Minnesota Journal of Law, Science & Technology

Volume 17 | Issue 2 Article 11

6-2016

An Unconstitutional Work of Art: Discussing Where the Federal Government's Discrete Intrusions Into One's Privacy Become an Unconstitutional Search Through Mosaic Theory

Steven Graziano

Note

An Unconstitutional Work of Art: Discussing Where the Federal Government's Discrete Intrusions Into One's Privacy Become an Unconstitutional Search Through Mosaic Theory

*Steven Graziano**

Modern technology has brought new challenges to notions of privacy, both practically and legally. Governmental abilities to surveil individuals, as well as the ability of citizens to seemingly carry around their entire lives in their electronic devices, has made the risk of egregious governmental intrusion into privacy a serious concern. Following the disclosures from Edward Snowden in the summer of 2013, the American public became far more aware, and arguably less approving, of the surveillance the government conducts.[1] The National Security Agency's (NSA) metadata collection program received extra

---

* J.D. Candidate, 2017, University of Minnesota Law School. The author would like to thank all the staff members and editors of the Minnesota Journal of Law, Science & Technology, with added thanks to James Meinert for all his hard work in the editing process. The author would also like to thank Professor William McGeveran for guidance and support throughout the entire note-writing process. Special thanks to Professor Deven Desai for the unexpected, yet greatly appreciated, assistance. Additionally, the author would like to thank Edward Snowden for, at the very least, sparking a much needed policy discussion within our nation.

1. *See* George Gao, *What Americans Think About NSA Surveillance, National Security and Privacy*, PEW RES. (May 29, 2015), http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy (showing a majority of American's disapprove of the government's collection of phone and internet data as part of anti-terrorism efforts); Brett LoGiurato, *Edward Snowden's Leaks Have Caused a 'Massive Shift' in the Public's Views of Government Surveillance*, BUS. INSIDER (July 10, 2013, 8:41 AM), http://www.businessinsider.com/edward-snowden-poll-nsa-surveillance-asylum-venezuela-2013-7 (noting a shift in public opinion toward believing that government surveillance methods go "too far in restricting civil liberties").

attention because of the volume of information it collects.[2] The metadata collection program was enjoined for a time by a federal district court judge who ruled the program likely to be unconstitutional,[3] and Congress responded by altering some of the NSA's powers with the USA FREEDOM Act (Freedom Act) in the summer of 2015.[4] However, the legal doctrine that allowed for its initial creation, and continued use—the third-party doctrine—is still alive in American courts.

The third-party doctrine states that an individual has no legitimate or reasonable expectation of privacy in information freely shared with a third-party, and thus government collection of that information is not a search under the Fourth Amendment of the United States Constitution.[5] While the origins of this doctrine seem largely reasonable, technological advances create new issues in its implementation.[6] All the information now turned over to third-parties, while seemingly insignificant individually, offers vast insight into the private

---

2. *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order ("[C]ommunication records of millions of US citizens are being collected indiscriminately and in bulk – regardless of whether they are suspected of any wrongdoing."); Chandra Steele, *7 Chilling Ways the NSA Can Spy on You*, PC MAG. (Jan. 15, 2014, 8:00 AM), http://www.pcmag.com/article2/0,2817,2429502,00.asp (describing backdoor access methods built into hardware and software the NSA is reported to use to monitor activity).

3. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 29–42 (D.D.C. 2013) (granting an injunction against Government collection of any telephony metadata associated with Verizon accounts), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam).

4. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified as amended at 12 U.S.C.A. § 3414, 18 U.S.C.A. 2280–2281, 2332(i), 2709, 50 U.S.C.A. §§ 1841–1843, 1861–1862, 1871–1874, 1881a (West 2015)); *see* Bill Chappell, *Senate Approves USA Freedom Act, Obama Signs It, After Amendments Fail*, NAT'L PUB. RADIO (June 2, 2015, 9:48 PM), http://www.npr.org/sections/thetwo-way/2015/06/02/411534447/senate-is-poised-to-vote-on-house-approved-usa-freedom-act.

5. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

6. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[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 . . . ." (citations omitted)).

life of an individual when pieced together.[7] In response, scholars crafted mosaic theory, which posits that at some point these discrete intrusions into one's privacy become a search, which triggers constitutional protections and therefore requires probable cause and a warrant.[8] Although a valiant attempt at redefining third-party doctrine for the modern age, mosaic theory also has its shortcomings. First, at what point does a collection of small intrusions into privacy become a search?[9] Second, how can non-searches ever become a search?[10]

This Note will discuss how a collection of isolated intrusions constitute a search carried out by government surveillance programs. The first part of this Note discusses the history, role, and power of the NSA. It also discusses Edward Snowden and his effect on the debate surrounding the NSA's use of mass surveillance. Part II discusses legal issues surrounding surveillance. Specifically, Part II analyzes recent challenges to the NSA's programs, highlighting the different approaches taken by different courts. Part II also illustrates third-party doctrine and the emergence of mosaic theory as a means to adapt third-party doctrine for modern purposes. This part concludes by presenting critiques of mosaic theory. Part III responds to critiques of mosaic theory by determining a point where a large number of discrete, presumably constitutional, intrusions into one's privacy transform into an unconstitutional, warrantless search. This Note attempts to provide the legal community with reasoned guidance on the

---

7. *See generally* United States v. Maynard, 615 F.3d 544, 562–63 (D.C. Cir. 2010) (discussing how discrete pieces of information retrieved from a GPS tracking device can offer insight into the subject's habits), *aff'd in part sub nom. Jones*, 132 S. Ct. 945.

8. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) ("The mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps. . . . [T]he mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group.").

9. *See Jones*, 132 S. Ct. at 954 (questioning how a court can determine the line where non-searches can become a search). *See generally* Mike Gentithes, *When the Government Mines "Big Data," Does It Conduct a Fourth Amendment Search?*, CBA REC., Jan. 2015, at 36, 36–37 ("At some unknown point . . . constant and ubiquitous monitoring infringes upon privacy in a way that individual instances of the same monitoring do not.").

10. *See generally* Gentithes, *supra* note 9, at 37 ("Critics might also point out a glaring logical inconsistency in mosaic theory. It seems impossible that some quantity of non-searches can somehow equal a search.").

implementation of mosaic theory, which preserves both the government's power to conduct intelligence gathering activities, and the people's right to be safe from unreasonable searches in the context of modern technology.

I. NSA HISTORY

A. NSA CREATION

To address America's national security needs after World War II, the United States Government took many steps to increase not only its military, but also its intelligence capabilities.[11] The NSA was founded by President Harry S. Truman in 1952 against the backdrop of the Korean War to consolidate intelligence gathering functions from various branches of the military and civilian law enforcement agencies.[12] President Truman discretely created the agency in a memorandum adopted substantially from a report by two consultants from the civilian intelligence community.[13] Due to its role as an intelligence collection operation, the government kept the NSA confidential and the public did not become aware of the agency's existence until long after it was created.[14]

---

11. *See* National Security Act of 1947, Pub. L. No. 80-253, §§ 101–102, 61 Stat. 495, 496–99 (codified as amended at 50 U.S.C. § 3021–3024) (merging intelligence functions across the military branches into the National Security Council, and establishing a civilian intelligence agency, the Central Intelligence Agency). *Cf.* Sean Gallagher, *A Short History of the NSA*, JURIST (July 22, 2013, 9:14 AM), http://jurist.org/feature/2013/07/nsa-overview-2.php ("The US military and intelligence agencies transformed in the aftermath of World War II.").

12. *See* Gallagher, *supra* note 11.

13. Memorandum from President Harry S. Truman to the Secretary of State and the Secretary of Defense (Oct. 24, 1952), http://nsarchive.gwu.edu/NSAEBB/NSAEBB23/docs/doc02.pdf. *See generally* THOMAS L. BURNS, CTR. FOR CRYPTOLOGIC HISTORY, NAT'L SEC. AGENCY, THE ORIGINS OF THE NATIONAL SECURITY AGENCY 1940–1952 (U), at 99–108 (1990), https://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf (describing the Brownell Committee Report, which outlined the needs of a new intelligence agency and was adopted in large part in President Truman's memorandum establishing the NSA).

