**NSA Surveillance Under Section 215 of the PATRIOT Act**

Ashling Gallagher

Table of Contents

I. Section 215 – Arguments and Analysis2

A. Constitutional Claims3

1. First Amendment3

I. ACLU v. Clapper3

II. Klayman v. Obama5

III. Privacy and Civil Liberties Oversight Board Report5

2. Fourth Amendment7

I. ACLU v. Clapper7

II. Foreign Intelligence Surveillance Court Interpretation9

III. Obama Administration White Paper10

IV. Klayman v. Obama13

V. Privacy and Civil Liberties Oversight Board Report15

VI. The Third Party Doctrine17

VII. Smith v. Maryland: The Case That Established the Doctrine19

VIII. 215 Program: Seizure Under the Fourth Amendment?23

5. Fifth Amendment25

B. Statutory Claims25

1. ACLU26

2. Klayman30

3. Foreign Intelligence Surveillance Court Interpretation31

4. Obama Administration White Paper 37

5. Privacy and Civil Liberties Oversight Board Report40

Conclusion48

1. Government Surveillance Conducted under Section 215 –   
   Arguments and Analysis

Naturally, there are two camps on the Constitutional legality of bulk metadata collection under Section 215 of the PATRIOT Act; those who believe it violates the Constitution, and those do not. In determining the overall legality of the practice of bulk collection of U.S. persons’ telephony metadata (hereafter referred to as the “215 Program” or simply the “Program”), we must also examine whether or not the Program exceeds the authorities provided by the plain language of the statute itself.

This paper will proceed in two parts. Part one will address the constitutional claims brought in civilian lawsuits and reports commissioned by the administration, but will also contemplate the related question of the relevancy of the Third Party Doctrine in 21st Century life. Part two, will look at claims concerning the United States Government (hereafter called the “Government”) exceeding statutory limitations. Both sections will depend heavily on the ongoing lawsuits, *American Civil Liberties Union v. Clapper* and *Klayman v. Obama,* as well as the Privacy and Civil Liberties Oversight Board (“PCLOB” or the “Board”) January 23, 2014 report, but will also bring in commentary from governmental proceedings and reports. I will not draw from the President’s Review Group report dated December 12, 2013, as this report only made recommendations for policy changes and did not contemplate the legality or constitutionality of National Security Agency (NSA) practices.

**A. Constitutional Claims**

Claims of Constitutional violations under the Foreign Intelligence Surveillance Act (FISA) business records provision commonly known as section 215 (hereinafter referred to as “Section 215” or simply “215”) codified as 50 U.S.C. § 1861, have been the most prominent in national news media in allegations of Governmental overreach. Here, I will attempt to parse out the various accusations, defenses, and reasoning behind each of the arguments.

**1. First Amendment**

While most of the dialogue of the Constitutionality of the 215 Program centers on the Fourth Amendment’s promise of the right to privacy, both the American Civil Liberties Union (ACLU) and Larry Klayman, founder of the government watchdog group Freedom Watch, argue in their respective lawsuits filed against the Government in 2013 that the 215 Program violates, among other things, the First Amendment. The PCLOB also weighed in on the First Amendment implications exerted by the 215 Program and found that it does place pressure on that Amendment’s freedom of association.

I. ACLU v. Clapper

In *ACLU v. Clapper*, the ACLU argues, “[t]he fact that the government is collecting information is likely to have a chilling effect on people who would otherwise contact Plaintiffs.” While the Government contends that, “surveillance consistent with Fourth Amendment protection . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities.”[[1]](#footnote-1) Judge William Pauley, presiding over the case in the U.S. District Court for Southern District of New York, in citing *Clapper v. Amnesty International USA[[2]](#footnote-2)*, responds, “It is unnecessary to decide whether there could be a First Amendment violation in the absence of a Fourth Amendment violation because *Amnesty International* compels the conclusion that the bulk metadata collection does not burden First Amendment rights substantially . . . There must be a direct and substantial or significant burden on associational rights in order for it to qualify as substantial. Mere incidental burdens on the right to associate do not violate the First Amendment.” (internal quotations omitted).[[3]](#footnote-3) Judge Pauley additionally found that “Any alleged chilling effect here arises from the ACLU’s speculative fear that the Government will review telephony metadata related to the ACLU’s telephone calls. For telephony metadata to be used to identify those who contact Plaintiffs for legal assistance or to report human-rights or civil liberties violations it must actually be reviewed and the identities of the telephone subscribers determined. Fear that telephony metadata relating to the ACLU will be queried or reviewed or further investigated relies on a highly attenuated chain of possibilities. Such a fear is insufficient to create standing. Neither can it establish a violation of an individual’s First Amendment rights.” (internal quotations and citations omitted).[[4]](#footnote-4) Thus, Judge Pauley found that because it cannot be shown that the NSA or any other governmental agency actually queried and analyzed Plaintiffs’ *already collected* metadata, the 215 Program does not implicate the First Amendment’s freedom of association. Interestingly, Judge Pauley did not draw his line at the action of collection, rather at the action of analysis. He found that because there was a negligible likelihood that Plaintiffs’ metadata had been analyzed associational freedoms were not violated.

II. Klayman v. Obama

Klayman’s arguments before Judge Richard Leon of the U.S. District Court of the District of Columbia mirrored those of the ACLU’s in terms of the First Amendment claim: “[T]he mass surveillance program and the broad-sweeping Verizon Order exposes private and sensitive information regarding Plaintiffs’ communications and contacts, which consequently directly impacts their ability to continue their advocacy activities.”[[5]](#footnote-5) Judge Leon neither examines nor dismisses the First and Fifth Amendment claims brought by Klayman, but issued the preliminary injunction on the basis that the Plaintiff’s Fourth Amendment claims will succeed.

III. Privacy and Civil Liberties Oversight Board Report

The PCLOB in their report dated January 23, 2014 found that “By indefinitely collecting information about all Americans’ telephone calls, the NSA’s telephone records program clearly implicates the First Amendment freedoms of speech and association.”[[6]](#footnote-6) Having stated this, the Board goes on to examine whether or not the 215 Program’s chilling effects will be minimal or significant; if they find the effects to be significant the “exacting scrutiny” test is applied, “and the question becomes whether the government possesses a sufficiently important interest and employs means closely drawn to avoid unnecessary abridgement of associational freedoms.” (internal quotations omitted).[[7]](#footnote-7) As we know, the 215 Program does not collect telephony metadata on a specified target; rather the Program sweeps up a large cache of information regarding individuals who have no connection to terrorist or otherwise illicit activities. As such, “the NSA’s bulk collection of telephone records can be expected to exert a substantial chilling effect on the activities of journalists, protestors, whistleblowers, political activists, and ordinary individuals.”[[8]](#footnote-8) A more particularized investigation, on the other hand, does not exert the same pressures on the First Amendment’s right to freedom of association because “individuals can expect that their records will not be collected unless they are connected to a specific criminal or terrorism investigation.” The Board concludes that “the likely deterrence of these associational activities by the 215 bulk collection program rises to the level of a significant interference with the protected rights of political association, and thus the exacting scrutiny test should apply.”(internal quotations omitted).[[9]](#footnote-9) The Board concedes that the Government’s obligation to fight terrorism is a compelling reason to encroach upon Constitutionally protected areas, but they ultimately find “it doubtful that the NSA’s program satisfies the requirement that the program be drawn narrowly to minimize the intrusion on associational rights.”[[10]](#footnote-10)

**2. Fourth Amendment**

The Fourth Amendment guarantees “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”[[11]](#footnote-11)

I. ACLU v. Clapper

In analyzing the Fourth Amendment claims brought by the ACLU, Judge Pauley draws on the Supreme Court decisions of (i) *Katz v. United States*, which established that a “search” occurs when the Government violates a person’s “reasonable expectation of privacy”, and (ii) with greater importance, *Smith v. Maryland*, which established that individuals have no “legitimate expectation of privacy in information provided to third parties.”[[12]](#footnote-12) For Judge Pauley, the Government, and the Foreign Intelligence Surveillance Court (FISC), *Smith* is unequivocally the controlling case in assessing Fourth Amendment rights violations in bulk metadata collection under Section 215.

