Excerpts from the United States' Briefs in *ACLU v. Clapper*, No. 13-cv-03994 (S.D.N.Y.)

[These excerpts are adopted from three briefs recently filed by the Department of Justice in the case brought by the ACLU, challenging the Section 215 "Telephony Metadata" collection program. I have consolidated the excerpts from the three briefs, and have omitted most references to the record in the case. The ACLU challenges the program not only on constitutional grounds, but also on statutory grounds. The statutory arguments are omitted here.]

Plaintiffs challenge a program by which the National Security Agency (NSA) obtains, pursuant to orders of the Foreign Intelligence Surveillance Court (FISC), bulk telephony metadata – business records created by telecommunications service providers that include such information as the telephone numbers placing and receiving calls, and the time and duration of those calls. Targeted electronic searches of these data, based on telephone numbers or other identifiers associated with foreign terrorist organizations, can reveal communications between known or suspected terrorists and previously unknown terrorist operatives, located in this country, who may be planning attacks on U.S. soil. Information gleaned from analysis of bulk telephony metadata obtained under this program has made important contributions to the FBI's counter-terrorism mission. The bulk collection of telephony metadata for these limited purposes has been authorized and periodically reauthorized over the past seven years under thirty-four separate orders issued by fourteen separate judges of the FISC. The program operates under FISC orders, together with stringent supervision and oversight by all three branches of Government, to prevent access to, use, or dissemination of the data for any purpose other than foreign intelligence. In a detailed opinion issued on August 29, 2013, the FISC concluded that the telephony metadata program is authorized by statute, and lawful under the Constitution.

Plaintiffs' motion for a preliminary injunction is based entirely on conjecture as to how the Government might misuse telephony metadata collected under the program, and consequences that might ensue. While Plaintiffs purport to base their case on public statements by the Government about how this program operates, they ignore crucial limitations, described in the very same documents, on the Government's collection and use of the metadata, and contend, with no basis in fact, that the Government is using these metadata to track the associations of U.S. citizens, compile profiles on them, and draw comprehensive social maps of their lives.

Plaintiffs' portrayal of the program is unsupported by any evidence. Under the challenged program, the NSA collects only numeric telephony metadata – *i.e.,* call detail records – including such session-identifying information as the telephone numbers that placed and received a call, and the date, time, and duration of the call. The Government does not collect the substantive content of any telephone call under this program, it does not listen to or record the contents of any call, nor does it collect cell-site location information. In

addition, under this program the Government does not collect the name, address, or financial information of any subscriber, customer, or any party to a call. The metadata collected under this program do not reveal that a whistleblower called the ACLU, or that an individual called an abortion clinic, a criminal-defense lawyer, or a suicide hotline, as Plaintiffs speculate.

Equally important, the FISC orders authorizing the program prevent the NSA from accessing the metadata collected under the program to ascertain any such information or to draw "comprehensive social maps" of anyone's lives. The NSA may only query the collected metadata for counter-terrorism purposes, and even then, only if there is a reasonable, articulable suspicion that the selection term (e.g., the telephone number) to be queried is associated with a specified foreign terrorist organization approved for targeting by the FISC. This requirement bars the type of indiscriminate querying of the metadata, using identifiers not connected with terrorist activity, about which Plaintiffs speculate. As a result, only a tiny fraction of the collected metadata are ever reviewed, much less disseminated, by NSA analysts. These constraints on the NSA's access to and use of the metadata are critical to the program's continued authorization by the FISC, and the FISC has not hesitated to take action to enforce them.

* * * *

Statutory Background

Congress enacted FISA to authorize and regulate certain governmental surveillance of communications and other activities conducted for purposes of gathering foreign intelligence. In enacting FISA, Congress also created the FISC, an Article III court of 11 appointed U.S. district judges with authority to consider applications for and grant orders authorizing electronic surveillance and other forms of intelligence-gathering by the Government. 50 U.S.C. § 1803(a); *see In re Motion for Release of Court Records,* 526 F. Supp. 2d 484, 486 (F.I.S.C. 2007).

