August 1, 2013

MEDIA LEAKS FACTS & CONTEXT (LONG VERSION)

The nation needs both **NATIONAL SECURITY** and **PROTECTION OF CIVIL LIBERTIES AND PRIVACY**. The issue is not "security OR privacy;" it is both.

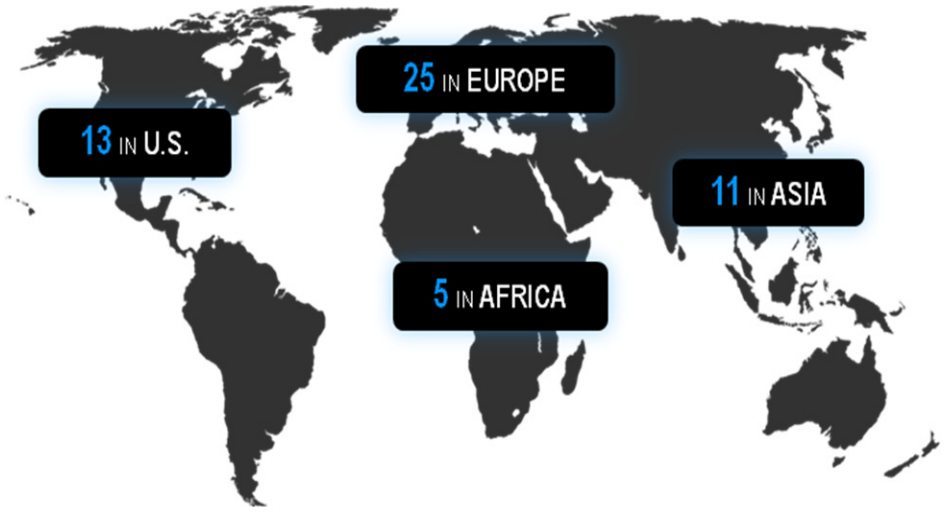
The events that led up to 9/11/2001 show how terrorists operated inside our borders and used our communications networks to connect to planners and financiers overseas. They executed the largest attack on U.S. soil in the 20th Century.

The 9/11 Commission criticized the Intelligence Community for failing to "connect the dots," particularly between terrorists overseas and their operatives in the United States. After 9/11, we as a nation—the Administration, Congress, courts, military, and citizens—said, "Never again."

The Administration, Congress, and the Court developed programs and capabilities to address this issue, keep the nation safe and protect the privacy and civil liberties of U.S. citizens. Section 215 Authority or "Business Records FISA" helps us connect the dots between foreign terrorists and domestic operatives. Section 702 Authority focuses on foreign intelligence targets overseas and contributes significantly to our global counterterrorism mission.

Using these capabilities, we and our allies have successfully disrupted 54 terrorist events in the U.S. homeland and abroad.

Companies are legally compelled to comply with these programs. Most developed countries have lawful intercept programs to compel their communications providers to provide data supporting counterterrorism or foreign intelligence investigations. All companies, U.S. and foreign, are compelled to comply with these lawful intercept programs. The European Union Data Retention Directive is a case in point.



Section 215 Authority, Business Records FISA

BR FISA is used in a narrow and focused way. In 2012, less than three hundred numbers were approved to be queried.

The BR FISA telephony metadata program was one of our responses to the lessons of 9/11. This program is specifically focused on detecting terrorist plots that cross the seam between foreign terrorist organizations and the U.S. homeland. Many will recall the inability of the U.S. intelligence community to make such a connection between 9/11 hijacker Khalid al Midhar who was in California and an al-Qa'ida safe house in Yemen. NSA had collected the Yemen end of the communications but due to the nature of our collection, we had no way of determining the number or the location of al Midhar. We did not have the tools to do that. Section 215 provides those tools – the phone metadata to help make that connection.

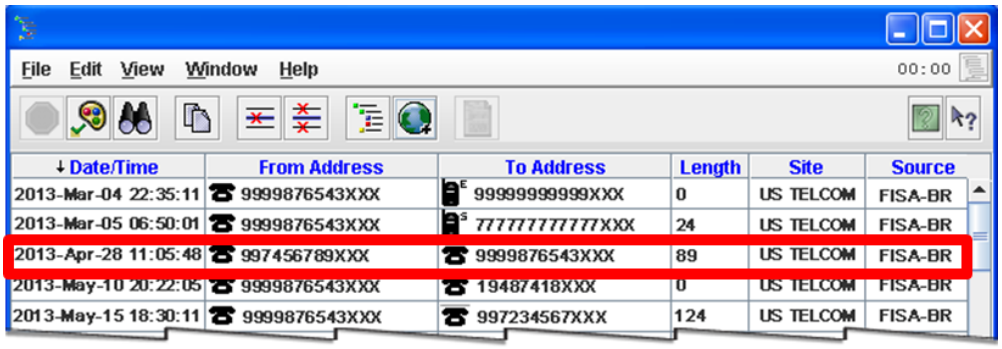
The BR provision of FISA was authorized by Congress under Section 215 of the Patriot Act. This program has been approved by the Administration and the Foreign Intelligence Surveillance Court. It compels carriers to share telephone metadata for counterterrorism purposes only. Any other use of this data is prohibited.