14. *See* Gallagher, *supra* note 11 ("The Agency remained relatively unknown to the American Public. But during the course of a 1975 US Senate investigation, many Americans learned that not only did the NSA exist, but that it monitored Americans."); Daniel Schorr, *A Brief History of the NSA*, NAT'L PUB. RADIO (Jan. 29, 2006, 8:00 AM), http://www.npr.org/templates/story/story.php?storyId=5176847 ("[T]he multi-

B. NSA PRE-PATRIOT ACT

The Foreign Intelligence Surveillance Act of 1978 (FISA) explicitly endowed the NSA with a statutory basis for its various powers.[15] Generally, this act authorized the NSA to surveil foreign powers and their agents suspected of terrorism or espionage without a warrant.[16] The act required that to intentionally surveil a "United States person," the NSA needed to establish probable cause that the target is an agent of a foreign power.[17] The original FISA broadly authorized the use of any "electronic, mechanical, or other surveillance device" to obtain "the contents of any wire or radio communication."[18]

Additionally, FISA's pre-Patriot Act amendments authorized the use of pen registers, trap and trace devices,[19] and court orders compelling the production of tangible things.[20]

---

billion dollar agency had been a deep secret until it was unveiled in a Senate investigation in 1975.").

15. Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871).

16. *Id.* § 102, 92 Stat. at 1786 (codified at 50 U.S.C. § 1802(a) ("[T]he President . . . may authorize electronic surveillance without a court order . . . directed at . . . the acquisition of the contents of communications transmitted by means of communications used exclusively between or among *foreign powers* . . . ." (emphasis added)); *id.* § 101, 92 Stat. at 1783 (codified at 50 U.S.C. § 1801(a)) (defining "Foreign power," *inter alia*, as "a group engaged in international terrorism").

17. *Id.* § 105, 92 Stat. at 1790 (codified at 50 U.S.C. § 1805(a)(2) (requiring "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . ."); *see id.* § 101, 92 Stat. at 1783–84 (codified at 50 U.S.C. § 1801(b)(2)) (defining "agent of a Foreign power" to include "any person" who "knowingly engages" or "aids or abets" intelligence activities of a Foreign power).

18. *Id.* § 101, 92 Stat. at 1785 (codified at 50 U.S.C. § 1801(f)) (providing a definition of "electronic surveillance").

19. Pen registers and trap and trace devices are physical devices that can be used to record the numbers dialed, but not the contents, of incoming and outgoing calls on a telephone line. The use of such devices by law enforcement was only restricted in 1986 when Congress required law enforcement to obtain a warrant for their use; however, their use in intelligence surveillance was allowed through sealed FISA Court orders and may be done without any court order in times of emergency or war. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (making the use of pen registers and trap and trace devices illegal without a warrant); Intelligence Authorization Act for 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404–10 (1998) (codified at 50 U.S.C. §§ 1841–1846).

20. *See* Intelligence Authorization Act for 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410 (1998) (codified at 50 U.S.C. §§ 1861–1862) (allowing

The Electronic Communications Privacy Act of 1986 mandated a warrant for the use of pen registers and trap and trace devices by traditional law enforcement—even when the Fourth Amendment itself did not require a warrant—as their use is a form of metadata collection.[21] The NSA was given Congressional authority in 1998 to use pen registers and trap and trace devices if the agency obtained an order from the FISA Court finding that the use of the techniques was based on an investigation to gather foreign intelligence or information on international terrorism.[22]

Another development from FISA was the creation of the Foreign Information Surveillance Court (FISC), which grants or denies government requests for data collection.[23] This court is comprised of eleven district court judges and is charged with issuing warrants to surveil the NSA's targets.[24] The FISC handles both electronic and physical surveillance.[25] The act also created the Court of Review, which hears appeals of the

---

the NSA to compel, through court order, physical records from common carriers, and prohibiting the common carrier from disclosing that the records were sought or obtained), *replaced after expiration by* USA FREEDOM Act of 2015, Pub. L. 114-23, §§ 101–103, 129 Stat. 268, 269–72 (codified at 50 U.S.C.A. §§ 1861–1862 (West 2015)); *see also* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423 (1994) (codified at 50 U.S.C. §§ 1821–1829) (authorizing the use of a "physical search" into "premises or property" for purposes of "seizure, reproduction, inspection, or alteration of information, material, or property" when a person would have a "reasonable expectation of privacy and a warrant would be required for law enforcement purposes").

21. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301, 100 Stat. 1848, 1868–72 (codified as amended at 18 U.S.C. §§ 3121–3127 (2012)) (requiring a warrant for these investigative methods).

22. Intelligence Authorization Act for 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404–10 (1998) (codified at 50 U.S.C. §§ 1841–1846).

23. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, § 103, 92 Stat. 1783, 1788 (codified at 50 U.S.C. § 1803(a)).

24. *Id.* ("[D]esignate 11 district court judges from at least seven of the United States judicial circuits . . . .").

25. *Id.* ("[The court] shall have jurisdiction to hear applications for and grant orders approving electronic surveillance anywhere within the United States."); 50 U.S.C. § 1822(b)–(c) (addressing physical searches).

FISC's decisions.[26] Twelve warrants have been denied by the FISC over a course of thirty-three years.[27]

Congress withheld three types of surveillance from FISA's authorization: "(1) electronic communications outside U.S. borders, (2) surveillance in the U.S. and overseas following outside the statutory definition of 'electronic communication,' and (3) incidental collection of U.S. person communication."[28] Realizing that these types of surveillance are different from those that traditionally fell within FISA's authorization, President Reagan signed Executive Order 12333 to address the NSA's powers in that area.[29]

The order allowed for physical surveillance of U.S. persons overseas if the purpose was "to obtain significant information" that otherwise could not be acquired.[30] Additionally, by authorizing retention of data collected on U.S. citizens while pursuing foreign intelligence targets and information, E.O. 12333 effectively did away with a requirement the agency make individualized showings of suspicion before collecting the data, and effectively removes any limits on the volume of data that could be collected.[31]

---

26. 50 U.S.C. § 1803(b) ("[The court of review is comprised of] three judges, one of whom shall be publicly designated as the presiding judge, from the United States district courts or courts of appeals . . . .").

27. *See Foreign Intelligence Surveillance Act Court Orders 1979-2014*, ELECTRONIC PRIVACY INFO. CTR., https://www.epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Feb. 22, 2016).

28. Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 144 (2015) (citing H.R. REP. NO. 95-1283, pt. 1, at 50–54 (1978)).

29. Exec. Order No. 12,333, 3 C.F.R. 200 (1982); *see Mission*, NAT'L SECURITY AGENCY, https://www.nsa.gov/about/mission/index.shtml (last modified Apr. 15, 2011) (describing Executive Order 12333 as "delineat[ing] the NSA/CSS roles and responsibilities" to include: collection of intelligence information, managing the National Security Systems, and advocating for security regulations).

30. Exec. Order No. 12,333, 3 C.F.R. 200, § 2.4(d).

31. *See id*. § 2.3 (authorizing the collection and retention of "information concerning United States persons" as long as it is "information obtained in the course of a lawful foreign intelligence . . . or international terrorism investigation;" "[i]nformation acquired by overhead reconnaissance not directed at specific United States persons;" or "[i]ncidentally obtained information that may indicate involvement in activities that may violate federal, state, local or foreign laws"). *See generally Executive Order No. 12333*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/surveillance/12333/ (last visited Mar. 30, 2016) ("Executive Order 12333 authorizes the collection

The NSA's power—before September 11, 2001 and the passage of the Patriot Act—was laid out primarily in FISA of 1978, FISA's further amendments, as well as E.O. 12333. Although these documents do not offer a large amount of specificity about the limits of conduct the NSA was authorized to conduct, it is clear that the agency was able to surveil communications of those suspected of espionage or terrorism. Furthermore, E.O. 12333 clarified these powers by authorizing retention of data collected on U.S. citizens.[32]

C. EXPANSION OF NSA POWER

A large shift occurred in the NSA's scope after the September 11, 2001 terrorist attacks against the United States (9/11)[33] and the passage of the USA PATRIOT Act (Patriot Act).[34] The United States Government, whether actually warranted or not, felt that steps were needed to protect the population from further terrorist attacks.[35] The Patriot Act broadened the powers of the NSA;[36] most prominently through Section 215 of the act, which authorized a large amount of new surveillance policies.[37] The 2008 FISA Amendments also enlarged the NSA's powers.[38] The Bush Administration

---

of not only metadata, but of the actual communications of US citizens, so long as the communications are collected 'incidentally.'").

