Berkeley Technology Law Journal

Volume 29
Issue 4 *Annual Review 2014*

Article 19

8-1-2014

NSA Metadata Collection and the Fourth Amendment

Joseph D. Mornin

Link to publisher version (DOI)
https://doi.org/10.15779/Z38XX3T

NSA METADATA COLLECTION AND THE FOURTH AMENDMENT

Joseph D. Mornin[†]

On June 5, 2013, the *Guardian* published a classified order from the U.S. Foreign Intelligence Surveillance Court ("FISC"), which it obtained from former government contractor Edward Snowden.[1] The order compelled Verizon to deliver millions of records of its customers' telephone calls to the National Security Agency ("NSA").[2]

Further disclosures continue to reveal the scope of the NSA surveillance program and its legal justifications. In response, the federal government has declassified several additional documents, many of them heavily redacted.[3] Together, the materials show that since September 11, 2001, the NSA has collected and analyzed vast amounts of U.S. internet and telephone communications.

Many of the documents published thus far relate to the NSA's collection of phone call records,[4] known as "telephony metadata."[5] Metadata includes

---

† J.D. Candidate, 2015, University of California, Berkeley, School of Law.

1. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also* Peter Maass, *How Laura Poitras Helped Snowden Spill His Secrets*, N.Y. TIMES (Aug. 13, 2013), http://www.nytimes.com/2013/08/18/magazine/laura-poitras-snowden.html.

2. Greenwald, *supra* note 1.

3. *See, e.g.*, Jane Chong, *The Latest NSA Documents III: The Government Responds*, LAWFARE BLOG (Sept. 11, 2013), http://www.lawfareblog.com/2013/09/the-latest-nsa-documents-iii-the-government-responds.

4. Further disclosures continue to reveal new facets of the NSA's surveillance activities. For instance, at the time of this writing, the *Washington Post* reported that the NSA collects nearly five billion records per day about the locations of cellphones around the world (although not in the United States). *See* Barton Gellman and Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html. So far, the Obama administration has publicly offered a legal rationale only for the telephony metadata collection program.

5. Secondary Order at 2, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services, Inc., No. BR 13-80 (FISC Apr. 25,

information about a phone call—who, where, when, and how long—but not the content of the conversation.[6] The FISC order to Verizon, for instance, compelled disclosure of "all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[7] Government officials have acknowledged that the FISC has issued similar orders to the other major U.S. telephone carriers, suggesting that the NSA gathers metadata from virtually every American phone call.[8]

The legal justification for the government's bulk metadata collection rests on Section 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act").[9] In addition, the government has argued that the surveillance program is consistent with the First and Fourth Amendments.[10] The FISC, which operates in secret, has approved well over ninety-nine percent of the government's requests.[11]

2013) [hereinafter Verizon Order], *available at* http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

6. *Id.* The FISC order indicates that the call records do not include the names of customers, but NSA Director Keith Alexander has written that the agency can easily correlate phone numbers with caller identities. *See* Kurt Opsahl, *Gems Mined from the NSA Documents and FISA Court Opinions Released Today*, EFF DEEPLINKS BLOG (Sept. 10, 2013), https://www.eff.org/deeplinks/2013/09/gems-mined-nsa-docs-released-today.

7. Verizon Order, *supra* note 5, at 2.

8. Siobhan Gorman et al., *U.S. Collects Vast Data Trove*, WALL ST. J. (June 7, 2013), http://online.wsj.com/article/SB10001424127887324299104578529112289298922.html ("[E]very time the majority of Americans makes a call, NSA gets a record of the location, the number called, the time of the call and the length of the conversation.").

9. The Uniting and Strengthening American by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. *See* Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act 2 (Aug. 9, 2013), *available at* http://big.assets.huffingtonpost.com/Section215.pdf [hereinafter Administration White Paper].

10. *Id.*

11. *See Foreign Intelligence Surveillance Act Court Orders 1979–2012*, EPIC, https://epic.org/privacy/wiretap/stats/fisa_stats.html (last updated May 4, 2012) (noting that the FISC has rejected eleven out of approximately thirty-five thousand requests since 1978). *But see* Letter from Judge Reggie B. Walton, FISC, to Senator Patrick J. Leahy, Chairman, Senate Comm. on the Judiciary (July 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/honorable-patrick-leahy.pdf (contesting the view of the court as a "rubber stamp," noting that in some cases the FISC has required the government to amend its requests before the FISC will issue an order).

The Snowden disclosures have sparked public controversy and provoked constitutional challenges in federal courts.[12] This Note aims to contribute to that debate in two ways. First, it collects information scattered across numerous government documents—some of which Edward Snowden has disclosed, others of which the government has declassified—to tell the story of the NSA's telephony metadata collection program since September 11, 2001. Second, it assesses the government's argument that call record data lacks protection under the Fourth Amendment. In particular, this Note asks whether the NSA's prolonged collection of telephony metadata is consistent with Fourth Amendment doctrine in light of the U.S. Supreme Court's 2012 decision in *United States v. Jones*, in which the Court raised serious doubts about the constitutionality of unfettered metadata collection and analysis.[13]

Part I reviews the development of the NSA surveillance program and its legal basis since September 11, 2001.

Part II explores the government's Fourth Amendment arguments. The government relies on the third-party doctrine, first developed in *United States v. Miller*, which held that there are no Fourth Amendment protections for information voluntarily disclosed to third parties.[14] In particular, the government relies on *Smith v. Maryland*, which held that callers lack a Fourth Amendment interest in the numbers they dial because they voluntarily turn over that data to their telephone providers.[15] Since callers have no right to privacy in their metadata, the government argues, the NSA can gather, store, and analyze any amount of telephony metadata over any period of time.[16]

Part III addresses the details of the telephony metadata gathered under the NSA program. Research in computer science shows how metadata analysis can reveal a wide range of sensitive information. In the age of "big data," the line between "metadata" and "content" tends to blur, raising doubts about *Smith*'s holding that metadata categorically lacks any Fourth Amendment protection.