The ACLU, in their oral argument before Judge Pauley on November 22, 2013, ask (i) does long-term telephony metadata collection constitute a search for Fourth Amendment purposes and (ii) is such collection reasonable. They answer this by stating that yes telephony metadata collection does constitute a search (which search happens at the moment the information is obtained) because it places an extraordinary amount of information about Americans in the hands of the government and thus violates an individual’s reasonable expectation of privacy. And no, indefinite and pervasive collection of every Americans’ telephone call metadata for use at some point in the future is not reasonable. Judge Pauley responds to this by stating, “There is no reasonable expectation of privacy in this exact kind of information – dialed telephone numbers – and therefore the Fourth Amendment is not implicated here. Moreover, even if the Fourth Amendment were applicable, the production of metadata ordered by the FISC would satisfy the reasonableness standard applicable to suspicionless searches that serve special government needs, in which the intrusion on privacy interests is balanced against the Government’s interest in the search.”[[13]](#footnote-13) The Government, as defendant in this lawsuit, relies heavily on *Smith v. Maryland*, an argument Judge Pauley ultimately accepts. Pauley writing in his final decision to dismiss the case declared, “[T]he Supreme Court did not overrule *Smith*. And the Supreme Court has instructed lower courts not to predict whether it would overrule a precedent even if its reasoning has been supplanted by later cases . . . Telephones have far more versatility now than when *Smith* was decided, but this case only concerns their use as telephones. The fact that there are more calls placed does not undermine the Supreme Court’s finding that a person has no subjective expectation of privacy in telephony metadata.”[[14]](#footnote-14)

II. Foreign Intelligence Surveillance Court

Thanks to a treasure trove of recently declassified FISC opinions, we now know that the judges of that secretive court find the same. Judge Claire Eagan wrote in no uncertain language, “The Production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision *Smith v. Maryland*.” (internal citation omitted). This is the only basis upon which Judge Eagan finds the constitutionality of the 215 Program in her brief three-page treatment on the subject of the Fourth Amendment. She goes on, “[T]he Supreme Court concluded that a person does not have a legitimate expectation of privacy in telephone numbers dialed and, therefore, when the government obtained that dialing information, it was not a ‘search,’ and no warrant was required under the Fourth Amendment.” (internal quotations omitted).[[15]](#footnote-15) Note here that a discussion on whether or not the 215 Program could be considered a “seizure” under the Fourth Amendment didn’t enter into Judge Eagan’s analysis. Nor does she, or any other defender of the Program, contemplate the differences of the pen register employed in *Smith*, which *only* records the numbers dialed without revealing whether or not a connection was made, and the collection of telephony metadata under the 215 Program, which date stamps and records information regarding the numbers dialed and received, and the duration of both incoming and outgoing calls. This distinction is critical to our analysis here. For the pen register employed in *Smith* did not have the capabilities necessary to reveal the same type of personal information that we find the 215 Program is able to capture. We can take, for example, a scenario where for a period of weeks or months the same number repeatedly called a target, but only after 11 p.m. and for short two or three-minute phone calls. Then at some point a record shows that the target number called a local gynecologist office, perhaps to make an appointment for an examination. The analysts now know that the target number belongs to a female. The following week the target receives a call from the same gynecologist’s office and immediately thereafter has a long conversation with the late night caller after which she calls a facility that provides abortions. It is easy to see that developing and analyzing a pattern of calls allows the Government to glean information from data that taken singly would not reveal much at all. Under the construction established by the 215 Program, the Government is able to uncover much more than they would have were they only using a simple pen register.

III. Administration White Paper

The Obama Administration unsurprisingly took the same *Smith* approach as Judges Eagan and Pauley, but also went a bit farther in its assertion that the 215 Program is constitutional. In a white paper dated August 9, 2013, the Administration found that “[a] section 215 order for the production of telephony metadata is not a ‘search’ as to any individual because, as the Supreme Court has expressly held, participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone numbers dialed.”[[16]](#footnote-16) Interestingly, the white paper did not find the search component altered by the scale of the Program. Stating, “Collection of telephony metadata in bulk from telecommunications service providers under the program does not involve searching the property of persons making telephone calls. And the volume of records does not convert that activity into a search . . . No Fourth Amendment-protected interest is generated by virtue of the fact that the telephony metadata records of many individuals are collected rather than those of a single individual.”[[17]](#footnote-17) Perhaps this is true. But how does the scale of collection apply to the individual? A program of collecting telephony metadata has existed for a period of at least eight years since Section 215 was first used as a legal basis in 2006 for the Program. Prior to that, metadata collection was conducted under a highly classified directive issued by President George W. Bush in October 2001 following the September 11 attacks. This authorization directed the NSA to collect the contents of certain international communications and non-content information such as telephony and Internet metadata.[[18]](#footnote-18)

The Administration goes on to defend the 215 Program under the “reasonableness” standard, which requires, “a balancing of ‘the promotion of legitimate Governmental interests against the degree to which [the search] intrudes upon an individual’s privacy’.”[[19]](#footnote-19) Further, in the Government’s view, even if the 215 Program did involve a search under the meaning of the Fourth Amendment, “that search would satisfy the reasonableness standard that the Supreme Court has established in its cases authorizing the Government to conduct large-scale, but minimally intrusive, suspicionless searches.”[[20]](#footnote-20)

Also taken into consideration in this Administration white paper is the “exceedingly important objective” of “forward-looking prevention of the loss of life, including potentially on a catastrophic scale.”[[21]](#footnote-21) Here, the Government has balanced the “minimal, if any, Fourth Amendment intrusion” against the “exceptionally strong public interest in the prevention of terrorist attacks”[[22]](#footnote-22) and found in favor of continuing the 215 Program.

The balance, however, has recently tipped in the other direction. The majority of Americans disapprove of Governmental metadata collection and a number of experts have found that the Program has provided limited value in the ongoing effort to secure our nation.[[23]](#footnote-23) As a result of these revelations, President Obama is preparing legislation to end the practice of bulk metadata collection as it exists today.[[24]](#footnote-24) The working proposal, which has yet to go through Congressional approval, will end the NSA’s practice of systematic collection and storage of Americans’ calling data. Telecommunication companies will continue to collect and hold calling information as they normally would for business purposes but will not be required to retain such information any longer than the eighteen months currently mandated by federal law. The intelligence community will retain their capability of analyzing links between callers by moving to individualized and targeted metadata collection wherein each identified telephone number of interest will require a new kind of court order issued by the FISC. Once such a target is identified and approved for surveillance, telecommunication companies will provide telephony metadata to the appropriate intelligence agency on an ongoing daily basis along with any numbers within two hops of the original target.

IV. Klayman v. Obama

Judge Leon, of the U.S. District Court of the District of Columbia, in *Klayman* questioned the relevance of *Smith* in 21st Century communication. Leon’s findings were antithetical to those of Judge Pauley, the FISC and the Government; he wrote, “I am convinced that the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search.” Leon goes on to list the following reasons to account for those differences:

The short-term, forward-looking (as opposed to historical), and highly–limited data collection is what the Supreme Court was assessing in *Smith*. The NSA telephony metadata program, on the other hand, involves the creation and maintenance of a historical database containing *five years’* worth of data . . . Second, the relationship between the police and the phone company in *Smith* is nothing compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies . . . It’s one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government. Third, the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979 . . . Finally, *and most importantly,* not only is the Government’s ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people’s telephony metadata is much greater, as well. (emphasis in original).[[25]](#footnote-25)

Much like Judge Pauley, Judge Leon agrees that metadata itself is not changed since the 1970s, but adds “the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly*, what that information can tell the Government about people’s lives.” (emphasis in original).[[26]](#footnote-26) Leon eloquently writes, “the *Smith* pen register and the ongoing NSA Bulk Telephony metadata Program have so many significant distinctions between them that I cannot possibly navigate these unchartered Fourth Amendment waters using as my North Star a case that predates the rise of cell phones.”[[27]](#footnote-27) Judge Leon ultimately leaves his decision on the constitutionality of the 215 Program to another day stating only that it *probably* violates the Fourth Amendment. In the meantime, the judge has issued a preliminary injunction (which he immediately stayed pending the Government’s appeal) on the collection of Plaintiffs’ calling records and poses a question to which we are beginning see an answer. Judge Leon asks whether or not there is a legitimate societal expectation of privacy “that is violated when the Government, without any basis whatsoever to suspect [people] of any wrongdoing, collects and stores five years of their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval.”[[28]](#footnote-28)

V. Privacy and Civil Liberties Oversight Board Report

The PCLOB devote much of their treatment of the Fourth Amendment to the primary authority used by the Government as a constitutional defense of the 215 Program; those authorities are *Smith v. Maryland* and the Third-Party Doctrine. Both the case and doctrine are discussed in detail below. But first, it will be useful to examine some of the foundational considerations touched upon by the PCLOB in their report.