32. *See* Exec. Order No. 12,333, 3 C.F.R. 200, § 2.3 (1982).

33. *See generally September 11th Fast Facts*, CNN (Sept. 7, 2015, 12:41 PM), http://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/ (describing the terrorist attacks that took place on September 11, 2001).

34. USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 8 U.S.C., 15 U.S.C., 18 U.S.C., 22 U.S.C., 31 U.S.C., 42 U.S.C., 49 U.S.C., and 50 U.S.C.).

35. *See generally* G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861, 877–80, 883 (2013) (providing a timeline of changes at the NSA after 9/11).

36. *See* USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272.

37. *Id.* § 215, 115 Stat. at 287–88 (codified at 50 U.S.C. §§ 1861–1862), *replaced after expiration by* USA FREEDOM Act of 2015, Pub. L. 114-23, §§ 101–103, 129 Stat. 268, 269–72 (codified at 50 U.S.C.A. §§ 1861–1862 (West 2015)) (prohibiting the bulk collection of tangible things in place of the old authority to broadly access business records). *See generally* Donohue, *supra* note 28, at 124–31 (highlighting the provisions used to collect bulk Internet metadata and content, and the evolving interpretive theories used to defend the collection programs).

38. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified in part at 50 U.S.C. §§ 1861, 1881, 1885 (2012)). *See generally* Sinha, *supra* note 35, at 877–80, 883–

believed that the passage of both these laws were vital to protecting America's national security after 9/11.[39]

The Patriot Act amended FISA.[40] Section 215 of the act has garnered tremendous attention, as it allowed the government to request an order from the FISC that would require targets to turn over tangible items to the agency, such as business records.[41] Section 215 originally stated that the government "shall specify that the records concerned are sought for" an investigation into international terrorism or clandestine intelligence activities.[42] However the 2006 amendments to the Patriot Act lessened the burden, only requiring a "statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[43] The government used this provision to obtain bulk metadata from American telecom companies.[44] However,

---

89 (discussing the political battle over the passage of the 2008 amendments and provisions that survived into the final law).

39. *See* Sinha, *supra* note 35, at 883 ("In late July of 2007, claiming that '[o]ur national security depend[ed] on it,' President Bush used a radio address to call for further revision or modernization of FISA." (alterations in original) (citation omitted)).

40. USA PATRIOT ACT of 2001, Pub. L. No. 107-56, 115 Stat. 272.

41. *Id.* § 215, 115 Stat. at 287–88 (codified at 50 U.S.C. §§ 1861–1862) (replacing the authority to order a common carrier to release records upon a showing of "specific and articulable facts" that the records pertain to a "foreign power or an agent" with a generic authority to issue an "order requiring the production of any tangible things" including things pertaining to a "United States person" as long as the investigation was not "solely upon the basis of activities protected by the first amendment"), *replaced after expiration by* USA FREEDOM Act of 2015, Pub. L. 114-23, §§ 101–103, 129 Stat. at 269–72 (codified at 50 U.S.C.A. § 1861–1862 (West 2015)).

42. USA PATRIOT ACT of 2001, Pub. L. No. 107-56, § 215, 115 Stat. at 287–88 (codified at 50 U.S.C. §§ 1861–1862 (2012)) (requiring an order to pertain to an investigation "to protect against international terrorism or clandestine intelligence activities"), *replaced after expiration by* USA FREEDOM Act of 2015, Pub. L. 114-23, §§ 101–103, 129 Stat. at 269–72 (codified at 50 §§ 1861–1862 (West 2015)).

43. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 192, 196 (2006) (codified at 50 U.S.C. § 1861 (2012)), *replaced after expiration by* USA FREEDOM Act of 2015, Pub. L. 114-23, §§ 101–103, 129 Stat. at 269–72 (codified at 50 U.S.C.A. §§ 1861–1862 (West 2015)).

44. *See generally* Donohue, *supra* note 28, at 126–28 ("The Administration initially based the President's authority to conduct the President's Surveillance Program on three legal theories: (1) the President's inherent Article II authorities as Commander in Chief; (2) the 2001 Authorization for the Use of Military Force (AUMF); (3) and the War Powers Resolution

there has been recent pushback against the validity of this interpretation of these amendments. In 2015, the Second Circuit ruled that Section 215 actually did not authorize the bulk collection of telephony metadata and the NSA had exceeded its statutory authorization.[45] Another controversial aspect of Section 215, was that the FISC orders were done *ex parte*, and once one was issued, the reasons why it was issued could not be discussed.[46]

Additionally, the 2008 FISA Amendments further broadened the NSA's powers.[47] While these amendments were not part of the Patriot Act, they were also enacted during the post-9/11 period when the U.S. Government was engaged in a global war on terrorism. After the passage of the Patriot Act, amidst terrorism concerns, the Bush administration took part in further surveillance programs without Congressional approval.[48] Specifically, the administration took part in collection of both contents and metadata collected from telephony records and e-mails.[49] Despite pushback from

---

(WPR) . . . . In the face of mounting pressure, the legal basis for the component parts of the President's Surveillance Program gradually altered. On May 24, 2006, the NSA transferred the bulk collection of telephony metadata to FISA's Section 501 "tangible things" provisions (as amended by USA PATRIOT Act Section 215)." (footnotes omitted)).

45. Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 821 (2d Cir. 2015) ("[W]e hold that the text of § 215 cannot bear the weight the government asks us to assign to it, and that it does not authorize the telephone metadata program.").

46. *See id.* at 828–30 ("The FISC's hearings are, as noted, held *ex parte*."); *see also* 50 U.S.C. § 1861(c), (d) (2012) (providing for *ex parte* judicial orders, and prohibiting disclosure of any order), *replaced after expiration by* USA FREEDOM Act of 2015, Pub. L. 114-23, §§ 101–103, 129 Stat. at 269–72 (codified as amended at 50 U.S.C.A. § 1861(b)–(d) (West 2015)) (preserving *ex parte* judicial orders and prohibition on disclosure of any orders, but prohibiting bulk collection of tangible things).

47. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

48. *See* Donohue, *supra* note 28, at 125–26 (citing confidential documents released by *The Guardian*, including Authorization for Specified Electronic Surveillance activities During a Limited Period to detect and Prevent Acts of Terrorism Within the United States, Oct. 4, 2011, cited in OFFICE OF THE INSPECTOR GEN., NAT'L SEC. AGENCY CTR. SEC. SERV., WORKING DRAFT ST-01-0002, at 1, 7–8, 11, 15 (2009)). *See generally NSA Inspector General Report on Email and Internet Data Collection Under Stellar Wind – Full Document*, GUARDIAN (June 27, 2013), http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

49. *See* Donohue, *supra* note 28, at 125–26.

Congress and from the public against the executive branch claiming such broad powers, Congress eventually amended FISA in a way that allowed statutory authorization for these broader intelligence gathering activities.[50] Section 702 of the 2008 amendments allowed for the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[51] Additionally, when a telecom provider is provided with an order under Section 702, they must obey it unless the request is determined to be unlawful by FISC.[52] Failure to turn over the communication records, without such a determination, could result in being found in contempt.[53] While Section 702 focused on non-U.S. persons outside the United States, Sections 703 and 704 dealt with targeting U.S. persons outside the country.[54] These sections require similar, but somewhat different showings before records must be turned over to the government. Once the government requests an order from the FISC, the court must determine if the subject, or communication, is indeed abroad.[55] Section 704 is more lax than Section 703, as it does not require the government show that collection could be done by normal investigative means, and does not require the same extent of minimization as 702 or 703.[56]

The 2008 Amendments also declared that telecom companies must turn over records to the NSA and comply with the issuance of mass acquisition orders that target entire categories of individuals, rather than individualized orders pertaining to a specific subject.[57] Reaffirming the Bush

---

50. *See id* at 137–38.

51. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438 (codified at 50 U.S.C. § 1881a (2012)) (adding Section 702 to FISA).

52. *Id*. at 122 Stat. at 2453–57 (codified at 50 U.S.C. § 1881c(c)).