---

12. *See Obama administration drowning in lawsuits filed over NSA surveillance*, RT.COM (July 16, 2013), http://rt.com/usa/snowden-leaks-surveillance-suits-174.

13. United States v. Jones, 132 S. Ct. 945 (2012).

14. United States v. Miller, 425 U.S. 435 (1976).

15. Smith v. Maryland, 442 U.S. 735 (1979); *see also* Administration White Paper, *supra* note 9, at 19–20.

16. Administration White Paper, *supra* note 9, at 20 ("Although the telephony metadata obtained through Section 215 includes, in addition to the numbers dialed, the length and time of the calls and other similar dialing, routing, addressing, or signaling information, under the reasoning adopted by the Supreme Court in Smith, there is no reasonable expectation of privacy in such information, which is routinely collected by telecommunications service providers for billing and fraud detection purposes.").

Part IV assesses the government's Fourth Amendment argument in light of *United States v. Jones*.[17] This Note argues that the government's reasoning is consistent with the Supreme Court's precedent in *Smith*, since the Court has yet to revise its position on Fourth Amendment protections for third-party records. Yet, the NSA's large-scale metadata collection raises a familiar Fourth Amendment dilemma: as new technology makes it easier for the government to detect and apprehend criminals, it also sharpens threats to personal privacy and disrupts the balance of power between citizens and government. *Jones* signals the possibility that the Court is willing to revisit the third-party doctrine under new technological circumstances. The *Jones* Court based its holding on the fact that officers trespassed onto the suspect's property, avoiding the question of whether a privacy invasion had occurred. But five concurring Justices argued that data collection in the aggregate implicates Fourth Amendment concerns, even if the individual data points lack protection. Under the theory of these five Justices, the NSA's surveillance program tests the limits of current Fourth Amendment doctrine.

I. NSA SURVEILLANCE AFTER 9/11

This Part reviews the history and scope of the NSA's metadata collection activities since the terrorist attacks of September 11, 2001 ("9/11"). The NSA program initially operated under a series of presidential authorizations, known collectively as the President's Surveillance Program ("PSP").[18] After several White House officials questioned the PSP's legal foundations, the authority for the NSA's activities shifted to secret orders from the FISC.[19] The FISC orders have compelled American telephone companies to turn over extensive call records to the NSA for storage and analysis.

A. THE PRESIDENT'S SURVEILLANCE PROGRAM

In the days following the 9/11 attacks, NSA Director General Michael Hayden implemented an emergency surveillance program to monitor communications involving phone numbers associated with foreign terrorists.[20] Shortly afterward, the White House began advocating for a permanent expansion of the NSA's authority to conduct domestic surveillance. General Hayden prepared a report for Vice President Cheney's

17. *Jones*, 132 S. Ct. 945.

18. *See* ST-09-0002 Working Draft, Office of the Inspector General 20 (Mar. 24, 2009), *available at* https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf [hereinafter IG Report #1].

19. *See id.* at 37.

20. *See id.* at 3.

office on existing gaps in the NSA's operations.[21] He emphasized that "access to metadata of communications with one end in the United States would significantly enhance NSA's analytic capabilities."[22]

On October 4, 2001, Vice President Cheney's legal counsel, David Addington, drafted a presidential authorization granting the expanded authority General Hayden had requested.[23] The initiative, known as the President's Surveillance Program, allowed surveillance of international terrorism targets for thirty days.[24] It authorized the NSA to collect[25] four types of information—telephony content, telephony metadata, internet content, and Internet metadata—if (1) there was probable cause that one party was in Afghanistan or involved with international terrorism, (2) at least one party was outside the United States, or (3) neither party was a U.S. citizen.[26] The project relied on fifty dedicated servers to store and process data.[27] Its initial budget was $25 million.[28]

The presidential authorizations underlying the PSP expanded the NSA's authority to include surveillance of domestic communications. Prior to the PSP, the NSA lacked the authority to collect metadata from communications in which one end—the recipient address of the email or the phone number

21. *See id.* at 4.
22. *See id.*
23. *Id.* at 1–2, 8.
24. *See id.* at 7.
25. There is controversy around the definition of "collection" in the surveillance context. According to Director of National Intelligence James Clapper, the NSA's efforts to gather call record data is not "collection." *See DNI James Clapper Interview with Andrea Mitchell, NBC News Chief Foreign Affairs Correspondent*, IC ON THE RECORD (June 8, 2013), http://icontherecord.tumblr.com/post/57729424567/dni-james-clapper-interview-with-andrea-mitchell. Similarly, Department of Defense regulations indicate that information "shall be considered as 'collected' only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties." *See* DEPARTMENT OF DEFENSE, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (Dec. 1982), *available at* http://www.fas.org/irp/doddir/dod/d5240_1_r.pdf. Privacy advocates have accused the Obama administration of using the term evasively. *See, e.g.*, Philip Bump, *The Most Recent Updates to Your NSA Surveillance Dictionary*, ATLANTIC WIRE (Aug. 8, 2013), http://www.theatlanticwire.com/politics/2013/08/most-recent-updates-your-nsa-surveillance-dictionary/68140. However, the Department of Justice treats "production" of records by phone companies as synonymous with government "collection." *See* Administration White Paper, *supra* note 9, at 2 (referring to the NSA's telephony metadata activities as "collection"). This Note follows the DOJ's convention in describing the NSA's acquisition of phone records as "collection" or "gathering."
26. *See* IG Report #1, *supra* note 18, at 8–9.
27. *See id.* at 10.
28. *See id.*

being called—was in the United States.[29] The PSP granted this authority, greatly expanding the NSA's ability to conduct surveillance within U.S. borders.[30]