At issue here is the "business records" provision of FISA, 50 U.S.C. § 1861, enacted by section 215 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("Section 215"). Section 215 authorizes the FISC to issue an order for the "production of any tangible things (including books, records, papers, documents, and other items) for an investigation [1] to obtain foreign intelligence information not concerning a United States person or [2] to protect against international terrorism" (provided, in the case of a counter-terrorism investigation of a "United States person," that "such investigation ... is not conducted solely upon the basis of activities protected by the first amendment to the Constitution"). 50 U.S.C. § 1861(a)(1). The records must be of a type obtainable by either a grand jury subpoena, or an order issued by a U.S. court directing the production of records or tangible things. *Id.* § 1861(c)(2)(D).

The Government's application for an order under Section 215 must include, among other things, a statement of facts showing that there are "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation ... to obtain foreign

intelligence information not concerning a United States person or to protect against international terrorism." *Id.* § 1861(b)(2)(A). The investigation must be authorized and conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor thereto). *Id.* § 1861(a)(2)(A), (b)(2)(A). Information acquired from the records or other tangible items received in response to a Section 215 order "concerning any United States person may be used and disclosed by [the Government] without the consent of [that] person only in accordance with ... minimization procedures," adopted by the Attorney General and enumerated in the Government's application, that "minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the [Government's] need ... to obtain, produce, and disseminate foreign intelligence information." *Id.* § 1861(b)(2)(B), (g)(2), (h). The FISC must find that these requirements have been met before it issues the requested order, which in turn must direct that the minimization procedures described in the application be followed. *Id.* § 1861(c)(1). Section 215 includes a scheme providing for judicial review of a business records order, but only in limited circumstances. Specifically, it allows "[a] person receiving a production order [to] challenge the legality of that order" by filing a petition with the "review pool" of FISC judges designated under 50 U.S.C. § 1803(e)(1) to review production orders under Section 215. *Id.* § 1861(f)(1), (2)(A)(i). A "pool" judge considering a petition to modify or set aside a production order may grant the petition if the judge finds that the order does not meet the requirements of Section 215 or "is otherwise unlawful." *Id.* § 1861(f)(2)(B). Thus, a production order can be set aside if it exceeds the authority conferred by Section 215 or is unconstitutional. 1 D. Kris & J. Wilson, National Security Investigations & Prosecutions § 19:10 at 714 (2d ed. 2012) ("Kris & Wilson"). Either the Government or a recipient of a production order may appeal the decision of the pool judge to the FISC Court of Review, with review available thereafter on writ of certiorari in the Supreme Court. 50 U.S.C. § 1861(f)(3); *see id.* § 1803(b). Section 215's carefully circumscribed provisions for judicial review were added when Congress reauthorized the USA PATRIOT Act in 2006, and these provisions authorized contested litigation before the FISC for the first time. 1 Kris & Wilson §5:5, 19:7 (2d ed. 2012). The FISA does not provide for review of Section 215 orders at the behest of third parties.

* * * *

Using Section 215 to Collect Telephony Metadata

One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. The exploitation of terrorist communications is a critical tool in this effort, and analysis of bulk telephony metadata provides the Government with a timely and effective means of discovering communications with and among unknown terrorist operatives.

Indeed, the telephony metadata program is aimed at filling a significant intelligence gap identified by the September 11, 2001 attacks. Prior to that tragic event, the NSA intercepted and transcribed seven calls made by hijacker Khalid al-Mihdhar, who was living in San Diego, California, to a telephone identifier associated with an al Qaeda safe house in Yemen. The NSA intercepted these calls using overseas signal intelligence capabilities, but those capabilities did not capture the calling party's telephone number identifier. Because they lacked the U.S. telephone identifier, NSA analysts mistakenly concluded that al-Mihdhar was overseas. Telephony metadata, however, if available at the time, would have included the missing information and might have permitted NSA analysts to place al-Mihdhar within the United States prior to the attacks and advise the FBI of that information.

Plaintiffs attempt to depict the telephony metadata program as one in which Americans' communications are "track[ed]" by intelligence officials and used to compile "rich profiles" and "comprehensive social maps" of their lives, but that description bears no resemblance to this stringently controlled program. Under the program, the Government obtains orders from the FISC, pursuant to FISA's "business records" provision, 50 U.S.C. § 1861, enacted by section 215 of the USA-PATRIOT Act, Pub. L. 107-56, 115 Stat. 272 (Section 215), that direct certain telecommunications service providers to produce telephony metadata, also referred to as call detail records, to the NSA. The NSA then stores, queries, and analyzes the metadata for counter- terrorism purposes. Under the terms of the FISC's orders, the Government's authority to continue the program expires after 90 days and must be renewed. The FISC first authorized the program in May 2006, and since then it has renewed the program thirty-three times under orders issued by fourteen different FISC judges.