53. *Id*.

54. *See* Donohue, *supra* note 28, at 142.

55. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. at 2448, 2453 (codified at 50 U.S.C. § 1881b–1881c).

56. *See id*. at 122 Stat. at 2454 (codified at § 1881c(c)(1)(C)). *See generally* Donohue, *supra* note 28, at 143–44 (comparing legal standards and requirements between Sections 703 and 704).

57. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, §§ 801–804, 122 Stat. at 2467–70 (codified at 50 U.S.C. §§ 1885–1885c); *see* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION

administration's original desire, Section 702 allows "captur[ing] [the] content of communications. This could include content in emails, instant messages, Facebook messages, web browsing history, and more."[58] With the passage of the Amendments, specifically Sections 702 through 704, FISA became the primary tool for surveilling overseas targets, rather than E.O. 12333, which had previously been the primary justification.[59]

As a result of the Patriot Act and the 2008 FISA Amendments, NSA's powers were greatly expanded. At that point, the agency could request *ex parte* mass acquisition orders of records from American telecom companies, and the companies would gain immunity in any action surrounding compliance with an order.[60] Also, the agency could target non-Americans for up to a year.[61] The metadata collection program the NSA has been conducting on U.S. citizens, under its authority from the Patriot act, was held to be likely unconstitutional by the District Court for the District of Columbia until the Appeals court reversed;[62] however, the domestic metadata collection program is just one of the many new tools at the disposal of the NSA in post-9/11 America.[63]

---

702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 6 (2014), https://www.pclob.gov/Library/702-Report-2.pdf ("There is no requirement that the government demonstrate probable cause to believe that an individual targeted is an agent of a foreign power, as is generally required in the 'traditional' FISA process under Title I of the statute. Instead, the Section 702 certifications identify categories of information to be collected, which must meet the statutory definition of foreign intelligence information.").

58. Dia Kayyali, *The Way the NSA Uses Section 702 Is Deeply Troubling. Here's Why*, ELECTRONIC FRONTIER FOUND. (May 8, 2014, 5:10 PM), https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why. Contents of communications have garnered greater protections in American law than records of those communications. *See* Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2012) (requiring a warrant for collection of contents, while only requiring a court order for production of records); *In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 611–12 (5th Cir. 2013) (holding that cellular phone location data is defined as records and thus does not require a warrant).

59. *See* Donohue, *supra* note 28, at 142.

60. *See* 50 U.S.C. §§ 1881a(h)(3), 1885–1885c.

61. 50 U.S.C. § 1881a(a).

62. Klayman v. Obama, 957 F. Supp. 2d 1, 29–42 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam).

63. *See, e.g.*, Steele, *supra* note 2.

D. EDWARD SNOWDEN

Due to the NSA's institutional secrecy, investigative journalists and whistleblowers from within the intelligence community play an essential role in informing the public of the NSA's operations. The most recent, and arguably most significant, such disclosure occurred in 2013 when Edward Snowden copied thousands of NSA internal documents and disclosed them to various media sources. While not a direct employee of the NSA, Snowden was a technician and contractor for the agency, which gave him access to various files about the agency's surveillance practices.[64] When working as a contractor in Hawaii, Snowden "cop[ied] and back[ed] up hundreds of thousands, maybe millions of pages of documents."[65] He did this in preparation for his memorable leaks to the media starting with the British newspaper, *The Guardian*.[66] In summer of 2013, through journalist Glenn Greenwald, Snowden leaked that telecom companies—specifically Verizon first—had been turning over their customers' records to the United States Government, without warrants and under direction of the NSA pursuant to FISC orders.[67] Snowden followed this disclosure with various others, including one to the *Washington Post* claiming that the NSA—through its program named PRISM—had direct access to the servers of

---

64. *See* Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance; Terry Gross, *Edward Snowden: From 'Geeky' Dropout to NSA Leaker*, NAT'L PUB. RADIO (Apr. 16, 2014, 3:44 PM), http://www.npr.org/2014/04/16/303733011/edward-snowden-from-geeky-drop-out-to-nsa-leaker.

65. *See* Gross, *supra* note 64.

66. Greenwald et al., *supra* note 64; *see also* Joshua Eaton & Ben Piven, *Timeline of Edward Snowden's Revelations*, AL-JAZEERA AM., http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html (last visited Mar. 30, 2016).

67. *See* Greenwald, *supra* note 2; *see, e.g.*, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [REDACTED], Order, No. BR-05 (FISA Ct. May 24, 2006), [https://www.eff.org/sites/default/files/filenode/docket_06-05_1dec201_redacted.ex_-_ocr_0.pdf] (original Section 215 order to Verizon authorizing bulk telephony metadata collection). Snowden was put into contact with Greenwald after reaching out to filmmaker Laura Poitras in early 2013. Irin Carmon, *How We Broke the NSA Story*, SALON (June 10, 2013), http://www.salon.com/2013/06/10/qa_with_laura_poitras_the_woman_behind_the_nsa_scoops.

Apple, Microsoft, and Google.[68] Former NSA director Keith Alexander estimated Snowden's disclosures at somewhere between 50,000 and 200,000 documents.[69] Snowden's disclosures led to negative reactions from the U.S. Government,[70] and as a result he has relocated to Russia to avoid possible prosecution. However, the disclosures have also led to a shift in opinions on the use of government surveillance and government power in general.[71] Citizens now view the issue with more skepticism, or at the very least, Snowden has raised awareness.[72]

E. ATTEMPTS TO CURB AND ALTER THE NSA

Much has been made of the NSA and its programs since the Snowden revelations. Specifically, there have been legislative and judicial attempts to curb the agency's collection programs.[73] However, steps have also been taken to revamp and strengthen the nation's data collection programs.[74]

In summer 2015, political debate circled around the expiration of key provisions of the Patriot Act.[75] Provisions that were set to expire included: the metadata collection program contained in Section 215; the ability to use a "roving wiretap" on all communication devices connected to a target without an

---

68. *See* Eaton & Piven, *supra* note 66.

69. Mark Hosenball, *NSA Chief Says Snowden Leaked up to 200,000 Secret Documents*, REUTERS (Nov. 13, 2014), http://www.reuters.com /article/us-usa-security-nsa-idUSBRE9AD19B20131114.

70. *See Edward Snowden: Leaks that Exposed US Spy Programme*, BBC (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964 ("[Snowden] has been charged in the US with theft of government property . . . .").

71. *See, e.g.*, Gao, *supra* note 1; LoGiurato, *supra* note 1.

72. *See, e.g.*, Gao, *supra* note 1.

73. *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 29–42 (D.D.C. 2013) (granting a preliminary injunction against government surveillance on constitutional grounds), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam); Chappell, *supra* note 4 (describing the USA Freedom Act, which revived but constrained the Patriot Act).

74. *E.g.* Kelsey Rupp, *Meet the NSA's Next Surveillance Program that Was Just Snuck Through in the Congress' Omnibus Bill*, INDEP. J. REV. (Dec. 2015), https://www.ijreview.com/2015/12/495767-surveillance-omnibus-bill-draf (describing an omnibus spending bill that "encourages private sector companies to share their consumer's information with the government and other companies").

75. *See* Chappell, *supra* note 4 ("The vote comes two days after controversial provisions of the Patriot Act expired . . . .").

individualized warrant for each target; and the ability to target "lone wolf" terrorists, who have no ties to any terror organizations.[76] Many civil libertarian-leaning politicians, including Rand Paul and Bernie Sanders, celebrated the end of the legislation.[77] However, some politicians feared that without an extensive data collection system in place, the United States could fall victim to acts of terrorism, as the nation's national security would become severely compromised.[78] In response to this fear, Congress passed the Freedom Act.[79] The act rescued, in some form, the three provisions from the Patriot Act that many national security-minded politicians feared losing.[80] The act extended the deadlines for the "lone wolf" provision and the "roving wire taps" until 2019.[81] Moreover, it limited the polarizing powers of Section 215 by banning mass metadata collection unless the government has "reasonable, articulable suspicion" that a "specific selection term" used to request telephone data is associated with terrorism.[82] Despite these provision, staunch detractors of government surveillance did not vote for it, as they viewed it as too weak of an attempt to limit government surveillance.[83]

In addition to the legislative attempt to constrain the authorizations of power to the NSA, the courts have also been employed to challenge the legality of the agency's actions. The first notable challenge against the NSA's mass surveillance programs was in *Clapper v. Amnesty International USA*.[84]

---

76. *See* Jeremy Diamond, *Patriot Act Provisions Expire: What Happens Now?*, CNN (June 1, 2015, 10:48 AM), http://www.cnn.com/2015/05/30/politics/what-happens-if-the-patriot-act-provisions-expire/.

