union et al. v. Clapper et al.*, 2nd U.S. Circuit Court of Appeals, No. 14-44 (2015), http://www.ca2.uscourts.gov/decisions/isysquery/5b758b27-c77d-44a2-b6e5-dbf456f5c142/1/doc/14-42_complete_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/5b758b27-c77d-44a2-b6e5-dbf456f5c142/1/hilite/. This section of the paper is taken in part from the court's opinion.

The Way Forward

The United States is in a state of armed conflict against al-Qaeda, the Afghan Taliban, ISIS, and associated forces. It must therefore rely on all lawful tools of national security, including but not limited to robust signals intelligence.

As the 9/11 Commission Report made crystal clear, one of the key failures of the United States before the 9/11 attacks was the government's inability to "connect the dots" between known or suspected terrorists. The artificial "wall" between domestic law enforcement and U.S. intelligence agencies, enacted during the 1990s, proved to be America's Achilles' heel.

Some analysts believe that had America had a Section 215–type program in place before 9/11, U.S. intelligence, along with domestic law enforcement, would have been able to connect the dots and prevent at least some of the hijackers from launching their devastating attack.[14]

In fact, according to a report by the House Permanent Select Committee on Intelligence, using the authorities under Section 215 of the PATRIOT Act and Section 702 of the FISA has contributed to thwarting 54 total international terrorist plots in 20 countries.[15] Thirteen of those plots were directed inside the United States.

As Americans, we cherish our constitutional rights, including our right to privacy. Numerous court decisions have held that data, in the hands of third-party providers, are not protected by the Fourth Amendment of the Constitution.[16] There is a case pending before the Court of Appeals for the District of Columbia Circuit in which the issue before the court is whether Section 215 violates the Fourth Amendment; that court has not yet issued its opinion.[17]

As Section 215 expires at the end of May 2015, policymakers are faced with the following quandary: How do they protect Americans from a determined enemy while respecting this nation's healthy distrust of government surveillance?

First, given the increasing nature of the threat and the unique nature of this enemy, it would be unwise to completely abandon the use of telephone metadata in helping to disrupt future terrorist plots and/or gain intelligence about known or suspected foreign terrorists.

Second, Senator Mitch McConnell (R–KY) has proposed a straight extension of Section 215 to the year 2020. However, that approach does not address the Second Circuit's ruling that the statute as written does not authorize the bulk metadata collection program and would likely result in the federal

14. Neil Monroe, "NSA Program Could Have Stopped 9/11, Says Obama Advisor," The Daily Caller, December 28, 2013, http://dailycaller.com/2013/12/28/nsa-program-could-have-stopped-911-says-obama-advisor/ (accessed May 13, 2015).
15. Permanent Select Committee on Intelligence, U.S. House of Representatives, "54 Attacks in 20 Countries Thwarted by NSA Collection: Four Declassified Examples," http://intelligence.house.gov/1-four-declassified-examples-more-50-attacks-20-countries-thwarted-nsa-collection-under-fisa-section (accessed May 15, 2015).
16. *Smith v. Maryland*, 442 U.S. 735 (1979).
17. The case awaiting decision in the U.S. Court of Appeals for the District of Columbia Circuit is *Klayman v. Obama*, No. 14-5209, on appeal from *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. December 16, 2013). In that case, the U.S. District Judge in the District of the District of Columbia concluded, among other things, "that plaintiffs have standing to challenge the constitutionality of the Government's bulk collection and querying of phone record metadata, that they have demonstrated a substantial likelihood of success on the merits of their Fourth Amendment claim, and that they will suffer irreparable harm absent preliminary injunctive relief." The Judge issued a preliminary injunction against the government and then stayed the effect of the injunction pending the appeal to the Court of Appeals for the District of Columbia Circuit. Subsequently, the U.S. Foreign Intelligence Surveillance Court explicitly rejected the holding and reasoning of the U.S. District Judge in the *Klayman* case. *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, No. BR 14-01, 2014 WL 5463097 (Foreign Intelligence Surveillance Court, March 20, 2014) ("The only question raised in the Petition is whether the production order is unlawful under the Fourth Amendment in light of Judge Leon's December 16 opinion in *Klayman*.... Turning now to the merits of the Fourth Amendment issue, this Court finds Judge Leon's analysis in *Klayman* to be unpersuasive and concludes that it provides no basis for vacating or modifying the Secondary Order issued [redacted] January 3, 2014."). Also, the U.S. District Court for the Southern District of California held that bulk telephony metadata collection under the Foreign Intelligence Surveillance Act did not violate the Fourth Amendment. *United States v. Moalin*, Crim. No. 10-4246, 2013 WL 6079518 (S.D. Cal. November 18, 2013) ("Because individuals voluntarily convey numerical information to the telephone company to complete a telephone call, one cannot possess a reasonable expectation of privacy in the telephone number dialed (as opposed to the content of the conversation). For these reasons, the court declines Defendants' invitation to depart from well-established precedent.") (citation omitted). A number of courts recently considering collection of telephone metadata obtained in various contexts for law enforcement investigations have held that such collection did not violate the Fourth Amendment. See, for example, *United States v. Graham*, 846 F. Supp 2d 384 (D. Md. March 1, 2012) and cases cited therein, and *United States v. Gordon*, Crim. No. 09-153-02 (RMU), 2012 WL 8499876 (D.D.C. February 6, 2012).