The PCLOB notes that Fourth Amendment interests are implicated when the Government carries out a warrantless search or seizure, but grant that it is sometimes difficult to determine what exactly constitutes a search or seizure. For the purpose of our discussion here, we will ask only ask if the 215 Program constitutes a ‘search’ under the Fourth Amendment. But at what point, if any, does that search occur? The PCLOB points out that telephony metadata records are obtained from the telecommunication companies with their assent and cooperation. The NSA does not tap into Americans’ computers, telephones, or homes in order to acquire the information. Nor does the NSA intercept communications in transit. For these reasons, among others, the Government asserts the 215 Program does not constitute a search under the meaning of the Fourth Amendment. If the Government is correct in this assumption, the reasonableness standard need not be met and the records may be collected without obtaining a warrant. But what constitutes a search?

Prior to the 1967 Supreme Court decision, *Katz v. United States,* the Constitution’s Fourth Amendment protections extended only to physical areas, such as one’s home or vehicle. *Katz* broadened the scope of the Fourth Amendment by establishing protections for people, not only places, and established a doctrine that includes protections to areas where there is a reasonable expectation of privacy. This standard must meet a “two-part test for determining whether government conduct qualifies as a search under the Fourth Amendment. This twofold requirement . . . requires first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable. Thus, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.” (internal quotations omitted).[[29]](#footnote-29) This test should render us better equipped to assess the Fourth Amendment pressures exerted on the American people by the 215 Program. But when it comes to a discussion of privacy rights in telephony metadata and the 215 Program, the two-part reasonableness requirement is in contention with another Fourth Amendment doctrine. *Smith v. Maryland*, the 1979 case that established the Third-Party Doctrine, states that individuals have no reasonable expectation of privacy in information voluntarily conveyed to a third party. To gain a better understanding of that doctrine as well as *Smith* and how they fit with a discussion of the 215 Program, we will take a closer look at both.

VI. The Third-Party Doctrine

Judge Pauley writes in his motion to dismiss the ACLU case, “[T]he business records created by Verizon are not ‘Plaintiffs’ call records.’ Those records are created and maintained by the telecommunications provider, not the ACLU. Under the Constitution, that distinction is critical because when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information.”[[30]](#footnote-30) This quotation highlights the unanswered questions that arise when we examine the interplay between ownership and the Third-Party Doctrine. We can then ask: does the concept of ownership and the application of the Third-Party Doctrine also extend to information collected and retained for medical purposes, email account information or content, credit card purchasing history, so on and so forth? Is it fair to assume that individuals have a reasonable expectation of privacy in the areas listed above? In a time when nearly all of our personal and professional activities engage a third party, can the Third-Party Doctrine still be consistent with one of the most cherished amendments of the Constitution?

The PCLOB questions the viability of the Third-Party Doctrine and outline in their report a number of critiques made by leading legal scholars. Criticisms of the Third-Party Doctrine began with *Smith* itself in the dissenting opinions of Justices Potter Stewart, Thurgood Marshall, and William Brennan*.* Under the Third Party Doctrine, the individual assumes the risk that personal information conveyed to a third party for business purposes may and can be disclosed to a governmental agency without the requirement of a warrant. Under this problematic view, an individual’s privacy rights and expectations are characterized as an absolute, where either the individual abstains entirely from engaging in activities that would communicate private information to a third party or the individual assumes the risks inherent in conducting personal and professional affairs through a third party. Justice Marshall took issue with this notion and opined in his dissent to *Smith*, “Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.”[[31]](#footnote-31)

More recently, Justice Sonya Sotomayor in her concurring opinion for *United States v. Jones* wrote, “[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectation, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.”[[32]](#footnote-32)

VII. Smith v. Maryland: The Case That Established the Doctrine

It bears on a conversation of the Third-Party Doctrine to examine also, at least superficially, the facts surrounding the case that established it. Michael Lee Smith, in March of 1976, robbed Patricia McDonough and subsequently made threatening and obscene phone calls to her home. Through descriptions provided by Ms. McDonough of her assailant’s vehicle, the police were able to trace the origins of the harassing phone calls to Mr. Smith’s home. At the request of police officers, but absent a warrant, the telephone company installed a pen register at the company’s central office. This device recorded, for a period of two days, *only* the telephone numbers dialed from Mr. Smith’s home. The pen register did not record incoming calls, whether or not a connection had been made, the time of day a call was placed, or the duration of a call. Shortly after its installation, the pen register revealed that a call was placed from Mr. Smith’s home to Ms. McDonough’s; based on this and other information a warrant was obtained and Mr. Smith’s property was searched. Sufficient evidence was secured from the property to make an arrest. Ms. McDonough identified Mr. Smith in a lineup and he was indicted in the Criminal Court of Baltimore for robbery.

Because a warrant was not obtained prior to the installation of the pen register the defense sought to suppress all evidence derived from the device. The motion to suppress evidence derived from the pen register was denied and Mr. Smith was sentenced to six years. With three judges dissenting, the Court of Appeals ultimately found that “there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment is implicated by the use of a pen register installed at the central offices of the telephone company.”[[33]](#footnote-33) Thus, no search was conducted and no warrant needed. Mr. Smith appealed to the Supreme Court.

In determining whether or not the pen register installed on Mr. Smith’s telephone line constituted a search under the Fourth Amendment, Justice Blackman in writing the opinion for the Supreme Court, first turned to the reasonable expectation of privacy test established by *Katz*. As discussed above, this touchstone of privacy must meet two criteria. First, did the individual conduct himself in a manner that “exhibited an actual (subjective) expectation of privacy”? And, secondly, is “the individual’s subjective expectation of privacy one that society is prepared to recognize as reasonable”? (internal quotations omitted).[[34]](#footnote-34)

Justice Blackman found that the pen register differed significantly from the listening device employed in *Katz*, “for pen registers do not acquire the *contents* of communications” (emphasis in original)[[35]](#footnote-35) and consequently rejects Mr. Smith’s claim that he had a reasonable expectation of privacy in the numbers dialed from his home. As Justice Blackman wrote, “we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial[.]”[[36]](#footnote-36) Secondly, the Justice found 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. This Court consistently has held that a person has no legitimate expectation of privacy in the information he voluntarily turns over to third parties.”[[37]](#footnote-37)

Justices Stewart, Marshall, and Brennan joined in dissent. Justice Stewart wrote, “The central question in this case is whether a person who makes telephone calls from his home is entitled to make a similar assumption about the numbers he dials . . . The numbers dialed from a private telephone – although certainly more prosaic than the conversation itself – are not without ‘content.’ Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person’s life.”[[38]](#footnote-38)

Justice Marshall’s view came from related angle. He wrote. “[E]ven assuming, as I do not, that individuals ‘typically know’ that a phone company monitors calls for internal reasons . . . it does not follow that they expect this information to be made available to the public in general or the government in particular . . . The crux of the Court’s holding, however, is that whatever expectation of privacy petitioner may in fact have entertained regarding his calls, it is not one society is prepared to recognize as reasonable.” (internal quotations omitted).[[39]](#footnote-39)

Thirty-five years since Justice Marshall penned this opinion his theory is finally being tested. Recent polls show that a majority of Americans do not approve of NSA surveillance[[40]](#footnote-40) and in all likelihood the 215 Program along with the Third-Party Doctrine will soon be scrutinized in Congress and before the Supreme Court.