President George W. Bush reissued PSP authorizations approximately every forty-five days.[31] The drafting process was highly secretive and tightly controlled. David Addington personally drafted the memos and brought them by hand to the NSA, where General Hayden stored them in a locked safe in his office.[32] For every forty-five-day period, the Central Intelligence Agency ("CIA") and National Counterterrorism Center would submit "Threat Assessment Memoranda" detailing known terrorist threats and recent intelligence-gathering activity.[33] The Department of Justice's ("DOJ") Office of Legal Counsel ("OLC") would review the memos to determine whether the threat of attack was sufficient to continue the warrantless surveillance.[34] Each reauthorization of the PSP found that "an extraordinary emergency continued to exist . . . ."[35]

The White House tasked the DOJ with reviewing the legality of the PSP. OLC Deputy Assistant Attorney General John Yoo was the sole DOJ official with knowledge of the PSP's existence.[36] Yoo issued his first memo in support of the program on November 2, 2001.[37] He argued that the Foreign Intelligence Surveillance Act of 1978 ("FISA"), which restricts the government's power to gain intelligence on foreign powers within U.S. borders, does not apply to surveillance for purposes of national security.[38] In addition, he argued (1) that the Fourth Amendment does not apply to non-U.S. persons outside the United States, (2) that communications crossing U.S. borders can be lawfully intercepted under the "border crossing exception," (3) that there are no constitutional protections against searches

29. *See id.* at 13.

30. *See id.*

31. *See* OFFICES OF THE INSPECTORS GENERAL OF THE DEPARTMENT OF DEFENSE, DEPARTMENT OF JUSTICE, CENTRAL INTELLIGENCE AGENCY, NATIONAL SECURITY AGENCY, AND THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 6 (July 19, 2009), *available at* https://www.fas.org/irp/eprint/psp.pdf [hereinafter IG Report #2].

32. *See* IG Report #1, *supra* note 18, at 22.

33. *See* IG Report #2, *supra* note 31, at 7–9.

34. *See id.*

35. *See id.* at 6.

36. *See id.* at 10.

37. *See id.* at 11.

38. *See id.* at 11–12.

and seizures in "direct support of military operations," and (4) that the PSP's activity did not require warrants because it was "reasonable."[39]

NSA officials sent two requests for access to Yoo's opinion.[40] The White House denied both requests.[41] Meanwhile, President Bush continued to periodically reauthorize the PSP.[42] Then, in 2003, Yoo and his supervisor left the DOJ. Their replacements, Jack Goldsmith and Patrick Philbin, both learned of the PSP's existence.[43] Goldsmith and Philbin seriously questioned Yoo's legal analysis. They told Addington and then-White House Counsel Alberto Gonzales that they did not think the PSP could continue in its current form.[44] In January 2004, Deputy Attorney General James Comey learned of the program as well and agreed that Yoo's analysis was problematic.[45]

On March 4, 2004, Attorney General John Ashcroft determined that he, too, had serious doubts about the PSP's legal justifications.[46] Upon Ashcroft's sudden hospitalization for gallstone pancreatitis, Gonzales immediately asked Goldsmith to draft a letter supporting Yoo's analysis.[47] Goldsmith, Comey, and Philbin quickly responded that the Yoo memo "did not provide a basis for finding that [the surveillance activities] were legal . . . ."[48] Facing an impasse with the DOJ, Gonzales visited Ashcroft at the hospital to seek his approval for the reauthorization.[49] Ashcroft refused.[50]

On March 11, 2004, Gonzales himself signed the PSP authorization without DOJ approval.[51] On March 16, the OLC submitted another memo reviewing the legality of the PSP.[52] It found legal support for collection of internet content, telephony content, and telephony metadata, but "it determined that, given the method of collection, bulk Internet metadata was

39. *See id.* at 10–13.
40. *See* IG Report #1, *supra* note 18, at 21.
41. *See id.*
42. *See* IG Report #2, *supra* note 31, at 13.
43. *See id.* at 19–20.
44. *See id.* at 20.
45. *See id.* at 21.
46. *See id.*
47. *See id.* at 21–22.
48. *See id.*
49. *See id.* at 24–25.
50. *See id.*
51. *See id.* at 26.
52. *See* IG Report #1, *supra* note 18, at 42.

prohibited by the terms of FISA and Title III [of the Omnibus Crime Control and Safe Streets Act]."[53]

Gonzales replied to Comey that the President's interpretation of the law was definitive, regardless of the DOJ's objections.[54] Several high-level officials at the DOJ and the Federal Bureau of Investigation ("FBI") planned to resign in protest, including Comey, Goldsmith, and FBI Director Robert Mueller, all of whom drafted letters of resignation. Comey said "he believed it was impossible for him to remain with DOJ if the President would do something DOJ said was not legally supportable."[55] Goldsmith "cited the 'shoddiness' of the prior OLC legal review, the 'over-secrecy' of the PSP, and the 'shameful' incident at the hospital as among his grievances."[56] According to his staff, Ashcroft himself considered resigning as well.[57]

Nonetheless, for reasons that remain unclear, President Bush rescinded the NSA's authority to collect internet metadata on March 19, 2004.[58] The DOJ began seeking alternative legal justifications for the NSA's surveillance activities. The OLC initially found authority for the program in the "all necessary and appropriate force" language in the Authorization for Use of Military Force—the bill passed in the days following 9/11.[59] Soon, however, it shifted its focus to FISA.[60]