district court judge who now has the case enjoining the government from continuing the program.

In view of ISIS and al-Qaeda's renewed determination to strike the American homeland, there are three major policy options that Congress should consider.

Policy Option No. 1. The first option would be to amend Section 215 specifically to allow the NSA to collect bulk telephone metadata and query that data pursuant to FISC court orders; codify the existing program as it has been modified by the Administration but add in cell phone data as well; and fold in the transparency, privacy, and civil liberties contained within the USA FREEDOM Act, discussed in detail below. Such an amendment would put the program on stronger statutory grounds and address the Second Circuit's holding. There are technical and business practice arguments in favor of this, but it would not address the concerns of many that the government was maintaining a database of telephony metadata.

While this approach offers the simplest method to query and analyze the metadata, as it is housed in one place, this approach currently suffers from lack of transparency, lack of civil liberties protections, and privacy concerns.

In 2014, the National Research Council appointed a committee of experts to assess "the feasibility of creating software that would allow the U.S. intelligence community more easily to conduct targeted information acquisition rather than bulk collection"[18] as called for in Section 5(d) of Presidential Policy Directive 28. Committee members and experts included people from Oracle, Microsoft, Google, and other industry and academic experts. After a thorough review, these experts found that there is currently no technologically feasible alternative to the current metadata bulk collection platform.

It is safe to assume that the commercial IT world is already working to find a way to provide the tools to do just that sort of analysis. Today, only by keeping all the data together and making appropriate inquiries of the data can the dots be connected, but in the immediate future, other options should become available.

Policy Option No. 2. The chief concern among policymakers who are skeptical of government surveillance, and in particular Section 215, is that it is the government that holds the telephony metadata. Such policymakers have also noted that there are not enough privacy protections built into the existing program.

One solution to the first concern would be to establish and require that a private, third-party entity house the telephony metadata, including cell phone metadata. The metadata would be collected in bulk but housed by a private third party. Court orders from the FISC would authorize select employees of the private entity, with appropriate security clearances, to query the database. Just as in policy option number one, the Congress could add transparency, civil liberties, and privacy protections to the FISC and program, as discussed below. This alternative would take time to develop and has gained little traction on either side of the debate.

Policy Option No. 3. The third policy option is the House-passed USA FREEDOM Act—legislation that reauthorizes Section 215 and reforms it to end government bulk collection of telephone metadata by the NSA. Instead, the metadata resides with the telephone carriers, where the government will have access to it subject to a court order by the FISC.

The USA FREEDOM Act replaces bulk collection with a program called a "Call Detail Record." Under this new program, whenever the NSA feels it has reasonable, articulable suspicion that a phone number is associated with international terrorism, it can seek an order to access information about that number from the FISC.