VIII. 215 Program: Seizure Under the Fourth Amendment?

As a final note to our Fourth Amendment analysis, it might be interesting to pose the question of whether the 215 Program could constitute a seizure under the Fourth Amendment. There has been little-to-no discussion about whether or not the 215 Program could be considered a seizure; rather most cases and commentary assert that the Program violates the search component of the Fourth Amendment. Defenders say that Fourth Amendment privacy interests are not implicated by the *collection* of data and that the vast amount of oversight needed in order to search the already collected data provides the needed Constitutional protections.[[41]](#footnote-41) The only reasoning I can account for the omission is that perhaps it is generally accepted by both critics and advocates of the Program that business records are wholly owned by the companies who collect and store them. The government briefly argued this point in the preliminary statement in their motion to dismiss the ACLU case and later when arguing that the Third Party Doctrine applied.[[42]](#footnote-42) If the records are willingly handed over by companies to the Government, that is to say, the records have not been seized without consent, does this mean that the Government does not need a warrant or even a subpoena?

This begs the question of who *owns* metadata. Judge Pauley writes in his decision to dismiss the ACLU case, “[T]he business records created by Verizon are not ‘Plaintiff’s call records.’ Those records are created and maintained by the telecommunications provider, not the ACLU.”[[43]](#footnote-43) But couldn’t it be argued that because metadata are created by the individual – that the data would not exist if not for the individual ­– proprietary rights or interests should be extended to the individual?

The question of overall ownership of metadata might be an interesting one to ask. As metadata has proven to be financially profitable for marketing purposes and seized for surveillance purposes, the individual is left completely out of the loop.

**5. Fifth Amendment**

In *Klaymen v. Obama*, Plaintiffs assert that they have demonstrated a Fifth Amendment claim as they have, “an individual privacy interests in their internet communications online activities, which reveals sensitive, confidential information about their personal, political and religious activities and which Plaintiffs do not ordinarily disclose to the public or to the government . . . Plaintiffs’ Fifth Amendment constitutional rights were clearly violated the moments Defendants provided and the NSA obtained direct and unlimited access and authority to obtain vast quantities of communication records contained in Defendants’ vast databases, which inherently includes communication records belong to Plaintiffs.” [sic].[[44]](#footnote-44) I believe what Klayman is aiming at in his Fifth Amendment claim is the final line of the text which reads, “No person shall . . . be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”[[45]](#footnote-45) But it is a stretch to get there. Perhaps this is why the ACLU did not claim Fifth Amendment rights violation, Judge Leon did not address it in his decision, the PCLOB did not report on it, and it has gotten little or no lip service in the media.

B. Statutory Claims

Among the critiques of bulk metadata collection is one that stands out as being particularly tricky – that of exceeding statutory limitations. This section will examine the claims of statutory excesses and the responses of Judges Pauley and Leon as well as the findings of the PCLOB report.

1. ACLU v. Clapper

The ACLU outlines three reasons why the 215 Program is not authorized by the statute. First, they reject the notion that detailed call records concerning every call made in the United States over a seven-year period is relevant to an authorized investigation. Second, the 215 Program, “impermissibly transforms a statutory provision that was meant to permit the collection of existing records into one that permits the ongoing collection of records not yet in existence.” And third, “the program replaces judicial supervision over the acquisition of information with executive discretion over the later use of information. The mass call-tracking program is the product of statutory alchemy; there is simply no way to justify it without rewriting the statute altogether.”[[46]](#footnote-46)

The Government, however, maintains that Congress intended Section 215 to incorporate a broad meaning of relevance and point to areas in which relevancy has an even larger legal definition, such as official investigations, grand jury subpoenas, and civil proceedings.[[47]](#footnote-47) The Government’s reasoning for this broad definition of ‘relevant’ is based upon the analytic and technological capabilities of the NSA, not necessarily the letter of the law; “Collecting these data is necessary to the effective use of NSA analytical tools, which, when applied to the data, produce information that can help identify clandestine terrorist operatives or networks within the United States. That process is not feasible without bulk collection of the data, because NSA analysts cannot know in advance which of the many phone numbers obtained might have connections to known or suspected terrorists.”[[48]](#footnote-48) Even Judge Pauley found that, “This blunt tool works only because it collects everything.”[[49]](#footnote-49) This, as it turns out, may not be the case. President Obama has commissioned the Attorney General and senior intelligence officials to find an alternative that would eliminate bulk collection but maintain the NSA’s analytic capabilities. And Professor Edward W. Felton, Director of the Center for Information Technology Policy and professor of Computer Science and Public affairs at Princeton University, filed a declaration in connection with *ACLU* denouncing the need for bulk metadata collection and detailing a scheme that would allow the government to “perform three-hop analysis without first building its own database of every American’s call records.”[[50]](#footnote-50)

Further, the Government asserts that Congress was aware of the practice of bulk metadata collection but reauthorized Section 215 without change in 2010 and 2011. This is proof positive that the Program legitimately adheres to the statute. The Government goes on to say, “Imposing a limiting construction now on Section 215’s relevance standard that would prohibit bulk collection of telephony metadata would be contrary to the express understanding of the statute that Congress ratified on two separate occasions.”[[51]](#footnote-51) The Government adds that nothing in the text of Section 215 prohibits the collection of records as they are generated; a point that was, as we will see in subsection five below, vehemently rejected by the PCLOB*.* In defending the Program’s production of future records, the Government states, “That requested information is not created until after a FISC order has been rendered, and is produced on an ongoing basis, does not affect its basic character as ‘documents,’ ‘records,’ or ‘other tangible things’ subject to the production under the statute.”[[52]](#footnote-52)

Judge Pauley moves through a number of points to support his finding that the 215 Program does not exceed the limits of the statute. He begins by refuting the ACLU’s claim that mass metadata collection results in a large portion of irrelevant information. Pauley states, “That argument has no traction here” because the government needs to collect all data points, otherwise it cannot be certain that it has connected the pertinent ones.[[53]](#footnote-53) Interestingly, Pauley then elaborates on the FISC’s practice of issuing orders and minimization procedure to the NSA, but in the same breath states that Section 215 “contemplates that tangible items will be produced to the FBI[.]” He concludes that “Without those minimization procedures, FISC would not issue any section 215 orders for bulk telephony metadata collection”, but does not contemplate at all the anomaly inherent in a system that does not adhere to the statute’s clear directive that items will be produced to the *FBI*.[[54]](#footnote-54) This appears to be a fundamental breakdown in separation of powers, where the FISC has usurped the authority of Congress and determined that the tangible items received as a result of a production order will go *not* to the FBI, as stipulated by the statute, but instead to the NSA. It is unfathomable that Judge Pauley does not address this potentially grievous violation of the law.

Judge Pauley then goes on to elucidate the legal meaning of relevancy. He writes, “Relevance has a broad legal meaning. The Federal Rules of Civil Procedure allow parties to obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense. This rule has been 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. Tangible items are relevant under section 215 if they bear on or could reasonably lead to other matter that could bear on the investigation. Under Section 215, the Government’s burden is not substantial. The Government need only provide a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant.” (internal citations and quotations omitted).[[55]](#footnote-55) Observing that it is difficult to know which information will bear on an investigation or lead to useful counterterrorism information, Pauley notes that other courts have authorized large scale collection even when much of the information received will not bear on the investigation. Judge Pauley finds that the scale of metadata collection at present is necessary and appropriate; he states, “Armed with all the metadata, NSA can draw connections it might otherwise never be able to find.”[[56]](#footnote-56)

2. Klayman v. Obama

Judge Leon, in his memorandum opinion, does not interpret the plain meaning of Section 215 or FISA as a whole. Rather, he simply addresses the Plaintiffs’ claims that the 215 Program “exceeds the statutory authority granted by FISA’s tangible things provision and thereby violates the Administrative Procedure Act (APA).”[[57]](#footnote-57) More particularly, the Plaintiffs argue that (i) bulk records collected under Section 215 are not relevant to an authorized national security investigation and (ii) the FISC is not permitted to prospectively order the production of items not yet in existence. The Government responds that Congress impliedly precluded APA review of such claims and thus Judge Leon does not have subject matter jurisdiction over the statutory claim. Judge Leon writes, “The Government insists that two statutes ­– 50 U.S.C. § 1861, the “tangible things” provision of FISA itself, and 18 U.S.C. § 2712, a provision of the USA PATRIOT Act, codified in the Stored Communication Act (SCA) – *impliedly* preclude this Court’s review of Plaintiffs’ statutory APA claim . . . The text of Section 1861, and the structure and purpose of the FISA statutory scheme, as a whole, do indeed reflect Congress’s preclusive intent.”[[58]](#footnote-58) Because Section 215 outlines a detailed scheme where only recipients of production orders may appeal to the FISC, Judge Leon found that Congress intended the system to be closed to third parties and district courts. Judge Leon accepted the Government’s argument in this instance and found his court precluded from reviewing Plaintiffs’ APA claims.[[59]](#footnote-59) Rather disappointingly, Judge Leon issued no opinion as to whether or not he finds the 215 Program exceeds the limitations laid out by the statute; instead he simply stated that his court is unable to entertain such claims brought by Plaintiffs.