77. *See* Chappell, *supra* note 4 (Both Paul and Sanders voted against the USA Freedom Act).

78. *See* Diamond, *supra* note 76.

79. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified at 12 U.S.C.A. § 3414, 18 U.S.C.A. §§ 2280–2281, 2332(i), 2709, 50 U.S.C.A. §§ 1841–1843, 1861–1862, 1871–1874, 1881a (West 2015)). The official title of the act is "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015." *Id.*

80. *See* Chappell, *supra* note 4; *USA Freedom Act: What's in, What's out*, WASH. POST (June 2, 2015), https://www.washingtonpost.com/graphics/politics/usa-freedom-act/.

81. *See USA Freedom Act: What's in, What's out*, *supra* note 80.

82. USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101, 129 Stat. at 270 (codified at 50 U.S.C.A. § 1861 (West 2015)).

83. *See* Chappell, *supra* note 4.

84. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

Amnesty International challenged the application of Section 702 of FISA as amended in the 2008 FISA Amendments.[85] That section "allows the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not 'United States persons.'"[86] However, before reaching the merits of that case, the Supreme Court determined that the respondents did not have standing to challenge the law because they could not "demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm."[87] After this decision, it seemed unlikely that anyone would have standing to challenge the NSA's surveillance programs, as it would seem almost impossible for challengers to prove that the NSA is specifically targeting them.[88] However, Edward Snowden's disclosures in 2013 offered support to those seeking standing to challenge the NSA.[89]

Edward Snowden's disclosures led to the eventual challenges that resulted in *American Civil Liberties Union v. Clapper* and *Obama v. Klayman*. *American Civil Liberties Union* held that the mass metadata collection methods of the NSA exceeded their Section 215 authorization.[90] The district judge ignored the statutory question and upheld the legality of the programs, as "[c]lear precedent applies because *Smith* held that a subscriber has no legitimate expectation of privacy in

85. *Id.* at 1142–43; *see also* 50 U.S.C.A. § 1881a (West 2015).

86. *Amnesty Int'l USA*, 133 S. Ct. at 1142.

87. *Id*. at 1155.

88. *See id.* at 1148 ("[R]espondents merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired under §1881a.").

89. *See generally* Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517, 520–30 (2015) (discussing standing issues before and after Snowden, noting different court's considerations of factual information disclosed by Snowden); Caspar S. Miller, Note, Clapper v. Amnesty International USA: *The "Certainly Impending" Standard for Article III Standing in Government Surveillance Cases*, 35 WHITTIER L. REV. 559, 587 (2014) ("One thing is clear, however, both of the district courts pointed out that the Snowden revelations, as well as other declassified information and decisions, provided the ammunition these plaintiffs needed to establish standing under *Clapper*.").

90. Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 792 (2d Cir. 2015).

telephony metadata created by third parties."[91] Despite this apparent strong adherence to precedent, the Second Circuit Court of Appeals vacated and remanded the trial court's decision.[92] The Second Circuit held that FISA could be subjected to judicial review under the Administrative Procedure Act, since nothing in FISA's text or legislative history precluded it from review—an determination the district court had not made believing it could not conduct a review.[93] The Second Circuit Court of Appeals stated that the Patriot Act required the metadata collected to be relevant to approved counterterrorism efforts, but noted that "the telephone metadata program . . . seeks to compile data in advance of the need to conduct any inquiry (or even to examine the data), and is based on no evidence of any current connection between the data being sought and any existing inquiry."[94] As a result, the court ruled that the metadata collection program overstepped its statutory basis and thus was illegal.[95] This decision became moot less than a month later, with the passage of the USA Freedom Act.[96] It is important to note that the different outcomes result from the trial court focusing on constitutional analysis, which it believed was justified by the need for national security and the third-party doctrine,[97] while the appeals court reviewed the statutory bases of the agency's

---

91. Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013), *aff'd in part, vacated in part, remanded*, 785 F.3d 787, 822 (2d Cir. 2015) (referencing Smith v. Maryland, 442 U.S. 735 (1979)). "Under the third-party doctrine, a citizen relinquishes any such privacy expectation in information that she discloses to a third party, be it a personal confidant or a business entity, even if he or she assumed that the information would be held confidentially." Gentithes, *supra* note 9 at 37.

92. *See Am. Civil Liberties Union*, 785 F.3d at 826 (vacating the district court's judgment).

93. *Id.* at 806–07.

94. *Id.* at 817–18. The relevant provision discussed in the case was 50 U.S.C. § 1861 (2012), *replaced after expiration by* USA FREEDOM Act of 2015, Pub. L. 114-23, §§ 101–103, 129 Stat. 268, 269–72 (50 U.S.C.A. § 1861 (West 2015)).

95. *Am. Civil Liberties Union*, 785 F.3d at 821.

96. *See USA Freedom Act: What's in, What's out*, *supra* note 80 ("The [USA Freedom Act] bans the bulk collection of data of Americans' telephone records and Internet metadata.").

97. Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 742 (S.D.N.Y. 2013) ("Even if the statutory claim were not precluded, it would fail."), *aff'd in part, vacated in part, remanded*, 785 F.3d 787, 822 (2d Cir. 2015).

actions, something the district court did not believe it had the power to do.[98]

Additionally, *Obama v. Klayman*, reached a similar conclusion, although it reached its conclusion on strictly constitutional grounds, rather than for statutory reasons. Judge Leon at the District Court for the District of Columbia held that "plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment."[99] He then ordered injunctive relief for the plaintiffs, but stayed his order pending appeal.[100] On appeal, the D.C. Circuit Court of Appeals determined that the plaintiffs did not meet the burden of proof to sustain the injunction, but remanded it back to the trial court for a conclusive ruling on the merits.[101] Judge Leon's decision illustrates both the constitutional limitations of the NSA's programs and the increasing skepticism courts have been using when analyzing the NSA's programs, either for constitutionality or statutory analysis.

Although there have been steps to limit the NSA's power, there have also been steps taken, specifically by the most recent Congress, to strengthen surveillance.[102] Very recently, Congress passed some provisions of the Cybersecurity Information Sharing Act (CISA) into law,[103] which has drawn sharp criticism from civil libertarians, as many view it as a new form of the Patriot Act.[104] Although Congress tries to

---

98. *Am. Civil Liberties Union*, 785 F.3d at 821.

99. Klayman v. Obama, 957 F. Supp. 2d 1, 41 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam).

100. *Id.* at 43.

101. Obama v. Klayman, 800 F.3d at 562.

102. *E.g.*, Rupp, *supra* note 74 (describing the version of the Cybersecurity Information Sharing Act of 2015 that was included in an omnibus bill).

103. Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, div. N, 129 Stat. 2242, 2935–85 (2015) (codified at 5 U.S.C.A. § 301, 6 U.S.C.A. §§ 131, 148, 151, 1501–1510, 1522–1525, 1531–1533, 44 U.S.C.A. §§ 3553–3554 (West 2015)).

104. *See generally* Lucian Armasu, *Meet CISA, a De Facto Cyber Patriot Act*, TOM'S HARDWARE (Dec. 16, 2015, 9:30 AM), http://www.tomshardware.com/news/cisa-the-cyber-patriot-act,30771.html ("Paul Ryan managed to push CISA into the 'omnibus' budget bill, but not before Congress stripped out all of its privacy protections and turned it from

characterize the act as a way for businesses and the government to share information in hopes of fighting terrorism and cyber-hacking, detractors view this bill as a whole—and especially the specific provisions passed into law—as a new way for the federal government to collect data from telecom companies.[105] Critics of the act claim that this act simply "remov[es] privacy and liability protections [from telecom companies] for the sake of cybersecurity."[106] Evan Greer, campaign director for the digital rights group known as "Fight For the Future," has stated that "CISA is the new Patriot Act. It's a bill that was born out of a climate of fear and passed quickly and quietly using a broken and nontransparent process."[107] To some, the Patriot Act and CISA both potentially authorize third-party disclosure of customer information to the government.[108] Due to the recent passage of this law, analysis is limited. Nonetheless, the executive branch is required to implement all statutes within the confines of the authorities given and the Constitution, so the future of CISA depends on how the government designs its surveillance programs.