B. FOREIGN INTELLIGENCE SURVEILLANCE COURT ORDERS

FISA established standards for electronic surveillance aimed at collecting "foreign intelligence" inside the United States.[61] Initially, FISA authorized "electronic surveillance of a foreign power or an agent of a foreign power for

53. *See id.* at 37. "Title III" refers to Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510–20 (2012), commonly known as the Wiretap Act. According to the Supreme Court, the Wiretap Act "authorizes the use of electronic surveillance for classes of crimes carefully specified in 18 U.S.C. § 2516. Such surveillance is subject to prior court order. Section 2518 sets forth the detailed and particularized application necessary to obtain such an order as well as carefully circumscribed conditions for its use." United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 301–02 (1972).

54. *See* IG Report #2, *supra* note 31, at 29.

55. *See id.* at 27.

56. *See id.*

57. *See id.*

58. *See* IG Report #1, *supra* note 18, at 38.

59. *See* IG Report #2, *supra* note 31, at 29.

60. *See id.*

61. Foreign Intelligence Surveillance Act of 1978, Pub L. No. 95-511, 92 Stat. 1783, 1784–98 (codified at 50 U.S.C. §§ 1801–11(2012)).

the purpose of obtaining foreign intelligence information . . . ."[62] The USA PATRIOT Act of 2001[63] amended FISA by relaxing the threshold for domestic surveillance, requiring foreign intelligence gathering to be for "a significant purpose" (rather than "the purpose").[64]

The FISC reviews government requests for FISA orders.[65] The Chief Justice of the Supreme Court selects eleven district court judges to sit on the FISC for a maximum of seven years. Government agencies argue before the court in secret ex parte proceedings, over which a single FISC judge presides. A three-judge panel, comprised of judges from the district and circuit courts, can hear appeals from FISC decisions.[66] The Supreme Court has jurisdiction to review the appellate court's decisions. Since the establishment of the FISC in 1978, it has denied only eleven out of approximately 35,000 government requests.[67]

As government officials grew increasingly wary of the legal basis for the President's Surveillance Program, the DOJ began transitioning the legal basis for the NSA's surveillance activities from presidential authorizations to FISC orders.[68] By January 2007, the authority for the NSA's data collection and analysis activities under the PSP had been fully replicated under FISA.[69] The final presidential authorization for PSP expired on February 1, 2007.[70]

C. METADATA COLLECTION AND ANALYSIS

The NSA collects the following types of telephony metadata:

> [C]omprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile station

62. Foreign Intelligence Surveillance Act § 102(b), 92 Stat. at 1787–88, *available at* http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf (emphasis added).

63. The Uniting and Strengthening American by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

64. 50 U.S.C. § 1804(a)(6)(B).

65. *See* 50 U.S.C. § 1803.

66. *See* § 1803(b). FISC appeals are rare. *See, e.g., In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).

67. *See Foreign Intelligence Surveillance Act Court Orders 1979–2012*, *supra* note 11. However, Chief Judge Reggie Walton has noted that the FISC often asks the government to amend its requests before it grants approval. *See* Carol D. Leonnig, *Secret court says it is no rubber stamp; work led to changes in U.S. spying requests*, WASH. POST (Oct 15, 2013), http://www.washingtonpost.com/politics/secret-court-says-it-is-no-rubber-stamp-led-to-changes-in-us-spying-requests/2013/10/15/d52936b0-35a5-11e3-80c6-7e6dd8d22d8f_story.html.

68. *See* IG Report #1, *supra* note 18, at 37.

69. *See id.* at 38–39.

70. *See* IG Report #2, *supra* note 31, at 30.

> Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.[71]

The FISC has indicated that its telephony metadata orders do not authorize the collection of cell site location information.[72] Director of National Intelligence James Clapper wrote to the Senate Intelligence Committee that "[u]nder this program NSA is not currently receiving cell site location data, and has no current plans to do so."[73] In response, Senators Ron Wyden and Mark Udall wrote that "while the NSA claims no current plans to turn Americans' cell phones into tracking devices, it clearly claims the authority to do so."[74]

The NSA uses a range of data mining techniques to draw insights from its vast collections of metadata. A key part of the NSA's post-9/11 operations was the Metadata Analysis Center ("MAC").[75] Twenty NSA analysts, reporters, and technologists staffed a "24-hour 7-day a week watch center" to analyze the bulk metadata collected under the new surveillance program.[76] A separate unit called the Counterterrorism Product Line was responsible for analyzing content.[77] The two programs "worked closely together to coordinate efforts and share information."[78] By 2004, the

71. Amended Memorandum Opinion at 2 n.2, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109 (FISA Ct. Aug. 29, 2013) [hereinafter August 2013 FISC Opinion], *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

72. *Id.*

73. *See* Mark Stanley, *When Wyden and Udall Talk NSA, Pay Close Attention*, CENTER FOR DEMOCRACY & TECH. BLOG (July 30, 2013), https://www.cdt.org/blogs/mark-stanley/3007when-wyden-and-udall-talk-nsa-pay-close-attention.

74. *See id.* Since this conversation between Clapper and the two Senators, the *Washington Post* has reported that the NSA collects nearly five billion cell phone location records each day. *See* Barton Gellman & Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show,* WASH. POST (Dec. 4, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html. However, according to the NSA, "there is no element of the intelligence community that under any authority is intentionally collecting bulk cellphone location information about cellphones in the United States." *Id.*

75. *See* IG Report #2, *supra* note 31, at 11–12.

76. *See id.* at 13.