3. FISC Interpretation

Judge Eagan begins her statutory analysis of Section 215 ­(after an enumeration of the various requirements and minimization procedures associated with the issuance of a production order) with a study of what is considered to be the domestic criminal equivalent, the Stored Communications Act (SCA) 18 U.S.C. § 2703. Under this section 2703 of the SCA government officials are permitted to seek a court order to collect, *inter alia*, telephony metadata provided that the, “entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of . . . the records or other information sought are relevant and material to an ongoing criminal investigation.”[[60]](#footnote-60) Judge Eagan argues that this distinctly specific language - as compared to Section 215’s rather broad language - shows that Congress knew how to include a higher and more rigorous standard. Congress did not apply this same type of specified language when enacting the PATRIOT Act, thus Section 215 can be interpreted and applied more broadly. Further, Congress removed the provision in section 1861 (commonly known as Section 215) of FISA that required the FBI to show “specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.”[[61]](#footnote-61) While Section 215 imposes a lower burden on those seeking business records, it dictates that the FBI adhere to the minimization procedures as imposed by the FISC’s Primary Order. Section 2703 of the SCA, on the other hand, includes no such provision for minimization procedures. The minimization procedures employed in connection with Section 215 are considered to be backend protections as they are employed only after items have been collected and retained. Section 2703, on the other hand, uses frontend protections by requiring more rigorous levels of scrutiny in order to obtain information.

An additional safeguard included in Section 215 is a “substantial and engaging adversarial process,”[[62]](#footnote-62) which provides recipients (i.e. the telecoms companies and only those companies) a means to challenge the legality of production orders within a pool of FISC judges. Despite this provision, Judge Eagan writes in her August 29, 2013 Opinion, no production order recipient had yet challenged such an order to produce telephony metadata. This piece of information is an interesting inclusion in the Opinion. It can be assumed that Eagan wrote this as a means for quieting worried minds by implying that the production orders received to date were well within the confines of the statute and therefore challenging such orders was unnecessary. But instead it highlights the problems inherent in a system that allows only those who have no real interest at steak to bring a challenge against government orders.

Judge Eagan concludes that the two statutes should work in a “complementary manner.” She writes:

In the criminal investigation context, Section 2703(d) includes front-end protections by imposing a higher burden on the government to obtain the information in the first instance. On the other hand, when the government seeks to obtain the same type of information, but for a foreign intelligence purpose, Congress provided the government with more latitude at the production stage under Section 215 by not requiring specific and articulable facts or meeting a materiality standard. Instead, it imposed post-production checks in the form of mandated minimization procedures and structured adversarial process. This is a logical framework and it comports well with the Fourth Amendment concept that the required actual predicate for obtaining information in a case of special needs, such as national security, can be lower than for use of the same investigative measures for an ordinary criminal investigation.[[63]](#footnote-63)

Moving to the issue of relevancy, Judge Eagan writes that because terrorists use telephones to communicate and because bulk collection is necessary to employ the NSA’s analytic tools to uncover connections between those terrorists, the 215 Program meets the relevancy standard of the statute. In citing a previous FISC opinion, Judge Eagan found that this “showing of necessity led the Court to find that ‘the entire mass of collected metadata is relevant to investigating [international terrorist groups] and affiliated persons.’ . . . The analysis of past connection is only possible ‘if the Government has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related’.”[[64]](#footnote-64) Therefore, it is the NSA’s analytic tools and capabilities that dictate the standard of relevancy, not the value of the intelligence sought. Furthermore, Judge Eagan finds, Congress left the term “relevant” undefined in the statute; thus, Judge Eagan affirms that we are to apply the word’s ordinary meaning,[[65]](#footnote-65) which, as the Government believes, is very broad. Judge Eagan holds the Government to the low standard of relevancy and writes that “if it can demonstrate *reasonable grounds to believe* that the information sought to be produced has *some bearing* on its investigations of the identified international terrorist organizations.”[[66]](#footnote-66) (emphasis added). “Reasonable grounds to believe” is broad and “some bearing” is broader still; Judge Eagan affords the government greater flexibility than the statute allows. The judge balances three factors on the matter of relevancy; (i) “relevant” is in itself a broad term (ii) but this broad interpretation of a broad term is, however, off-set by the comprehensive minimization procedures dictated by the FISC’s Primary Order, and (iii) the NSA’s analytic tools require a massive scale of collection in order to make the information obtained *relevant*.

Judge Eagan deploys the “re-enactment doctrine” in her final defense of the FISC’s interpretation of Section 215. She reasons that Congress was made aware of the FISC’s statutory interpretation of Section 215 at the time of re-authorization but extended the sunset date all the same (current sunset date is set to expire June 1, 2015). Eagan writes, “When Congress subsequently re-authorized Section 215 without change, except as to the expiration date, the re-authorization carried with it this Court’s interpretation of the statute, which permits the bulk collection of telephony metadata under the restrictions that are in place. Therefore, the passage of the PATRIOT Sunsets Extensions Act provides a persuasive reason for this Court to adhere to its prior interpretations of Section 215.”[[67]](#footnote-67)

To this, the PCLOB (whose extensive statutory interpretation of Section 215 is detailed below) responds with a few points. First, when Section 215 reached its initial sunset dates (in 2010 and again in 2011) the FISC had not yet written a legal opinion expounding its interpretation of Section 215;[[68]](#footnote-68) the Court had simply been signing orders. Second, even if FBI applications and FISC production orders may be taken in conjunction and considered as an interpretation of 215, the majority of Congress was barred from reviewing such applications or orders. Only members on the Intelligence Committees were given access to the orders; the remaining congressmen and women had to seek information from those privileged members in order to learn of the workings of the 215 Program. Third, it is improper to apply the re-enactment doctrine in an analysis of Congressional intent when members of Congress may not consult with aids, outside counsel, and advocates in order to formulate a decision. Fourth, the statute was not “re-enacted” in 2010 and 2011, rather the expiration date was delayed by one year and four years respectively. Furthermore, even if each member of Congress was aware of the interpretation and we were able to call on the re-enactment doctrine in good faith, that still leaves the American public unaware of the Government’s interpretation and use of Section 215. The voting public is thus unable to hold accountable their congressmen in what is purportedly a participatory democracy.[[69]](#footnote-69) The PCLOB goes on to cite a number of cases that found the plain language of a statute shall trump faulty statutory interpretation. As there is no ambiguity in the plain meaning of Section 215 the re-enactment doctrine cannot be relied upon as a meaningful defense of the 215 Program.

4. Administration White Paper

It is telling that the first defense of the 215 Program presented by the Administration in its interpretation of the statute states, “The collection of telephony metadata in bulk . . . complies with Section 215, *as fourteen different judges of the FISC have concluded* in issuing orders[.]”[[70]](#footnote-70) (emphasis added). The second preliminary point of defense: “This collection, moreover, occurs only in a context in which the Government’s acquisition, use, and dissemination of the information are subject to strict judicial oversight and rigorous protections to prevent its misuse.”[[71]](#footnote-71) But why not begin the analysis at the very foundation – with the statute? Instead, to borrow a familiar term, the Administration’s analysis begins one hop from the law, with judicial review, and then two hops from the law, governmental oversight.