The passage of the Freedom Act and the federal court decisions discussed above can be looked at as statements on the illegality and unconstitutionality of the NSA's surveillance programs, and indicative of a growing trend to look at NSA programs with skepticism and concern. However, the Freedom Act may be no different than the Patriot Act.[109] CISA offers very new challenges for understanding how the NSA is operating its surveillance programs, and will become a new

---

what was originally meant to be a cybersecurity bill into a *de facto* surveillance bill.").

105. *See* Rupp, *supra* note 74.

106. *Id*.

107. Jenna McLaughlin, *Hasty, Fearful Passage of Cybersecurity Bill Recalls Patriot Act*, INTERCEPT (Dec. 19, 2015, 10:05 AM), https://theintercept.com/2015/12/19/hasty-fearful-passage-of-cybersecurity-bill-recalls-patriot-act.

108. *See id*. ("[CISA would] make all of us more vulnerable to cyber attacks by letting corporations off the hook instead of holding them accountable when they fail to protect their customer's sensitive information.").

109. *See* Chappell, *supra* note 4 (noting some pro-privacy advocates characterizing the Freedom Act as a decisive victory while others opposed the bill as a mere continuation of the Patriot Act). *But see USA Freedom Act: What's in, What's out*, *supra* note 80 (detailing some differences between the USA Freedom Act and the Patriot Act).

focal point for those who question the NSA's tactics.[110] However, if the fears of privacy advocates turn out to be correct, the United States may have to deal with the consequences of another Patriot Act.[111]

F. REASONABLE EXPECTATIONS OF PRIVACY

Katz v. United States crafted the reasonable expectations of privacy test, which has been the paramount test used in Fourth Amendment analysis.[112] In *Katz*, the government wiretapped a phone booth, and the Court determined that where an individual had a reasonable expectation of privacy, the protections of the Fourth Amendment were triggered, as a search has been conducted.[113] In comparison to traditional notions of the Fourth Amendment—which had typically required physical trespass for a search to take place[114]—*Katz* is arguably not very intrusive, as it took place in a public phone booth and involved transmission of messages through the telephone. Nonetheless, the court determined the intrusion to be a search and the Fourth Amendment had been violated.[115]

Justice Harlan's concurrence, which has become the controlling opinion from the case, crafted the reasonable expectations of privacy test.[116] The test posits that a search takes place when the governments intrudes into an area where the citizen has a reasonable expectation of privacy.[117] Specifically, the test requires that there is an actual, subjective expectation of privacy, and this expectation is reasonable.[118]

---

110. *See* Rupp, *supra* note 74 (characterizing CISA as a "de facto cyber Patriot Act" and arguing that CISA may end up being used by the NSA to conduct mass surveillance as the agency did before the Freedom Act).

111. *See id*.

112. Katz v. United States, 389 U.S. 347, 359 (1967).

113. *Id.*

114. *See id.* at 352–53 ("[T]he absence of such [physical] penetration was at one time thought to foreclose further Fourth Amendment inquiry . . . .").

115. *Id.* at 358–59.

116. *Id.* at 360–61 (Harlan, J., concurring).

117. *Id.*

118. *Id*. (characterizing the critical facts establishing a subjective and reasonable expectation as the individual entering the phone booth, "shut[ing] the door behind him," which entitles him to assume "that his conversation is not being intercepted").

Another overarching concept derived from *Katz* is the idea that the Fourth Amendment "protects people, not places."[119]

G. THIRD-PARTY DOCTRINE

One of the primary legal doctrines used by the federal government to justify its surveillance programs has been the third-party doctrine.[120] The third-party doctrine states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[121] The Supreme Court has used this reasoning as grounds for upholding law enforcement's surveillance for decades.[122]

In *Smith v. Maryland*, the Court considered the Fourth Amendment prohibition on unreasonable searches in the context of a law enforcement practice of compelling telephone companies to install pen registers to monitor incoming and outgoing telephone numbers.[123] The Court held the surveillance practice did not violate the Fourth Amendment under the theory that the defendant in that case voluntarily turned over his information to the telephone provider, who then voluntarily turned that information over to the government.[124] Under this theory, the act of turning over information is paramount, and the individual's presumptions of privacy are secondary at best—"[u]nder the third-party doctrine, a citizen relinquishes any such privacy expectation in information that she discloses to a third party, be it a personal confidant or a business entity, even if he or she assumed that the information would be held confidentially."[125] Under third-party doctrine, even if an individual expects information he or she discloses to a third-party to be confidential, and thus satisfying the first prong of

---

119. *Id*. at 351 (majority opinion); *see id.* at 361 (Harlan, J., concurring) ("The point is not that the booth is 'accessible to the public' at other times, but that it is a temporarily private place whose momentary occupants' expectation of freedom from intrusions are recognized as reasonable." (citation omitted)).

120. Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 749–50 (S.D.N.Y. 2013), *aff'd in part, vacated in part, remanded*, 785 F.3d 787 (2d Cir. 2015).

121. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

122. *Id*.

123. *Id.* at 736–38.

124. *Id*. at 743–45.

125. Gentithes, *supra* note 9, at 37.

the reasonable expectations of privacy test as crafted in *Katz*, the second prong is not satisfied, as that expectation is not reasonable.[126] This doctrine was memorialized in *United States v. Miller*, where the Court held that an individual that turns information over to a third party does not have a reasonable expectation of privacy in that information.[127]

Third-party doctrine has also been rigidly applied at the trial court level. In *American Civil Liberties Union v. Clapper*, Judge Willian Pauley upheld the NSA's data collection programs because "[*Maryland*] held that a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties."[128] While third-party doctrine makes sense in the context of facilitating criminal investigations and prosecutions, such as when building evidence against a organized criminal gang; however, using the doctrine to justify collection of various pieces of information from innocent citizens presents problems. As the courts have noted, in the present day, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" and in doing so, unconsciously, rather than voluntarily, open themselves up to surveillance by the government.[129] Applying the third-party doctrine is becoming more of a problem because the use of modern technology has so permeated every aspect of our lives that "the elimination of human interaction is a standard business practice" and as a

126. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). The reasonable expectation of privacy test posits that a search occurs when the governments intrudes onto private action in which the private actor both has an actual, subjective expectation of privacy, and this expectation is reasonable. *See id*.

127. United States v. Miller, 425 U.S. 435, 443 (1978).

128. Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (citing *Maryland*, 442 U.S. at 744–45), *aff'd in part, vacated in part, remanded*, 785 F.3d 787, 822 (2d Cir. 2015).

129. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). Justice Sotomayor lists examples of these disclosures as the following: the phone numbers that [individuals] 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. *Id.*

result "there is not meaningful exposure" to other individuals that are not mediated by third-party technologies.[130]

H. MOSAIC THEORY

The United States Supreme Court has hinted toward discomfort with applying archaic Fourth Amendment analysis to modern technological instances in general. In *United States v. Jones*, the Supreme Court alluded to discomfort with third-party doctrine,[131] and in *Riley v. California* openly acknowledged that modern citizens carry around their entire lives in devices such as cellular phones, which may require Fourth Amendment jurisprudence as a whole to be reevaluated.[132]

In an attempt to solve practical problems that arise when trying to apply third-party doctrine to modern technological times, scholars have developed what is known as mosaic theory.[133] Mosaic theory posits that eventually a collection of discrete intrusions into one's private life offer such broad insight into one's actions and intentions that the intrusions

---

130. Deven Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 618 (2014).

131. *Jones*, 132 S. Ct. at 963–64.