77. *See id.*

78. *See id.*

metadata and content operations had merged into a single organization called the Advanced Analysis Division ("AAD"), subdivided into three teams: internet metadata, telephony metadata, and content (for both internet and telephony communications).[79]

The NSA's techniques for analyzing metadata include "contact chaining" and "three-hop network analysis" using a custom platform called MAINWAY.[80] Call chaining involves recording and analyzing the calling patterns of a suspect.[81] Each call the suspect makes counts as a "hop." Each call those recipients make is another hop. NSA Deputy Director Chris Inglis has testified that the NSA conducts three-hop network analysis—that is, it analyzes data up to three degrees of separation from initial terrorist suspects.[82] If a person has forty contacts, three-hop network analysis could encompass data relating to 2.5 million people.[83] When the NSA detects a lead on terrorist activity, it passes the tip to the FBI or the CIA for further investigation.[84]

II. THE GOVERNMENT'S FOURTH AMENDMENT ARGUMENT

Since 2007, the government has sought and obtained several FISC orders authorizing the collection of telephony metadata. The statutory basis for the orders is Section 215 of the USA PATRIOT Act, which establishes guidelines for government "investigation[s] to obtain foreign intelligence information . . . to protect against international terrorism."[85] In addition, the government has advanced several arguments in favor of the program's constitutionality. This Note addresses the government's contention that a "Section 215 order for the production of telephony metadata is not a 'search' as to any individual" under the Fourth Amendment.[86]

---

79. *See id.* at 15.

80. *See id.* at 16–17.

81. *See* Philip Bump, *The NSA Admits It Analyzes More People's Data Than Previously Revealed*, ATLANTIC WIRE (July 17, 2013), http://www.thewire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287.

82. *See id.*

83. *See* Will Oremus, *The One GIF That Shows Just How Wide the NSA's Surveillance Net Really Is*, SLATE (Sept. 4, 2013), http://www.slate.com/blogs/future_tense/2013/09/04/three_hops_gif_aclu_infographic_shows_how_nsa_s_surveillance_spreads_exponentially.html.

84. *See* August 2013 FISC Opinion, *supra* note 71, at 17–18.

85. 50 U.S.C. § 1861(a)(1) (2012).

86. Administration White Paper, *supra* note 9, at 19.

A. THE THIRD-PARTY DOCTRINE

The government's Fourth Amendment argument rests on the third-party doctrine, first articulated in the Supreme Court's 1976 holding in *United States v. Miller*.[87] The *Miller* Court based its analysis on *United States v. Katz*, which held that a Fourth Amendment search occurs when the government violates the defendant's "reasonable expectation of privacy."[88] The defendant in *Katz* prevailed, but the Court noted that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[89] In *Miller*, the Court extended this reasoning to hold that bank depositors do not have a reasonable expectation of privacy in financial information that they voluntarily convey to the bank. The Court based its holding on the principle that:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.[90]

A depositor "takes the risk" that the bank will disclose her information to the government.[91]

The Court applied the third-party doctrine to telephone information in its 1979 decision in *Smith v. Maryland*.[92] In that case, law enforcement agents suspected Smith of robbing a woman and making threatening phone calls to her.[93] The telephone company cooperated with agents to install a "pen register," a device which records the numbers the caller dials, but not the content of conversations.[94] The pen register data led to Smith's arrest and conviction. Smith argued that the government's warrantless installation of the pen register violated his Fourth Amendment rights because he had a reasonable expectation of privacy in the numbers he dialed.[95] The Court rejected Smith's argument on the ground that he voluntarily conveyed the information to the phone company, which collected it for a variety of

87. United States v. Miller, 425 U.S. 435 (1976).
88. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
89. *Id.* at 351.
90. *Miller*, 425 U.S. at 443.
91. *Id.*
92. Smith v. Maryland, 442 U.S. 735 (1979).
93. *Id.* at 737.
94. *Id.*
95. *Id.* at 741–42.

legitimate business purposes (such as fraud detection and billing).[96] Following *Miller*, the Court held that callers do not have a reasonable expectation of privacy in information they voluntarily disclose to phone companies.[97] As a result, "there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police."[98] Therefore, the Fourth Amendment does not require the government to seek a warrant before obtaining call metadata.

The FISC has extended the reasoning of *Smith* to authorize the government's bulk collection of telephony metadata under Section 215. "The production of telephone service provider metadata," the court wrote, "is squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*."[99] Phone companies continue to collect metadata for a variety of business purposes, and callers should be aware that this collection is taking place. As in *Smith*, callers assume the risk that companies will disclose this information to the government.[100] Since callers do not have a reasonable expectation of privacy in "dialing information," the FISC held, bulk government collection is not a search under the Fourth Amendment.

B. TYPES OF DATA

Smith was the product of a pre-digital, pre-cellular telephone era. The pen register used in that case was a mechanical device that "record[ed] the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released."[101] It could only record the numbers that the caller dials. It could not record other types of data, such as whether the recipient answered the call, how long the call lasted, or how the phone company routed the call through its network.