Digging a little deeper, the Government assures the reader that the FBI’s authorized investigations are conducted in accordance “with the *Attorney General’s Guidelines for Domestic FBI Operations*, U.S. Dep’t of Justice (2008)” and that the FBI is not only authorized to utilize every tool (namely Section 215) at its disposal but is *required* to do so.[[72]](#footnote-72) The difficulty here is – as we will see below ­– that investigations conducted under Section 215 are *not* done by the FBI, they are done by the NSA.

Moving to the issue of relevancy in an authorized investigation, much like the opinion from Judge Eagan, the White Paper states, “[I]n the circumstance where the Government has reason to believe that conducting a search of a broad collection of telephony metadata records will produce counterterrorism information – and that it is necessary to collect a large volume of data in order to employ the analytic tools needed to identify that information­ – the standard of relevance under Section 215 is satisfied.”[[73]](#footnote-73) Drawing on a volume of criminal and administrative case law, the White Paper builds an argument that permits bulk collection of individuals’ records even when it is known by government officials that a proportion of the information collected under Section 215 will have no bearing on an investigation. The White Paper states, “It is reasonable to conclude that Congress had that broad concept of relevance when it incorporated this standard into Section 215. The statutory relevance standard in 215, therefore, should be interpreted to be at least as broad as the standard of relevance that has long governed ordinary civil discovery and criminal and administrative investigations, which allows the broad collection of records when necessary to identify the directly pertinent documents.”[[74]](#footnote-74) Although, the White Paper concedes that the cited cases are not representative of the scale of collection at issue in the 215 Program, the Administration feels that “[the cases] do show that the ‘relevance’ standard affords considerable latitude, where necessary, and depending on the context, to collect a large volume of data in order to find the key bits of information contained within.” The White Paper asserts, nonetheless, that Congress intended Section 215 to be particularly broad.

On the issue of ongoing daily metadata collection, the White Paper maintains that nothing in Section 215, FISA as a whole, or the legislative history suggests that Congress intended FISC orders to be limited only to previously created records. The Paper states, “The fact that the requested information has not yet been created at the time of application, and that its production is requested on an ongoing basis, does not affect the basic character of the information as ‘documents,’ ‘records,’ or other ‘tangible things’ subject to production under the statute.” The White Paper adds that “[t]his type of prospective order also provides efficient administration for all parties involved ­– the Court, the Government, and the provider.”[[75]](#footnote-75)

5. PCLOB Report

Though the five members were split on some of the statutory conclusions, the PCLOB as a whole found that “Section 215 does not provide an adequate legal basis to support [the 215 Program].”[[76]](#footnote-76) The Board offers the following points upon which their decision was based: (i) production orders do not name a specific investigation conducted by the Federal Bureau of Investigations; (ii) wholesale collection of U.S. persons’ telephony metadata can in no way be considered “relevant”; (iii) prospective metadata collection ­­– as currently conducted under the 215 Program – lacks a foundation in the statute and circumvents other sections of FISA; (iv) the statute permits the FBI, not the NSA, to obtain tangible things for use in an investigation; and (v) the 215 Program violates the Electronic Communications Privacy Act. Each of these points will be taken individually below.

(i) “An Authorized Investigation”

The Board members begin with a look at the portion of the statute that states, “Each application under this section . . . shall include . . . a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation”.[[77]](#footnote-77) By scrutinizing the phrase “*an* authorized investigation”, which is in the singular, the Board concludes that the legislators intended that such an investigation must be a particularized investigation. As the 215 Program currently operates, FBI production orders do not specify a specific investigation; rather, the orders name multiple terrorist groups and states that they are all under investigation. The Board succinctly said of this type of general production order, “At its core, the approach boils down to the proposition that essentially all telephone records are relevant to essentially all international terrorism investigations.” In further support of their belief that Congress did not intend for such general orders, the Board points out that the statute specifically prohibits records collection for a “threat assessment,” which cannot be based on “arbitrary or groundless speculation.”[[78]](#footnote-78)

(ii) Relevance

In order to secure approval for a production request, the FBI must present to the FISC, “a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant* to an authorized investigation” (emphasis added). As we saw above and as the Board is inclined to point out, the FISC’s position is that all records are relevant because “bulk collection is necessary for NSA to employ [analytic] tools that are likely to generate useful investigative leads to help identify and track terrorist operatives” reasoning that “the subset of terrorist communication is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations[.]”[[79]](#footnote-79) The Board, however, contends that this interpretation of the statute is circular and renders the meaning of “relevant” to naught. “The implication of this reasoning is that if the government develops an effective means of searching through *everything* in order to find *something*, then *everything* becomes relevant to its investigation.” (emphasis in original).[[80]](#footnote-80)

The Board goes on to say that the Government’s “statement of facts” is limited to only two facts: that terrorists use telephones, and that it is necessary for NSA analysis to collect all calling records. “Neither of these facts shows why a particular group of telephone records may be relevant to an investigation, because the government has not limited its request to any particular group at all[.]” The Board observes that if all telephony metadata can be considered relevant under the above construction, then why not all metadata, or even all data.[[81]](#footnote-81)

(iii) Prospective Orders

Production orders are used to prospectively collect data on an ongoing daily basis for a period of ninety days, meaning that when the FISC grants a production order the records to be collected are not yet in existence. The Board points out that, under normal circumstances of discovery, when a subpoena is issued it requires the production of items already in the possession of the subpoena recipient and does not require the forfeiture of newly generated items over a set period of time as items are created.[[82]](#footnote-82) The Government, however, states, “nothing in the statute suggests that FISC orders may relate only to records previously created.”[[83]](#footnote-83) Three points are offered by the PCLOB to refute this claim.

First, the statute does not purport to authorize such orders, and case law involving the production of records in analogous contexts indicates that such authority cannot be inferred from statutory silence. Second, the text of Section 215 strongly suggests that it contemplates only the acquisition of items that already are in existence at the time the court issues an order. Third, interpreting Section 215 to permit the prospective collection of ­*telephone records­* renders superfluous another provision of FISA that directly authorizes such collection ­– circumventing the limitations associated with that other provision and violating the interpretive principle that one provision in a statute should not be construed to make another superfluous. (emphasis in original).[[84]](#footnote-84)

On this first point, the Board finds that the civil discovery cases presented by the Government in support of prospective ongoing record production are not comparable the 215 Program – that is to say they do not direct a party to produce on an on-going basis not yet created records.[[85]](#footnote-85) Rather, the Federal Rules of Civil Procedure, under the heading “Supplementing Disclosures and Responses”, allows for the *supplementation* to an original subpoena.

Additionally, the Board observes that Section 215 contains strongly suggestive language that points to the conclusion that the statute was written with the intention to limit production orders to records already in existence. For example, a FISC judge may issue an *ex parte* order “approving the *release of* tangible things” (emphasis in original). This word choice implies that the tangible things sought should exist at the time a production order is issued. Furthermore, production orders must include a date on which the tangible things sought must be produced; this provision is written in the singular, and does not seem to allow for ongoing daily metadata production for a period of ninety days. The Board members also look at what was not present in the statute, namely a provision that clearly illustrates the protocol for prospective production orders; limits and procedures are included when Congress intends for a statute to be used in such a manner.

Under section 1842 of FISA, the Attorney General or his designee “may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation.”[[86]](#footnote-86) The use of these devices will be limited to a period of time not exceeding ninety days, the results of which shall be furnished to a Government official on regular intervals over the life of the order.[[87]](#footnote-87) The Board argues “[c]onstruing Section 215 to permit ongoing acquisition of the very same data renders FISA’s pen register provision superfluous.”[[88]](#footnote-88)

(iv) FBI or NSA

While there were dissenting voices within the Board on the issue of which agency is authorized by the statute to receive telephony metadata from a telecommunication company, it ultimately found that “Section 215 expressly allows only the FBI to acquire records and other tangible things that are relevant to its foreign intelligence and counterterrorism investigations.”[[89]](#footnote-89) Indeed, the language in Section 215 creates a structure that would put the FBI in charge of the overall management of the records received under the statute. For example, the statute allows the FBI to submit a request to the FISC for the production of any tangible things. More pointedly, an application shall include “an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the *retention and dissemination by the Federal Bureau of Investigation* of any tangible things *to be made available to the Federal Bureau of Investigation.*”[[90]](#footnote-90) The “Use of Information” section of 215 also notes that “Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order . . . may be used and disclosed by Federal officers and employees . . . only in accordance with the minimization procedures adopted pursuant to subsection (g). No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this subchapter shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.”[[91]](#footnote-91) The minimization procedures noted in this provision specifically name the FBI as responsible for retention and dissemination of any tangible things.