Under the FISC's orders, the NSA is authorized to collect, as to each call, the telephone numbers that placed and received the call, other session-identifying information (e.g., International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card number, and the date, time, and duration of a call. The data are numerical only. The FISC's orders authorizing this program do not allow the NSA to collect the substantive content of any telephone call, nor the name, address, or financial information of a subscriber, customer, or any party to a call. The Government cannot, under this program, listen to or record the contents of anyone's communications.

The Government obtains these FISC orders by submitting detailed applications from the FBI explaining that the records are sought for investigations to protect against international terrorism that concern specified foreign terrorist organizations identified in the application. As required by Section 215, the application contains a statement of facts showing that there are reasonable grounds to believe that the metadata as a whole are relevant to the investigations of these organizations. The application is supported by a declaration from a senior official of NSA's Signals Intelligence Directorate. *Id.*

The FISC's orders strictly limit access to, analysis of, and dissemination of information derived from the metadata to valid counter-terrorism purposes. The NSA may access the

metadata for purposes of obtaining foreign intelligence information only through "contact-chaining" queries (term searches) of the metadata using identifiers (typically telephone numbers) approved as "seeds" by one of twenty- two designated officials in NSA's Signals Intelligence Directorate. Such approval may only be given upon a determination by one of these officials that, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the selection term to be queried is associated with one or more of the specified foreign terrorist organizations. Where the selection term is reasonably believed to be used by a U.S. person, NSA's Office of General Counsel must also determine that the term is not regarded as associated with a foreign terrorist group solely on the basis of activities protected by the First Amendment. These determinations are effective for a finite period of time.

This "reasonable, articulable suspicion" requirement bars the indiscriminate querying of the telephony metadata based on identifiers not connected with terrorist activity. Indeed, because of this requirement, the vast majority of the data obtained under this program are never seen by any person; only the tiny fraction of the records responsive to queries authorized under the "reasonable, articulable suspicion" standard are reviewed or disseminated by NSA analysts.

Also under the FISC's orders, once the NSA has obtained approval to conduct a query, the results are limited to records of communications within three "hops" from the seed. That is, the query results may only include identifiers and associated metadata having a direct contact with the seed (the first "hop"), identifiers and associated metadata having a direct contact with first "hop" identifiers (the second "hop"), and identifiers and associated metadata having a direct contact with second "hop" identifiers (the third "hop"). Query results do not include the names or addresses of individuals associated with the responsive telephone numbers, because that information is not included in the database in the first place.

The ability under this program to accumulate metadata in bulk, and to quickly conduct contact-chaining analyses beyond the first hop, is crucial to the utility of the database. These capabilities allow use of the database to conduct a level of historical analysis, and the discovery of contact links, that cannot practically be accomplished through targeted intelligence-gathering authorities, such as acquiring metadata of only direct communications with known terrorist operatives, or prospectively acquiring the metadata of communications occurring after a pen-register/trap-and-trace (PR/TT) device is installed. For example, the metadata may reveal that a seed telephone number has been in contact with a previously unknown U.S. telephone number. Examining the chain of communications out to the second and in some cases a third hop may reveal a contact with other telephone numbers already known to be associated with a foreign terrorist organization, thus establishing that the previously unknown telephone number is itself likely associated with terrorism. This type of contact-chaining under the program is possible because the bulk collection of telephony metadata creates an historical repository that permits retrospective analysis of terrorist-related communications across multiple telecommunications networks, and that can be immediately accessed as new terrorist-associated telephone identifiers come to light.

Not only is NSA's access to the telephony metadata obtained under this program limited as described above, its dissemination of query results is also tailored to provide only the most useful foreign intelligence information to the FBI and other agencies. The NSA does not use queries of these data to provide the FBI with profiles on suspected terrorists or comprehensive records of their associations. Nor does it provide the FBI with a list of all identifiers directly or indirectly connected (at one, two, and three hops) with a suspected terrorist identifier. Such a "data dump" of contact information would be of little investigative value to the FBI, particularly in the midst of investigations where time may be of the essence. Rather, the NSA applies the tools of signals intelligence tradecraft to focus only on those identifiers which, based on the NSA's analytic judgment and experience, and other intelligence available to it, may be of use to the FBI in detecting persons in the United States who may be associated with the specified foreign terrorist organizations, and acting in furtherance of their goals. Prior to dissemination of any U.S.-person information outside NSA, a senior NSA official must determine that the information is in fact related to counter-terrorism information, and is necessary to understand that information or assess its importance. And the NSA may not provide the FBI with any information derived from the metadata unless it is responsive to query terms approved under the "reasonable, articulable suspicion" standard.