If the FISC gives the order, the NSA will submit one or several queries to the telecom companies for historical and real-time data on the number in question. At that time, both historical and real-time data related to the suspicious number will flow into the NSA, as well as data on the two generations of numbers surrounding it (referred to as "hops"). This information will flow on a 24/7 basis for 180 days, double the amount of time that a FISC order currently authorizes. At the end of 180 days, the NSA can seek renewal for another 180-day time period.

Ending the bulk collection of telephone metadata by the government, or even housing it in a private third-party entity, may encumber the ability of the intelligence community to analyze all the data in

18. National Research Council, *Bulk Collection of Signals Intelligence: Technical Options* (Washington: National Academies Press, 2015), https://www.nsa.gov/civil_liberties/_files/BulkCollectionofSignalsIntelligenceTechOptions.pdf (accessed May 15, 2015).

real time across a known pool of data. Such a change will inevitably slow down investigators, but as the technology changes, this should be rectified. That said, numerous intelligence community leaders have said that while it is far from ideal, they could live with such a system, understanding that America is accepting some risk by doing so.

Section 102 provides for emergency authority for the Attorney General to require emergency production of tangible things absent a court order as long as he or she informs a FISC judge and subsequently makes an application to the court within seven days after taking this action. The USA FREEDOM Act also establishes several civil liberties protections for the existing program as it relates to the telephone metadata program.

Section 401 of the Act requires the presiding judges of the FISC to designate not fewer than five individuals to be eligible to serve as *amicus curiae*—friends of the court. Those designated shall be experts in privacy and civil liberties, intelligence collection, and communications technology and be eligible for a security clearance. The *amicus curiae* serve to assist the court in the consideration of any novel or significant interpretation of the law.

Section 402 of the Act also mandates the Director of National Intelligence, in consultation with the Attorney General, to conduct a declassification review of each decision, order, or opinion by the FISC and, to the extent practicable, make those decisions, orders, or opinions publicly available.

The USA FREEDOM Act also contains other reforms, including prohibiting bulk collection utilizing FISA pen register and the "trap and trace" procedures in Section 201.

The Act is the only legislative vehicle that has passed a chamber of Congress. It is not perfect and could be improved. For example, there should be a uniform period of time for carriers to maintain the telephone metadata. Another could be designating a specific format in which the carriers must maintain the data to allow more expeditious analysis once the data is appropriately obtained. The USA FREEDOM Act strikes a balance between maintaining our national security capabilities and protecting privacy and civil liberties, and this should always be the goal.

Conclusion

The threat of international terrorism is real and on the rise. The United States remains in a state of armed conflict against non-state actors: al-Qaeda, the Afghan Taliban, ISIS, and associated forces. Winning this armed conflict requires a coordinated, sophisticated, and comprehensive strategy that harnesses all aspects of America's national power.

For decades, over many armed conflicts, the United States has relied on and utilized the fruits of lawful signals intelligence to disrupt, degrade, detect, and ultimately defeat the enemies of the United States. Today, because of stunning advances in technology, we have the ability to search through billions of anonymous bits of telephone call data and draw connections among known and suspected foreign terrorists about whom we otherwise might never have known. Those connections and the connections made possible by other aspects of national power enable those who defend our freedoms to keep us safe.

In crafting the best policies with respect to mining telephone metadata, Congress has a solemn duty to abide by the Constitution, particularly our Fourth Amendment right to be secure in our persons, houses, papers, and effects against "unreasonable searches and seizures." At the same time, Congress has to recognize that telephone metadata is not a subscriber's personal property: It is owned by the telephone companies as part of their business records. Yet the data is sensitive, and American citizens expect that their phone records, even if they do not own them, are private information. Congress must find a way to balance these two interests, because allowing the capacity to query third-party telephone metadata—signals intelligence—to expire is unwise and dangerous, especially during a time of armed conflict.

The three options contained in this paper are all considered viable options by some. None will make everyone happy, but now it is time for Congress to make a choice.