132. Riley v. California, 134 S. Ct. 2473, 2484–85, 2489–91 (2014).

133. *See generally* Kerr, *supra* note 8, at 328–43 (identifying problems with applying mosaic theory as a standard in Fourth Amendment cases); Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 222–45 (2012) (considering the merits of judicial application of mosaic theory as a constitutional analysis versus as a theoretical statutory analysis); Erin Smith Dennis, Note, *A Mosaic Shield:* Maynard*, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 763–71 (2011) (arguing that mosaic theory is incompatible with third-party doctrine and even basic forms of electronic surveillance like pen registers). Although the true origin of the term mosaic theory is contested, many trace it back to the an argument used by the Federal Government, in which the government argued in the context of state secrets, that it could not turn over individual pieces of sensitive information even if they would not reveal anything substantial, because the accumulation of data, in the form of a mosaic, would reveal state secrets that could compromise the nation's well-being. *See* U.S. v. Reynolds, 345 U.S. 1, 8 (1953). The government seemingly flips this argument in the case of the Fourth Amendment. In the national security realm, they argue that there are various bits of information that on the whole could reveal important, private matters, but that in the Fourth Amendment context this is not a concern.

become a search subject to the protections of the Fourth Amendment.[134] Put differently:

> Under the mosaic theory, searches can be analyzed as a collective sequence of steps rather than as individual steps. Identifying Fourth Amendment searches requires analyzing police actions over time as a collective "mosaic" of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not.[135]

This type of "mosaic search" would involve a host of relatively non-intrusive government actions that become a search because "data from a GPS company, a cellular phone company, a search company, a credit card company, or a retailer reveals all the details of [a] person's life [and] no sophisticated . . . analysis is required [to] tell you exactly where someone went, what they bought, or what they read."[136]

The United States Supreme Court has alluded to mosaic theory as a viable legal option for establishing where Fourth Amendment boundaries exist when faced with applying third-party doctrine to instances of modern technology.[137] Justice Sotomayor, in her concurring opinions in *Jones*, explicitly brings up the necessity of revisiting third-party doctrine, stating that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[138] In the same case, Justice Alito, writing in a separate concurrence, suggested that extended use of the GPS tracker in that case, rather than one discrete use, transformed the surveillance into a Fourth Amendment search.[139] This is analogous to the collection of various small pieces of information on one's life eventually constituting a traditional search. In *United States v. Maynard*, the D.C. Circuit openly acknowledged, and adopted, mosaic theory.[140] It concluded that the sum of various intrusions into the petitioner's privacy resulted in an unconstitutional warrantless search.[141]

---

134. *See Reynolds*, 345 U.S. at 8; Dennis, *supra* note 133, at 748.
135. Kerr, *supra* note 8, at 313.
136. Desai, *supra* note 130, at 616.
137. *See Jones*, 132 S. Ct. at 956–57 (Sotomayor, J., concurring).
138. *Id.* at 957.
139. *Id.* at 958 (Alito, J., concurring).
140. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom. Jones*, 132 S. Ct. 945.
141. *Id.* at 562–64.

I. PROBLEMS WITH MOSAIC THEORY

Mosaic theory is not perfect and detractors are quick to point out its shortcomings. One criticism pertains to the point at which the isolated intrusions become one search—where is the point where a number of isolated, discrete intrusions transform into one illegal search?[142] Included in this critique is a more theoretical question, namely: how can non-searches ever become a search? Justice Scalia frames these potential issues nicely in *Jones*, when he, while critiquing the concurrences, wonders why a "4–week investigation is 'surely' too long . . . [?] What of a 2–day monitoring of a suspected purveyor of stolen electronics? Or of a 6–month monitoring of a suspected terrorist?"[143] A lack of clear guidance as a legal standard detracts from mosaic theory's ability to sufficiently address third-party doctrine's flaws.

II. ANALYSIS

A. RESPONSE TO PROFFERED CRITICISMS OF MOSAIC THEORY

1. Each intrusion under third-party doctrine is a partial search.

The first issue with mosaic theory is that is fails to distinguish where the discrete intrusions allowed by third-party doctrine reach a level that causes them to be viewed as a search.[144] Thus far, "[t]he best solution that mosaic advocates have . . . been able to muster is to draw bright, if arbitrary, lines based on how long officers use an investigative method or technology."[145] However, a better way of responding to that

---

142. *See* Gentithes, *supra* note 9, at 37; Kerr, *supra* note 8, at 344 ("The [mosaic] theory allows courts to say that techniques are sometimes a search. They are not searches when grouped in some ways (when no mosaic exists) but become searches when grouped in other ways (when the mosaic line is crossed).").

143. United States v. Jones, 132 S. Ct. 945, 954 (2012).

144. *See id*. at 957 (Sotomayor, J., concurring); *see also id*. at 954 (majority opinion); Gentithes, *supra* note 9, at 36–37.

145. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71 (2013). Gray and Citron argue that the solution to the mosaic theory puzzle should be whether the surveillance used by the government has the potential to "facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state." *Id*. at 72. However, the

critique is not to look at length of surveillance, but to look at overall, actual volume of collection, through the lens of *Katz*.[146]

To address this issue with mosaic theory, one must characterize each intrusion, as an incomplete, or partial search, not a non-search altogether. This conceptualization leads to what I call "partial search theory," which posits that at some point the individual partial-searches, when added together, accumulate into a mass in which the intrusions' subject has a reasonable expectation of privacy. Once that level is met, a constitutionally protected search has taken place, and a warrant is required. So, put simply, under partial search theory, the discrete intrusions into one's private life become a search at the point where there is both a subjective and a reasonable expectation of privacy in the mass of information collected.[147] It may be true that there is no reasonable expectation of privacy in each individual piece of information, but it is completely feasible, and expected, that there is a subjective, reasonable expectation of privacy in the vast accumulation of various parts of data, each of which pertaining to a unique aspect of an individual's life.[148] Conceptualizing the limits of partial search theory requires analyzing intrusiveness in light of the reasonable expectation privacy test. Although not completely predictive, connecting intrusiveness and reasonableness to *Katz* allows courts to use mosaic theory to protect information from mass surveillance by the NSA. It is true that this theory will leave discretion for judges, but the evolution of common law will further shape the doctrine until

---

response presented in this Note does not focus on the potential to take part in mass surveillance and the shadows that casts on society, but instead argues that when the actual volume of data collected becomes such that an individual has a reasonable expectation of privacy in the data, the government's actions trigger Fourth Amendment protections.

146. *Cf.* Desai, *supra* note 130, at 616 (discussing the ability to gain immense access into the private matters of an individual's life based on the collection of various isolated intrusions into their life).

147. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining the reasonable expectations test as, "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'").

148. *See generally* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (discussing how additions of cumulative information can transform the meaning in the information—"[p]rolonged surveillance reveals types of information not revealed by short-term surveillance"), *aff'd in part sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).

the test becomes more precise and uniform. That fact that partial search theory is not neatly defined should not prevent its effectiveness in providing constitutional protections, as the reasonable expectation test itself is equally unclear and fact-driven, yet it has been defined through years of jurisprudence.[149]

Mosaic theory may not allow us to exactly locate the point where the accumulation of non-searches becomes a search, but it does allow us to conclude when governmental action does surpass that point. Also, just as the reasonable expectations of privacy test allows for societal opinions of what is acceptable government action to guide its determination of reasonable, partial search theory does the same. The reasonable expectations of privacy test, which is the standard bearer in Fourth Amendment analysis, also does not explicate when an individual's expectations become reasonable, but it, just as partial search theory, allows a general principle by which judges can create a body of law.[150] The very test that has guided Fourth Amendment analysis for the decades, namely the reasonable expectations of privacy standard, as articulated by Justice Harlan, offers reasoned guidance in applying mosaic theory.[151] When the amount of data collected by the government becomes so intrusive that the subject of the surveillance had a reasonable expectation of privacy in that mass of data, a search has been conducted, which requires a warrant or some other recognized exception to the warrant requirement.[152]

2. Legal support for partial search theory

Partial search theory, while novel, has its roots in various United States Supreme Court decisions.[153] In addition, the theory's creation is a reaction to the changing role in society of

---

149. *See* Orin Kerr, *Answering Justice Alito's Question: What Makes an Expectation of Privacy 'Reasonable'?*, WASH. POST (May 28, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/28/answering-justice-alitos-question-what-makes-an-expectation-of-privacy-reasonable/ (discussing and summarizing jurisprudence related to *Katz*).

150. *See id.* (arguing that the subjective-expectations prong of the *Katz* test is irrelevant).

151. *See Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

152. *Id*.