The Government has recently made public FISC orders and opinions concerning various failures to fully implement and comply with these minimization procedures, owing to human error and technological issues, that were discovered in 2009. The Government reported these problems to the FISC (and Congress) and remedied them, and the FISC (after temporarily suspending the Government's authority to query the database without the court's approval) reauthorized the program in its current form. Importantly, even the most serious of these incidents did not involve the compilation of detailed profiles of Americans' lives, as Plaintiffs insinuate has been occurring.

The telephony metadata program has contributed to the fight against terrorism in important ways. Metadata analysis provides information that assists the FBI in detecting, preventing, and protecting against terrorist threats to the national security of the United States by providing the predication to open investigations, advance pending investigations, and revitalize stalled investigations. It can also rule out avenues of investigation, allowing the FBI to redirect scare resources. Metadata analysis can also provide early warning signals that alert the FBI to individuals who are inside the United States and are linked to persons who pose a threat to the national security. Similarly, metadata analysis can be of importance in situations where timely information about communications by and among suspected terrorists may be necessary to prevent the occurrence (or recurrence) of terrorist attacks.

The accompanying FBI declaration discusses unclassified examples in which telephony metadata analysis, together with other intelligence methods, played a role in the FBI's counter- terrorism successes. One such example is the contribution of telephony metadata analysis to the FBI's disruption, in fall 2009, of the plan by al-Qa'ida associated terrorist Najibullah Zazi and his associates to bomb the New York City subway. After signals

intelligence, together with FBI investigative efforts, revealed that Zazi was in contact with al Qa'ida-associated terrorists, NSA received Zazi's telephone number from the FBI and ran it against the telephony metadata, identifying and passing additional leads back to the FBI for investigation. One of these leads revealed a previously unknown number for co-conspirator Adis Medunjanin, and corroborated his connection to Zazi as well as to other U.S.-based extremists. Ultimately, Zazi and his co-conspirators were arrested; Zazi pled guilty to conspiring to bomb the New York City subway system, and Medunjanin was sentenced to life in prison.

* * * *

THE GOVERNMENT'S COLLECTION OF TELEPHONY METADATA DOES NOT VIOLATE PLAINTIFFS' FOURTH AMENDMENT RIGHTS

Critical to Plaintiffs' argument that the collection of telephony metadata under Section 215 violates their Fourth Amendment rights is the premise that the NSA also collects and analyzes subscriber-identifying information – that is, to whom the phone numbers making and receiving a call belong – in addition to purely numerical information (the phone numbers dialed, the time and duration of calls made). As explained above, however, under the FISC orders at issue, the NSA collects no information identifying the persons to whom phone numbers belong. Moreover, under the FISC's orders, no metadata can be examined except the tiny fraction of the records that are responsive to authorized queries made under the "reasonable, articulable suspicion" standard. Such queries, even when made, are conducted solely to detect communications with unknown terrorist operatives and to provide the FBI and other agencies with discrete information useful to their counter-terrorism mission, not to create profiles of ordinary Americans' lives.

Once its premise falls away, Plaintiffs' Fourth Amendment argument fails. There is no reasonable expectation of privacy in telephony metadata – all that is at issue here – as the Supreme Court squarely held in Smith v. Maryland, 442 U.S. 735 (1979).

Thus, the telephony metadata program involves no Fourth Amendment search. Even if there were a search, it would be reasonable. Any intrusion on privacy is minimal, again because only telephony metadata are collected, and is outweighed in any event by the paramount Government interest in thwarting terrorist attacks.