But under current procedures, the FBI becomes involved in an investigation only after the NSA has collected and analyzed metadata produced as a result of an order. If the NSA discovers connections between phone numbers associated with illicit activities, that information is handed off to the FBI (or other agencies within the intelligence community) for further investigation. NSA analysts must abide the minimization and dissemination procedures as dictated by the FISC production order - not the minimization procedures outlined in the statute - before the information is released to the appropriate intelligence agency.[[92]](#footnote-92)

Ms. Elisebeth Collins Cook, one of two dissenting voices on the Board, felt that the 215 Program is authorized under the terms of the statute. During the January 29,2014 Senate Judiciary Committee hearing she stated, “The Board has concluded that Section 215 prohibits providers from producing documents to the NSA instead of the FBI . . . but if you read Section 215 where it talks about production of tangible things there is no requirement whatsoever that it be made to the FBI. The majority has instead cobbled together this prohibition and wrested its legal analysis on this prohibition that does not appear on the face of the statute.”[[93]](#footnote-93) Ms. Collins Cook is correct in saying that nothing in the statute explicitly prohibits the NSA from receiving items under a production order. But, neither does the statute expressly state to whom exactly the items shall be produced. Instead, there is ample surrounding language that a good faith reading of the statute would result in the conclusion that Congress intended the FBI to avail of the allowances of Section 215.

Certainly, it does not appear that the statute allows for the NSA to obtain and retain the tangible things received as a result of a production order to the extent that it currently does. This raises a reasonable question; to what extent is the FBI legally permitted to outsource its signals intelligence work to other agencies or government contractors? Indeed, the FBI should be permitted to benefit from the technological expertise of the NSA. It is in the interest of citizens and governments alike for the intelligence community to coordinate investigations across agencies. But they should do so by using clearly drawn legal boundaries. There is a confounding interplay between the FBI, the NSA, and the FISC at issue here, which raises greater questions of how governmental institutions in national security should interact with one another.

(v) Electronic Communications Privacy Act

Not only does the Board find that the 215 Program is not grounded in FISA, but it also concludes the Program violates the Electronic Communications Privacy Act (ECPA). They write, the “ECPA limits the circumstances under which a telephone company . . . may divulge records about its customers. Apart from certain enumerated exceptions, a provider ‘shall not knowingly divulge a recorded or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity.’ These enumerated exceptions, among others, include situations in which the government secures a warrant, obtains a court order under ECPA, or utilizes a subpoena.”[[94]](#footnote-94) None of the exceptions, however, include orders issued under Section 215.

FISC initially addressed the tensions between the ECPA and Section 215 in 2008 and ultimately concluded that because there is an exception for national security letters, it would be “anomalous” for Congress to exclude orders written under Section 215; thus the FISC inferred an implicit exception under the ECPA for 215 orders.[[95]](#footnote-95) Because of Section 215’s generality and the ECPA’s specificity, the Board feels that the ECPA should be the ruling statute in this case. Further evidencing their conclusion that Section 215 cannot be considered the ruling statute, the Board points to the legislative history surrounding the enactment of the PATRIOT Act, which created Section 215 but also amended the ECPA in ways that would allow telecommunication companies to provide records to the government. This amendment to the ECPA did not include a provision to allow the disclosure of calling records pursuant to a FISC order. The Board urges that this omission should be respected.[[96]](#footnote-96)

Conclusion

To paraphrase PCLOB member Rachel Brand, reasonable people will disagree. The issue of government surveillance, terrorism, and national security is not straightforward and juggling the myriad pieces in our effort to ensure security is incredibly difficult. Whatever reasons may account for the catastrophic intelligence failure of 9/11, we as a nation cannot compromise the very fundamental tenets upon which this nation was built. We have entered a new phase in history and warfare. Our enemy is elusive and our intelligence capabilities limitless. The coming decades will test our intelligence officers, citizens, and legislators alike as we attempt to find both security and privacy.