BR FISA is used in a narrow and focused way. In 2012, less than three hundred numbers were approved to be queried.

Further, in order to search this data, there must be a relevant standard, or in legal terms, a reasonable articulable suspicion that a phone number to be queried is associated with a foreign terrorist organization. This rationale must be clearly justified in writing and approved by one of 22 designated and trained individuals.

Once approved, NSA obtains the date and time of the call, the calling number (from address) and the called number (to address); and the duration of the call.

NSA does not obtain the content of calls, names or subscriber information, or locational information. There is no data-mining or indiscriminate trolling through the data; every single number queried is audited.



UNDER 215, NSA **OBTAINS:**

- Date/Time of call
- Calling number (from address)
- Called number (to address)
- Duration of call (length)
- Origin of metadata record (site/source)

UNDER 215, NSA **DOES NOT OBTAIN**:

- Content of calls
  - NO voice communication
  - NO SMS/text messages
- Subscriber information
  - NO names
  - NO addresses
  - NO credit card numbers
- Locational information

Given its specific focus on plots against the homeland, this program provided value in 12 out of the 13 homeland-related terrorist events of the 54 total events provided to the Congress. In four of those cases, it told the FBI there were no significant connections, helping to disprove leads and conserve resources. In eight of those cases, it provided the FBI further lead information on numbers of interest to help focus their investigations.

On the question of why do you need so much data, in simple terms, you are looking for a needle, in this case a number, in a haystack. But not just any number. You want to make a focused query against a body of data that returns only those numbers that are connected to the one you have reasonable suspicion is connected to a terrorist group. But unless you have the haystack – in this case all the records of who called whom – you cannot answer the question. The confidence you will have in any answers returned by your query is necessarily tied to whether the haystack constitutes a reasonably complete set of records and whether those records look back a reasonable amount of time to enable you to discover a connection between conspirators who might plan and coordinate across several years. Hence "all" the records are necessary to connect the dots of an ongoing plot, sometimes in a time sensitive situation, even if only an extremely small fraction of them is ever determined to be the match you're looking for.

Questions have also been raised about whether this data should be stored on government servers or remain at the service providers; how long the data should be kept; and if more Court involvement is needed when querying the data. We should discuss the merits of different solutions within the context of the key operational attributes of the program: privacy and civil liberties must be protected; queries can be made in a timely manner to support the disruption of imminent terrorist plots; the repository of data is comprehensive enough to ensure we can confidently connect the dots between a foreign terrorist organization and domestic terrorist operatives.

Section 702 Authority

FAA/702 collection is a Court-approved program that concerns targeting of foreign persons reasonably believed to be located abroad for foreign intelligence purposes such as counterterrorism and weapons proliferation.

This program may not be and is not used to intentionally target any person known to be in the United States or a U.S. person abroad.

The Senate Select Committee on Intelligence conducted its own investigation between 2008 and 2012 and found, "Through four years of oversight, the Committee has not identified a single case in which a government official engaged in willful effort to circumvent or violate the law."

TOMORROW'S SECURITY RELIES ON TODAY'S CHOICES

Since 9/11, we have had great success in stopping terrorist activities here and abroad. We must continue that success and protect our civil liberties and privacy. We are open to ideas on how to better protect our networks, protect our civil liberties, and stop future attacks by finding terrorists who take sanctuary in our communications networks.

How these programs defend the nation and protect civil liberties and privacy

NSA is a foreign intelligence agency, which means it focuses on foreign intelligence targets that meet national intelligence priorities. One such priority is counterterrorism.

Foreign terrorists sometimes communicate with persons in the U.S. or Americans overseas. In targeting terrorists overseas, NSA may get both sides of a communication. If one side is in the U.S., we call that "incidental collection." If that communication involves a U.S. person, NSA must follow FISC-approved minimization procedures to ensure we protect the privacy of U.S. persons.

This was the case with Najibullah Zazi. While monitoring the activities of al-Qa'ida terrorists, NSA intercepted an email about a recipe for explosives from a terrorist located in Pakistan communicating with an individual who they believed to be in the U.S. NSA immediately tipped FBI of this communication, who subsequently identified the individual as Colorado-based Najibullah Zazi and provided NSA with Zazi's telephone number for use with the BR FISA metadata. On the basis of Zazi's connection with al-Qa'ida, NSA analyst found a reasonable articulable suspicion on Zazi and ran his number against the telephony metadata, passing lead information back to the FBI. One lead revealed a previously unknown number for U.S.-based co-conspirator Adis Medunjanin, corroborating a direct and recent connection to Zazi and highlighting his potential role in the plot. The FBI tracked Zazi as he traveled to New York to meet up with co-conspirators, where they were planning to conduct a terrorist attack. Zazi and Medunjanin, as well as additional co-conspirators were subsequently arrested and convicted for conspiring to bomb the NYC subway system.

Had this plot not have been prevented, it would have been the biggest terrorist attack since 9/11 on U.S. soil.

It is important to emphasize that virtually all developed countries have laws requiring their communications providers to provide data supporting counterterrorism or foreign intelligence investigations. The U.S. government stands out for the rigor of its oversight framework of these activities. All companies, U.S. and foreign, are compelled to comply with these lawful intercept programs. Absent this, communications mediums would become safe havens for terrorist planning and communications.