A. Collection and Query of Telephony Metadata Does Not Constitute a Search

Plaintiffs' Fourth Amendment claim is controlled by *Smith*, which held that the Government's recording of the numbers dialed from an individual's home telephone, through the off-site installation of a pen register, did not constitute a search under the Fourth Amendment. *Smith* held that individuals have no reasonable expectation of privacy in the telephone numbers they dial, because they convey the numbers to the phone company in the act of dialing, and "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." 442 U.S. at 743-

44. *Smith* directly applies here to the collection of telephone numbers and other telephony metadata that subscribers voluntarily turn over to providers.

Plaintiffs seek to avoid *Smith*'s holding by first alleging a subjective expectation of privacy in their telephony metadata, claiming to regard the mere fact of many of their calls as sensitive or confidential. But under the FISC's orders the NSA may collect only phone numbers, and other numeric data, that do not identify who places or receives calls. Without that information, a phone number by itself does not reveal whether the number dialed is an abortion clinic, a criminal-defense lawyer, or a suicide hotline, or that the person placing the call is a whistleblower. The call detail records instead merely show that one ten-digit number called another.

Plaintiffs further claim, again contrary to *Smith*, that an expectation of privacy in dialed telephone numbers is objectively reasonable. The *Smith* Court held that "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."'" 442 U.S. at 743 (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967)). The rationale for the holding was that the Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," such as, in *Smith*, the numbers a subscriber conveys to the phone company. Id. at 743-44. In the more than thirty years since *Smith* was decided, the strength of the third-party doctrine has not waned. And the third-party doctrine has consistently been applied, both pre- and post-*Smith*, to telephone call detail records like the business records at issue here, which are also third-party records.

Nor is there any reason to think that a subjective expectation of privacy in telephony metadata is any more reasonable now than it was in 1979. Just as they did in 1979, subscribers now "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." Id. at 743.[1]

* * * *

---

[1] Plaintiffs' citation to their Verizon contracts, in which Verizon agrees to protect the confidentiality of certain customer information, including local and toll billing information, is not helpful to them. Plaintiffs concede that their agreement is qualified by the words "in accordance with applicable laws, rules and regulations," and this case involves a court order to produce records. See also Verizon Privacy Policy at 3, available at http://www22.verizon.com/about/privacy/policy/ ("We may disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as: to comply with valid legal process including subpoenas, court orders or search warrants"). Nor is a provider's agreement to keep the information confidential legally relevant. See *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984); *United States v. Miller*, 425 U.S. 435, 443 (1976) ("the Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

Plaintiffs' reliance on the two concurrences in *United States v. Jones*, 132 S. Ct. 945 (2012), which opined on expectations of privacy concerning long-term GPS monitoring, is misplaced. As an initial matter, this Court is obviously bound only by the majority opinion in *Jones*, not by the concurring opinions (one by Justice Alito and one by Justice Sotomayor). In any event, the concerns expressed in the *Jones* concurrences do not apply to the NSA's telephony metadata program. As quoted by Plaintiffs, Justice Sotomayor expressed concern that the GPS monitoring at issue in *Jones* "'generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.'" That was so because the GPS device used in *Jones* was attached by law enforcement officers to a single, known person's vehicle and recorded the vehicle's locations over a period of time. Law enforcement learned from the GPS data where that particular person had been over 28 days and used that information to prosecute him. In contrast here, as discussed above, the telephony metadata program provides the NSA with information about calls between unidentified phone numbers, when the calls occurred, and how long the calls lasted. Thus, unlike in *Jones*, the NSA does not know the identity of anyone making or receiving the calls, and under the terms of the FISC's orders, cannot use the metadata to draw comprehensive maps of individuals' associations.

Even if it were otherwise, Plaintiffs have offered no evidence that the NSA or the FBI has ever viewed any metadata of their communications, let alone analyzed those data to map their associations. Plaintiffs not only have no support for their claim that the NSA programmatically collects subscriber-identifying information and analyzes it to create "richly detailed profile[s]" of persons living in the United States, they also have not shown that the NSA has done so with metadata of their calls. Even if the practices they hypothesize were taking place and violated individuals' legitimate expectations of privacy, the lack of any evidence that Plaintiffs have been the subject of such practices is fatal to their Fourth Amendment claim.

Plaintiffs' emphasis on the breadth of the telephony metadata program – i.e., the fact that under the program, telecommunications service providers provide the NSA with the call detail records of millions of Americans – does not alter that conclusion. The personal nature of Fourth Amendment rights precludes the argument that Plaintiffs' rights are violated by virtue of any collection or analysis of metadata pertaining to the calls of other persons. Nor is the fact that the collection is authorized for a period of 90 days material to this question. In *Miller*, 425 U.S. at 437-38, for example, the Court upheld a subpoena for all records of all bank accounts belonging to *Miller*, for a period of almost four months.