The government has acknowledged that the types of data collected under the Section 215 orders are significantly more complex. In addition to the numbers dialed, the telephony metadata the NSA collects includes "the length and time of the calls and other similar dialing, routing, addressing, or signaling information . . . ."[102] The data set also includes "session identifying

96. *Id.* at 743–44.
97. *Id.*
98. *Id.* at 747.
99. August 2013 FISC Opinion, *supra* note 71, at 6.
100. *See id.* at 7.
101. *Smith*, 442 U.S. at 736 n. 1.
102. Administration White Paper, *supra* note 9, at 20.

information," which uniquely identifies the caller, and "trunk identifiers," which approximate the caller's location.[103]

However, the government argues (and the FISC has agreed) that there is no constitutional difference between the numbers dialed in *Smith* and the richer telephony metadata that the NSA collects under the authority of the Section 215 orders. The FISC has held that "the same type of information" is at issue in *Smith* and the Section 215 program.[104] "The Court is aware," wrote Judge Eagan, "that additional call detail data is obtained via this production than was acquired through the pen register acquisition at issue in *Smith*."[105] However, the court concluded that the telephony metadata at issue "is nothing more than pen register and trap and trace data," so callers have no Fourth Amendment expectation of privacy.[106] The government argues further that the type of information is irrelevant. As long as callers voluntarily convey this information to their mobile service providers, the reasoning of *Smith* holds, and Fourth Amendment protections do not apply.[107]

C. THE SCOPE AND DURATION OF DATA COLLECTION

Both *Miller* and *Smith* involved the collection of a single person's data. The Section 215 orders, by contrast, compel the disclosure of millions of records concerning nearly every American with mobile or landline phone service.[108] Neither *Miller* nor *Smith* considered whether the scope of data collection would alter the Fourth Amendment analysis. The FISC, however, has held that the number of people under surveillance is "irrelevant" to the court's analysis.[109] If a single person lacks a reasonable expectation of privacy in information she discloses to third parties, "grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[110]

---

103. August 2013 FISC Opinion, *supra* note 71, at 2 n.2.
104. *Id.* at 6.
105. *Id.* at 6 n.11.
106. August 2013 FISC Opinion, *supra* note 71, at 6 n.11. A "trap and trace" device is:

> [A] device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication . . . .

18 U.S.C. § 3147 (2012).
107. Administration White Paper, *supra* note 9, at 20.
108. *See* August 2013 FISC Opinion, *supra* note 71, at 8.
109. *Id.* at 9.
110. *Id.*

Miller and *Smith* also involved data collection over relatively short periods of time. Neither the government nor the FISC has addressed whether the duration of data collection is constitutionally significant, but the implication of the court's logic is straightforward: if a caller lacks a reasonable expectation of privacy in a single call record, then no Fourth Amendment interest appears *ex nihilo* to protect two records, or ten, or ten thousand.

The FISC's Fourth Amendment analysis has remained consistent. In an opinion dated October 11, 2013—the most recent public FISC opinion to date—Judge McLaughlin affirmed the court's earlier analysis: "[t]he Court has conducted an independent review of the issues presented by the application and agrees with and adopts Judge Eagan's analysis as the basis for granting the Application."[111]

III. WHAT METADATA CAN REVEAL

Following the Snowden disclosures, President Obama sought to calm the public controversy:

> [N]obody is listening to your calls. That's not what this program's about. As was indicated, what the intelligence community is doing is looking at phone numbers and durations of calls. They are not looking at people's names, and they're not looking at content. But by sifting through this so-called metadata, they may identify potential leads with respect to folks who might engage in terrorism.[112]

Similarly, Director of National Intelligence James Clapper wrote:

> The program does not allow the Government to listen in on anyone's phone calls. The information acquired does not include the content of any communications or the identity of any subscriber. The only type of information acquired under the Court's order is telephony metadata, such as telephone numbers dialed and length of calls.[113]

111. *Id.* Judge McLaughlin extended the court's Fourth Amendment analysis to address the Supreme Court's holding in *United States v. Jones*. For a discussion of the FISC's treatment of *Jones*, see *infra* Part IV.

112. *Transcript: Obama's Remarks on NSA Controversy*, WALL ST. J. (June 7, 2013), http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy.

113. Press Release, Office of the Director of National Intelligence, DNI Statement on Recent Unauthorized Disclosures of Classified Information (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information.

The government acknowledges that some aspects of telephone communications—"people's names" and the "content" of conversations—should receive stronger constitutional protections because they contain sensitive personal information.[114] Metadata, on the other hand, deserves lower protection because it poses a minimal privacy threat.

Yet, metadata analysis can lead to significant insights. Indeed, the value of metadata allows the NSA to justify spending millions of dollars on its phone record surveillance program. Metadata can expose private information on three distinct levels: first, records of individual calls; second, a caller's records collected over time; and third, an aggregation of many callers' records.[115]

A. INDIVIDUAL RECORDS

On the individual level, "metadata is often a proxy for content."[116] That is, there are circumstances in which a single call record reveals as much (or more) about the call as does the content of the conversation. The clearest examples involve single-use hotlines—for instance, services that offer support for domestic violence and rape. Other examples include suicide prevention and whistleblowing, including an anonymous whistleblowing hotline for the NSA itself.[117] Calls to those numbers will "reveal information that virtually everyone would consider extremely private."[118]

Another type of single-use phone number relates to charities, activist organizations, and political campaigns that accept donations via text message. In those cases, call records tell detailed stories of the sender's ideological positions and political affiliations, raising significant free speech and privacy concerns.[119]

B. RECORDS OVER TIME

Analysis of a caller's records over time can also reveal private information. Analysis of multiple records can reveal a detailed picture of the

114. *Id.*

115. The structure of this analysis draws from the declaration of computer science professor Edward Felten in *ACLU v. Clapper*. *See* Declaration of Professor Edward W. Felten, American Civil Liberties Union v. Clapper, 2013 WL 6819708, No. 13 Civ. 3994 (S.D.N.Y. Dec. 27, 2013), *available at* http://ia801803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf [hereinafter Felten Decl.].

116. *Id.* at 14.

117. *See Office of the Inspector General (OIG) Hotline*, NATIONAL SECURITY AGENCY, http://www.nsa.gov/about/oig/oig_hotline.shtml (last modified Sept. 1, 2010).