1. Memorandum & Order at 45, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-1)
2. The Supreme Court held in *Amnesty* that attorneys and advocacy groups could not challenge the FISA Amendment Act in court because they could not show that they were subject to surveillance. This case predates the unauthorized disclosures of June 2013. As such there was no evidence of surveillance at that time. [↑](#footnote-ref-2)
3. Memorandum & Order at 46, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013), in citing *Tabbaa v. Chertoff* 509 F.3d at 101 [↑](#footnote-ref-3)
4. Memorandum & Order at 46, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-4)
5. *Klayman v. Obama*, No. 13-0851, Plaintiffs’ Reply in Support of Their Motions for Preliminary Injunction, at 17. Retrieved at http://www.freedomwatchusa.org/pdf/131125-Reply%20Brief.pdf [↑](#footnote-ref-5)
6. PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court,* 23 Jan. 2014, at 134. Hereafter cited as “PCLOB Report”. Retrieved at: <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf> [↑](#footnote-ref-6)
7. *Id.*, at 135 [↑](#footnote-ref-7)
8. *Id.*, at 135 [↑](#footnote-ref-8)
9. PCLOB Report, at 135 [↑](#footnote-ref-9)
10. *Id.*, at 135 [↑](#footnote-ref-10)
11. U.S. Const. amend.IV. [↑](#footnote-ref-11)
12. Memorandum & Order at 38-39, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-12)
13. Memorandum & Order at 42, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-13)
14. Memorandum & Order at 43-44, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-14)
15. FISC court opinion, Eagan, C. at, 7-8; Docket number 13-109 [↑](#footnote-ref-15)
16. Obama Administration White Paper, at 19; 13 Aug. 2013. Hereafter cited as “Obama Administration White Paper”. Retrieved from <https://www.aclu.org/files/natsec/nsa/20130816/Section%20215%20-%20Obama%20Administration%20White%20Paper.pdf> [↑](#footnote-ref-16)
17. *Id.*, at 20 [↑](#footnote-ref-17)
18. PCLPB Report, at 37 [↑](#footnote-ref-18)
19. Obama Administration White Paper, at 21; in citing *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) [↑](#footnote-ref-19)
20. *Id.*, at 21 [↑](#footnote-ref-20)
21. *Id.*, at 21 [↑](#footnote-ref-21)
22. *Id.*, at 21 [↑](#footnote-ref-22)
23. See e.g. PCLOB Report, beginning at144; “Liberty and Security in a Changing World: Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies” 12 Dec. 2013, at 104. Retrieved from <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> [↑](#footnote-ref-23)
24. See <http://www.washingtonpost.com/world/national-security/bipartisan-house-bill-would-end-nsas-bulk-collection-of-americans-phone-data/2014/03/24/f8fac99a-b391-11e3-8020-b2d790b3c9e1_story.html> and <http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html> [↑](#footnote-ref-24)
25. Memorandum Opinion at 47-49, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013) [↑](#footnote-ref-25)
26. *Id.* at 51-52 [↑](#footnote-ref-26)
27. Memorandum Opinion at 55, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013) [↑](#footnote-ref-27)
28. *Id.* at 56 [↑](#footnote-ref-28)
29. PCLOB Report, pg 109; in citing Justice John Marshall Harlan’s concurring opinion in *Katz,* 389 U.S. at 361 [↑](#footnote-ref-29)
30. Memorandum & Order at 42, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-30)
31. PCLOB Report, at 118, in citing *Smith, 442* U.S. at 749 (Marshall, J., dissenting) [↑](#footnote-ref-31)
32. *United States v. Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) [↑](#footnote-ref-32)
33. *Smith v. Maryland*, 442 U.S. 735 (1979) at 738 [↑](#footnote-ref-33)
34. *Id.* at 740 [↑](#footnote-ref-34)
35. *Id.* at 741 [↑](#footnote-ref-35)
36. *Smith v. Maryland*, 442 U.S. 735 (1979) at 742 [↑](#footnote-ref-36)
37. *Id.* at 743-4 [↑](#footnote-ref-37)
38. *Id.* at 747-8 [↑](#footnote-ref-38)
39. *Smith v. Maryland*, 442 U.S. 735 (1979) at 749 [↑](#footnote-ref-39)
40. See e.g. <http://thehill.com/blogs/blog-briefing-room/195931-poll-public-turning-against-nsa-practices> and <https://www.eff.org/deeplinks/2013/10/polls-continue-show-majority-americans-against-nsa-spying> [↑](#footnote-ref-40)
41. Some of the oversight measures include; the reasonable articulable standard, identities are not revealed when querying the database - only numbers, rigorous minimization procedures, FISC provides judicial oversight and Congress (in reauthorizing the surveillance program) provides legislative oversight. [↑](#footnote-ref-41)
42. Memorandum & Order at 12 and 43, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-42)
43. *Id.* at 42 [↑](#footnote-ref-43)
44. Plaintiffs’ Reply in Support of Their Motions for Preliminary Injunction at 18-19, *Klayman v. Obama*, No. 13-0852 [↑](#footnote-ref-44)
45. U.S. Constitution, V amendment [↑](#footnote-ref-45)
46. Memorandum & Order at 8-9, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Aug. 26, 2013) [↑](#footnote-ref-46)
47. Defendants’ Memorandum of Law in Support of Motion to Dismiss the Complaint at 21, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Aug. 26, 2013) [↑](#footnote-ref-47)
48. Defendants’ Memorandum of Law in Support of Motion to Dismiss the Complaint at 29, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Aug. 26, 2013) [↑](#footnote-ref-48)
49. Memorandum & Order at 42, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-49)
50. Supplemental Declaration of Professor Felton at 3, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Oct. 25, 2013); retrieved from <https://www.aclu.org/files/assets/2013.10.25_aclu_pi_reply_-_suppl_felten_decl.pdf> [↑](#footnote-ref-50)
51. Defendants’ Memorandum of Law in Support of Motion to Dismiss the Complaint at 28, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Aug. 26, 2013) [↑](#footnote-ref-51)
52. *Id.* at 30 [↑](#footnote-ref-52)
53. Memorandum & Order at 32, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-53)
54. Memorandum & Order at 33, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013). The full passage reads, “And it was the FISC that limited the NSA’s production of telephony metadata to the FBI. While section 215 contemplates that tangible items will be produced to the FBI, FISC orders require that bulk telephony metadata be produced directly – and only – to the NSA. And the FISC forbids the NSA from disseminating any of that data until after the NSA has identified particular telephony metadata of suspected terrorists. Without those minimization procedures, FISC would not issue any section 215 orders for bulk telephony metadata collection.” [↑](#footnote-ref-54)
55. Memorandum & Order at 33, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Dec. 27, 2013) [↑](#footnote-ref-55)
56. *Id.* at 35 [↑](#footnote-ref-56)
57. Memorandum Opinion at 23-24, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013) [↑](#footnote-ref-57)
58. Memorandum Opinion at 25, *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013) [↑](#footnote-ref-58)
59. *Id.* at 24 [↑](#footnote-ref-59)
60. SCA 18 U.S.C. § 2703(d) [↑](#footnote-ref-60)
61. Amended Memorandum Opinion at 13, *In re Application of the Federal Bureau of Investigation for an order Requiring the Production of Tangible Things,* No. 12-109 (FISA Ct.Aug. 29, 2013). In citing FISA 50 U.S.C. § 1861(b)(2)(B) prior to the PATRIOT Act [↑](#footnote-ref-61)
62. Amended Memorandum Opinion at 15, *In re Application of the Federal Bureau of Investigation for an order Requiring the Production of Tangible Things,* No. 12-109 (FISA Ct.Aug. 29, 2013) [↑](#footnote-ref-62)
63. Amended Memorandum Opinion at 16-17, *In re Application of the Federal Bureau of Investigation for an order Requiring the Production of Tangible Things,* No. 12-109 (FISA Ct.Aug. 29, 2013) [↑](#footnote-ref-63)
64. *Id.* at 20 & 22 [↑](#footnote-ref-64)
65. The Oxford English Dictionary defines relevant as, “Bearing on or connected with the matter in hand; closely relating to the subject or point at issue; pertinent to a specified thing.” This definition seems to be more restrictive than the one currently used under the 215 Program. After all, can it be possible that the mass of the telephony metadata is ‘closely relating’ or ‘pertinent’ to an authorized investigation? [↑](#footnote-ref-65)
66. Amended Memorandum Opinion at 19, *In re Application of the Federal Bureau of Investigation for an order Requiring the Production of Tangible Things,* No. 12-109 (FISA Ct.Aug. 29, 2013) [↑](#footnote-ref-66)
67. Amended Memorandum Opinion at 27-28, *In re Application of the Federal Bureau of Investigation for an order Requiring the Production of Tangible Things,* No. 12-109 (FISA Ct.Aug. 29, 2013) [↑](#footnote-ref-67)
68. Judge Eagan’s Opinion detailed above is regarded as the first FISC opinion interpreting the statute. Some have even charged that Judge Eagan’s Opinion was written with the intention to ultimately declassify for release to the public, which was done on September 17, 2013, less than one month after the opinion was penned. See <http://www.nytimes.com/2013/09/18/us/opinion-by-secret-court-calls-collection-of-phone-data-legal.html> and http://www.lawfareblog.com/2013/09/congress-has-no-clothes-a-quick-and-dirty-summary-of-the-new-fisc-opinion/ [↑](#footnote-ref-68)
69. PCLOB Report, at 96 [↑](#footnote-ref-69)
70. Obama Administration White Paper, at 5 [↑](#footnote-ref-70)
71. *Id.* at 6 [↑](#footnote-ref-71)
72. Obama Administration White Paper, at 6-7 [↑](#footnote-ref-72)
73. *Id.*, at 8-9 [↑](#footnote-ref-73)
74. Obama Administration White Paper, at 11 [↑](#footnote-ref-74)
75. *Id.*, at 16 [↑](#footnote-ref-75)
76. PCLOB Report, at 57 [↑](#footnote-ref-76)
77. *Id.*, at 58-9 [↑](#footnote-ref-77)
78. PCLOB Report, at 60 [↑](#footnote-ref-78)
79. *Id.*, at 61 [↑](#footnote-ref-79)
80. PCLOB Report, at 62 [↑](#footnote-ref-80)
81. *Id.*, at 63 [↑](#footnote-ref-81)
82. *Id.*, at 81 [↑](#footnote-ref-82)
83. Obama Administration White Paper, at 16 [↑](#footnote-ref-83)
84. PCLOB report, at 82 [↑](#footnote-ref-84)
85. *Id.*, at 83 [↑](#footnote-ref-85)
86. 50 U.S. Code § 1842(a)(1) [↑](#footnote-ref-86)
87. 50 U.S. Code § 1842(f) and (g) [↑](#footnote-ref-87)
88. PCLOB report, at 86 [↑](#footnote-ref-88)
89. PCLOB report, at 88 [↑](#footnote-ref-89)
90. 50 U.S. Code § 1861(b)(2)(B) (emphasis added) [↑](#footnote-ref-90)
91. 50 U.S. Code § 1861(h) [↑](#footnote-ref-91)
92. Obama Administration White Paper, at 4 [↑](#footnote-ref-92)
93. Senate Judiciary Committee Hearing, 29 January 2014, at 1:17:00, retrieved from <http://www.senate.gov/isvp/?comm=judiciary&type=live&filename=judiciary021214> [↑](#footnote-ref-93)
94. PCLOB report, at 91; citing 18 U.S. Code §§ 2702(a)(3), 2702(c), 2703(c) [↑](#footnote-ref-94)
95. *Id.*, at 92. The Board notes that Judge Pauley adopted the FISC’s reasoning in the *ACLU* decision. [↑](#footnote-ref-95)
96. *Id.*, at 93 [↑](#footnote-ref-96)