Given the conclusive, controlling effect of *Smith* on this case, there is no likelihood that Plaintiffs will succeed on the threshold question presented by their Fourth Amendment claim – whether a search occurred.

B. The Government's Acquisition of Metadata Is Reasonable

Even if collecting telephony metadata involved a Fourth Amendment "search" (it does not), the Fourth Amendment bars only "unreasonable" searches and seizures, whereas the collection of metadata at issue here is reasonable under the standard the Supreme Court applies to assess suspicionless searches that serve special government needs. That standard requires a court to balance "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Maryland v. King,* 133 S. Ct. 1958, 1970 (2013) (internal citation and quotation marks omitted). That balance overwhelmingly favors the Government here.

First, if, contrary to *Smith,* Plaintiffs could be said to have any Fourth Amendment privacy interest that is implicated by collection of non-content telephony metadata, that interest would be minimal. Moreover, the intrusion on that interest would be mitigated still further by the statutorily mandated restrictions on access to and dissemination of the metadata that are written into the FISC's Primary Order. *See King,* 133 S. Ct. at 1979 (safeguards limiting DNA analysis to identification information alone reduced any intrusion into privacy); *Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls,* 536 U.S. 822, 833 (2002) (restrictions on access to drug testing results lessened intrusion on privacy); *Vernonia Sch. Dist.,* 515 U.S. at 658 (intrusion of urine-testing on student athletes' privacy was significantly reduced by the fact that they were tested only for illegal drugs and not for any medical condition).

On the other side of the balance, the collection and analysis of telephony metadata promotes overriding public interests. The Government's interest in identifying and tracking terrorist operatives for the purpose of preventing terrorist attacks is a national security concern of overwhelming importance. Bulk collection of telephony metadata is a "reasonably effective means" of promoting the Government's national security objectives, inasmuch as accumulating metadata enhances the Government's ability to uncover and monitor unknown terrorist operatives who could otherwise elude detection. Given that the Government's collection of metadata serves exceedingly important public interests, with minimal, if any, intrusion on the privacy of telephone subscribers, it would be constitutional even if the Fourth Amendment's reasonableness standard applied.

* * * *

Plaintiffs' primary attack on the reasonableness of the program is to assert it is a "general warrant for the digital age." But the cases Plaintiffs rely on for this comparison -- Berger v. State of New York, 388 U.S. 41 (1967); United States v. U.S. Dist. Court (Keith), 407 U.S. 297 (1972); United States v. Tortorello, 480 F.2d 764 (2d Cir. 1973); United States v. Bobo, 477 F.2d 974 (4th Cir. 1973); United States v. Cafero, 473 F.2d 489 (3d Cir. 1973) -- are inapposite. Those cases involved the authorization of electronic eavesdropping on the contents of private conversations, a far greater intrusion on privacy interests than the collection of numerical telephony metadata devoid of any subscriber- identifying information or substantive content.

* * * *

Plaintiffs argue that the Supreme Court's special-needs analysis is inapplicable here, and that the warrant and probable-cause requirements apply instead. In particular, Plaintiffs argue that special-needs analysis applies only where the primary purpose of the government's action is "above and beyond criminal law enforcement," and where the special needs make the warrant and probable cause requirements "impracticable." But even accepting those propositions *arguendo*, both requirements are met here.

First, the undisputed purpose of the telephony metadata program is identifying unknown terrorist operatives and preventing terrorist attacks—forward-looking goals that fundamentally differ from ordinary criminal law enforcement, which focuses on solving crimes that have already occurred, not protecting public safety and national security. The Supreme Court has distinguished between domestic-security surveillance and surveillance in connection with ordinary crime: The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime . . . .

Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

Second, requiring individualized suspicion here would indeed be impracticable. The Government's interests in identifying unknown terrorist operatives and preventing terrorist attacks are great and cannot be as effectively achieved by requiring individualized suspicion to collect telephony metadata because such a requirement would not permit the type of historical analysis and contact chaining that the broader collection enables. Thus, given that the program might be entirely infeasible without the collection, it would certainly be "impracticable" to require individualized suspicion in this context.