118. Felten Decl., *supra* note 115, at 15.

119. *See id.* at 16.

caller's social network, identifying close relationships and professional associations.[120] In some cases, it reveals more than the content of the conversations. For instance, suppose that:

> A woman calls her gynecologist; then immediately calls her mother; then a man who, during the past few months, she had repeatedly spoken to on the telephone after 11pm, followed by a call to a family planning center that also offers abortions. A likely storyline emerges that would not be as evident by examining the record of a single call.[121]

In addition, researchers have shown that mobile phone usage patterns can predict the caller's gender, age, marital status, job, and household size, with accuracy rates up to eighty-seven percent.[122] If an organization's call records are analyzed over time, they could also reveal the identities of confidential sources or anonymous litigants.[123] Consider the case of former CIA director David Petraeus: despite his attempts to conceal his identity and the identity of his paramour, Paula Broadwell, FBI agents were able to discover the identities of both using only their trail of metadata.[124]

C. AGGREGATED RECORDS

Metadata is perhaps most revealing when analyzed on a large scale. Research in "big data" has shown that the impact on individual privacy increases with the size of the data set under analysis.[125] Therefore, "a universal database containing records about all Americans' communications will reveal vastly more information, including new observable facts not currently known to the research community, because no researcher has access to the kind of data set the government is presumed to have."[126]

The government's arguments reveal the extent to which it believes large-scale metadata analysis can lead to significant insights. According to the government, it can collect "entire repositories of records [without a warrant], even when a particular record is unlikely to directly bear on the matter being

120. *See id.* at 17.

121. *Id.* at 18.

122. *See* Josh Jia-Ching Ying et al., *Demographic Prediction Based on User's Mobile Behaviors*, NOKIA RESEARCH CENTER (June 18–19, 2012), https://research.nokia.com/files/public/mdc-final241-ying.pdf.

123. *See* Felten Decl., *supra* note 115, at 19.

124. *See A Guardian Guide to Your Metadata*, THE GUARDIAN (June 12, 2013), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance.

125. *See* Felten Decl., *supra* note 115, at 21.

126. *Id.* at 21–22.

investigated, because searching the entire repository is the *only feasible means* to locate the critical documents."[127] In other words, there will be meaningful information that the government can only discern through sophisticated analysis of extremely large databases.

IV. METADATA COLLECTION AFTER *UNITED STATES V. JONES*

In *United States v. Jones*, the Supreme Court examined the Fourth Amendment implications of prolonged collection and analysis of publicly available information. In particular, the Court addressed the issue of whether prolonged GPS tracking on public roads constitutes a Fourth Amendment search.[128]

Police had installed a GPS device on Jones's wife's car.[129] They had a warrant, but it stipulated that they had to install the tracking device within ten days. They installed it on the eleventh day and tracked Jones for twenty-eight days.[130] The district court suppressed evidence obtained from the device while the car was parked at Jones's house but allowed the remaining data on the ground that "Jones had no reasonable expectation of privacy when the vehicle was on public streets."[131] The D.C. Circuit reversed, holding that the surveillance violated Jones's reasonable expectation of privacy.[132]

Justice Scalia, writing for a 5-4 majority, began his analysis by exploring the Fourth Amendment's basis in private property and common-law trespass.[133] He looked to eighteenth-century precedent to establish that the government's physical occupation of private property for the purpose of obtaining information violates the Fourth Amendment.[134] The government argued that Jones did not have a reasonable expectation of privacy in his movements on public roads.[135] But Scalia did not address the government's contention, holding that Jones's expectations were irrelevant because the government had physically intruded.[136] He surveyed cases after *Katz* to show that the Fourth Amendment's protections against physical intrusion apply,

127. *Id.* at 10.
128. United States v. Jones, 132 S. Ct. 945 (2012).
129. *Id.* 945–46.
130. *Id.*
131. *Id.* (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).
132. United States v. Maynard, 615 F.3d 544, 555, 564 (D.C. Cir. 2010).
133. *Jones*, 132 S. Ct. at 948.
134. *Id.*
135. *Id.* at 950.
136. *Id.*

even if the government did not violate the individual's expectation of privacy.[137] Here, the Court held that a Fourth Amendment search occurred because the government physically intruded, but it did not reach the question of whether prolonged collection and analysis of personal information would violate reasonable expectations of privacy.[138]

Justice Alito, concurring in the judgment with Justices Ginsburg, Breyer, and Kagan, argued that recent Fourth Amendment case law discarded the trespass test in favor of the *Katz* test.[139] In addition, Justice Alito argued that the trespass test fails to protect against privacy invasions where no physical intrusion has occurred.[140] Justice Scalia responded that he would not apply the property test as the exclusive measure of Fourth Amendment violations, but rather as a minimum level of protection.[141]

Justice Alito also argued that extensive data collection and analysis implicates Fourth Amendment concerns. For instance, the trespass test "disregards what is really important"—prolonged GPS tracking—and instead focuses on a "trivial" trespass.[142] Additionally, the trespass test produces incongruous results—for instance, it would prohibit short-term tracking via a physically planted GPS device, but it would allow limitless aerial surveillance.[143]

Since modern technology is changing rapidly, Justice Alito advocated legislative intervention and judicial restraint. In the absence of statutory guidelines, however, he argued that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[144]

Justice Sotomayor, concurring separately, joined the holding on narrow trespass grounds, but she recognized that the trespass test "may provide little guidance" in many modern cases.[145] Ubiquitous surveillance, for instance, may "chill[] associational and expressive freedoms," raising Fourth Amendment concerns.[146] Personal data, when aggregated and analyzed, can "reveal private aspects of identity."[147] She suggested that the Fourth

137. *Id.* at 950–51.
138. Id.
139. *Id.* at 957–58 (Alito, J., concurring).
140. *Id.*
141. *Id.* at 953 (majority opinion).
142. *Id.* at 961 (Alito, J., concurring).
143. *Id.*
144. *Id.* at 964.
145. *Id.* at 955 (Sotomayor, J., concurring).
146. *Id.* at 956.
147. *Id.*

Amendment should offer stronger protections for information disclosed to third parties. This "business records" doctrine of *Smith*, she argued,

> [I]s 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[148]

Together, five Justices took the view that metadata collection and analysis can raise Fourth Amendment concerns, despite having been voluntarily disclosed to a third party. "Although ultimately resolved on narrow grounds," write Professors Danielle Keats Citron and David Gray, "five Justices joined concurring opinions in *Jones* expressing sympathy for some version of the 'mosaic theory' of Fourth Amendment privacy. This theory holds that we maintain reasonable expectations of privacy in certain quantities of information even if we do not have such expectations in the constituent parts."[149]

In its defense of the NSA surveillance program, the government has given two reasons in light of *Jones* why it believes mass metadata collection is not a Fourth Amendment search. First, NSA collection of telephony metadata does not involve trespass, whereas the holding in *Jones* turned on the officers' physical intrusion.[150] Second, call records do not include location information (except trunk data, which reveals approximate location), whereas *Jones* addressed precise GPS location data specifically.[151]

The government's reading of Fourth Amendment doctrine is consistent with the Court's development of the third-party doctrine in *Smith*. However, as Professor Yochai Benkler has noted, "there is no question that all three *Jones* opinions offer a very strong argument that the dramatically lower cost of pervasive, sustained surveillance of publicly observable data in bulk implicates the Fourth Amendment . . . ."[152] Justice Scalia, invoking Justice Rehnquist's warning in *United States v. Knotts*, wrote that "different

148. *Id.* at 957.

149. David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J. L. & TECH. 381, 381–82 (2013).

150. Administration White Paper, *supra* note 9, at 20.

151. *Id.*

152. Yochai Benkler, *In Secret, Fisa Court Contradicted US Supreme Court on Constitutional Rights*, THE GUARDIAN (Sept. 22, 2013), http://www.theguardian.com/commentisfree/2013/sep/22/secret-fisa-court-constitutional-rights.

constitutional principles may be applicable" to "dragnet-type law enforcement practices," suggesting that publicly available data may acquire Fourth Amendment protections after prolonged collection.[153] Justice Alito argued that "what is really important" is not technical trespass, but rather the level of private information that long-term data collection and analysis can reveal.[154] Justice Sotomayor cautioned against the dangers of applying narrow Fourth Amendment doctrine in a new technological environment: "Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[155]

The FISC has endorsed the government's reading of *Jones*. Judge McLaughlin wrote for the court that the five concurring Justices in *Jones* recognized that "precise, pervasive monitoring by the government of a person's location could trigger Fourth Amendment protection . . . ."[156] However, NSA telephony metadata collection "concerns the acquisition of non-content metadata other than location information."[157]

The government's position, however, is an overly narrow reading of the concerns of the five Justices. Their concern about "precise, pervasive monitoring" of GPS location data was an illustration of a broader principle. Individual data points alone may reveal little sensitive information, which is why the third-party doctrine does not assume they are protected by a reasonable expectation of privacy. When aggregated and analyzed, however, they can become highly revealing. In the context of location data, a single visit to an HIV clinic may not be revealing. But it becomes revealing, in a way that the five *Jones* Justices recognized, when combined with a visit shortly after to family members' houses, a trip to the pharmacy, and sudden time off from work. Similarly, a single phone call from an HIV clinic is not revealing. But it becomes so when combined with a call to an insurance company, a doctor, and family members.

The NSA metadata collection program falls within the area of concern that the five Justices in *Jones* identified. As explained above, metadata collection—particularly on a large scale and over long periods of time—can

153. *Jones*, 132 S. Ct. at 951–52 n.6 (citing United States v. Knotts, 460 U.S. 276, 284 (1983)).

154. *Id.* at 961 (Alito, J., concurring).

155. *Id.* at 956 (Sotomayor, J., concurring).

156. Memorandum at 5, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-158 (FISA Ct. Oct. 11, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf.

157. *Id.*

be equally or more revealing than the content of conversations. The Justices stopped short of calling into question the rationale underlying the third-party doctrine, although Justice Sotomayor argued strongly that the doctrine should receive especially close judicial scrutiny given, the types of data and tools for analysis now available to law enforcement.

Rather, the Justices recognized that the Fourth Amendment implications of data-driven surveillance might be qualitatively and quantitatively different than the circumstances in which the third-party doctrine developed. *Smith* involved the surveillance of a carefully targeted suspect for a few days at most. NSA metadata collection, on the other hand, involves the collection of virtually every American phone call over multiple years, bearing a strong resemblance to Justice Scalia's fear of "dragnet-type law enforcement practices."[158] In addition, the police officers in *Smith* sought to identify a specific person making harassing calls to a specific number. But the NSA program gathers as much data as possible in the hope that certain key data points will emerge. Certainly, government agents can use sophisticated data mining techniques to capture insights that may assist the legitimate needs of law enforcement. But queries may also expose a great deal of private information about innocent people. The principle underlying the *Jones* concurrences is that the Fourth Amendment may offer protection against the privacy harms resulting from government queries of massive databases, even if the individual data points themselves lack protection.

158. *Jones*, 132 S. Ct. at 951–52 n.6.