153. *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014); *Jones*, 132 S. Ct. at 954; *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

technology and the conclusion that the law cannot rely on archaic notions of constitutional law.[154] The framers of the Constitution expected society to evolve,[155] and while they could not have foreseen today's specific technologies, they expected the Constitution to have continued meaning for structuring American life, which involves a continuing evolution of the interpretive theories used to apply the Constitution's text.

Katz supports the creation of partial search theory, as the accumulation of the partial-searches becomes a search when the subject of the intrusions has a reasonable expectation of privacy in the collection of intrusions. Both *Riley* and *Jones* also support the creation of this Note's proposal. *Riley* discusses various issues related to applying traditional Fourth Amendment jurisprudence to modern technology.[156] Chief Justice Roberts, in the majority decision, states that searching one's cellular phone incident to lawful arrest "would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[157] From this analogy, he concludes that there are so many small pieces of information in the citizens' electronics that searching through them—even if justified under traditional legal doctrine—is too intrusive to be legal under the text of the Constitution.[158] The

---

154. *See, e.g.*, *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (suggesting the third-party doctrine may be "ill suited to the digital age").

155. *See generally* M'Culloch v. State, 17 U.S. 316, 407 (1819) ("A constitution, to contain an accurate detail of all the subdivisions of which its great powers will admit, and of all the means by which they may be carried into execution, would partake of the prolixity of a legal code, and could scarcely be embraced by the human mind. It would probably never be understood by the public. Its nature, therefore, requires, that only its great outlines should be marked, its important objects designated, and the minor ingredients which compose those objects, be deduced from the nature of the objects themselves.").

156. *Riley*, 134 S. Ct. at 2484 ("These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life.").

157. *Id.* at 2491.

158. The government in *Riley* argued that the search of the cellular phone was justified under the search incident to arrest exception to the warrant requirement. *Id.* at 2486. This exception is well-established, yet the Court ruled against the government and decided to distinguish the petitioner's case due to the pure volume of information contained in a cell phone, as compared to the typical level of intrusiveness of a search under this exception. *Id.* 2494–95. This reasoning should also apply to third-party doctrine. Even if this is a well-established doctrine, the use of mass surveillance allows for potential courts to distinguish from traditional third-party cases.

Court's reasoning for finding a search has occurred is that this level of intrusion becomes categorically different because "[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so."[159]

In *Jones*, Justice Sotomayor and Justice Alito's concurrences also warn against falsely analogizing between past technologies and present, advancing ones.[160] As mentioned above, Justice Sotomayor's concurrence questions whether third-party doctrine needs to be reworked in the light of modern technology.[161] Justice Alito's concurrence expressly references mosaic theory by noting that the continued surveillance of the appellant, for twenty-eight days, created an unreasonable search.[162] Both of these concurrences make use of mosaic theory, but do not address the issues associated with the theory.[163] Those problems are solved by partial search theory.

Another decision favorable to partial search theory comes from the D.C. Circuit Court of Appeals, not the United States Supreme Court. In *Maynard*, the court decided that the discrete, incomplete searches by the government accumulate into a constitutionally protected search.[164] In doing so, the court adopted mosaic theory.[165] The Eleventh Circuit also alluded to the need to rethink third-party doctrine, and possibly adopt mosaic theory.[166] Two other federal district courts have alluded to the possible need for mosaic theory in

159. *Id*. at 2489.

160. United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); *Id.* at 957 (Alito, J., concurring).

161. *Id.* at 957 (Sotomayor, J., concurring).

162. *Id*. at 957–58 (Alito, J., concurring).

163. *See, e.g.*, *id*. at 954 (Sotomayor, J., concurring).

164. *See* United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010), *aff'd in part sub nom. Jones*, 132 S. Ct. 945.

165. *Id.* at 562.

166. United States v. Davis, 754 F.3d 1205 (11th Cir.) (determining that one cell phone data point can reveal private information), *vacated and en banc reh'g granted*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014) (*Davis* has been vacated as it awaits rehearing *en banc*).

light of modern technologies, albeit not in the context of NSA surveillance.[167]

Computer science expert, Edward Felten, also highlights the dangers of metadata collection through his declaration in *ACLU v. Clapper*.[168] Metadata can disclose records of individual calls, a caller's records maintained over time, and an aggregation of various callers' records kept over time.[169] When discussing individual calls, "metadata is often a proxy for content."[170] These records have the potential to disclose highly sensitive information or information denoting associationalties.[171] Collection of a caller's records over time also allows insight into their private life, associations, and relationships.[172] Further, aggregate records over time allow the government to reach factual conclusions about an individual's actions that other records would not illustrate.[173]

In addition to the explicit reasoning and holdings from various court decisions, partial search theory is founded in a broader, more general principle. The law must adapt in order to protect citizens from arbitrary, unjustified, and unlawful intrusions into their privacy.[174] The framers of the Constitution

---

167. *See* United States v. White, 62 F. Supp. 3d 614, 620–24 (E.D. Mich. 2014) (finding that the defendant had a reasonable expectation of privacy in his whereabouts over the course of the 30 day investigation because of the accumulation of small intrusions, but ultimately denying Defendant's motion to suppress evidence because the officers acted in good-faith reliance on their warrant, thus not triggering the exclusionary rule); United States v. Vargas, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672, *1–3 (E.D. Wash. Dec. 15, 2014) (granting motion to suppress video evidence from a camera installed without a warrant 100 yards away from the defendant's home that displayed the defendant's front lawn continuously for six weeks, on grounds that the surveillance constituted an unreasonable search).

168. Declaration of Professor Edward W. Felten, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13 Civ. 3994), ECF No. 27, http://ia801803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf [Hereinafter Felten].

169. *Id*. at 13–14.

170. *Id*. at 14.

171. *Id*. at 15–16. These concerns with association, specifically political associations, parallel the thesis of Professor Desai. *See generally* Desai, *supra* note 130, *passim* (arguing that mass surveillance chills associational freedom).

172. Felten, *supra* note 168, at 17.

173. *Id*. at 21–22.

174. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); United States v. White, 401 U.S. 745, 757 (1971) (Douglas, J., dissenting).

realized that times would change and that the interpretation of the Constitution would need to adapt to match the times.[175] Extensive technologies that allow for the mass surveillance of every U.S. citizen and advances in popular technology, through things such as smart phones, were not the subject of the Fourth Amendment when it was drafted. As a result, the Constitution, and the doctrines used to decide constitutional cases, must be re-evaluated to protect the public's rights. Mosaic theory is an attempt to afford this protection, but even it has its issues.[176] Partial search theory realizes the evolving nature of technology, the stagnancy of the law, and creates a theory, through comparison to intrusiveness of a search and the *Katz* test, which limits the amorphous nature of the mosaic theory.

The United States Supreme Court has issued various opinions that support that creation of partial-search theory.[177] *Jones* and *Riley* illustrate the reluctance to use third-party doctrine under modern conditions,[178] while *Katz* relates the partial search theory back to the doctrinal foundation of the reasonable expectations of privacy test.[179] While acting as explicit legal support for this theory, these cases also illustrate the more general principle that the United States Constitution, specifically the Fourth Amendment, was drafted in a time far removed from the modern technological amenities.[180] As the framers likely did not foresee the extent of government surveillance, even if said surveillance is justified, mass surveillance requires rethinking Fourth Amendment analysis. Similarly, the framers did not foresee things such as smart phones, which allow for large amounts of information pertaining to one's life to be held in a single location, out of the home, and able to be accessed by the government.

---

175. *E.g.*, M'Culloch v. State, 17 U.S. 316, 406–07 (1819).

176. *See supra* Section II.B.1 (discussing issues with mosaic theory).

177. *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014); *Jones*, 132 S. Ct. at 954 (2012); Katz v. United States, 389 U.S. 347 (1967); *M'Culloch*, 17 U.S. at 407.

178. *See Riley*, 134 S. Ct. at 2484; *Jones*, 132 S. Ct. at 956–57 (Sotomayor, J., concurring).

179. *See Katz*, 389 U.S. at 360 (Harlan, J., concurring) (explaining the reasonable expectations test).

180. *See, e.g.*, *Riley*, 134 S. Ct. at 2484 (the court analyzed the search warrant requirement for modern cell phones "[a]bsent . . . precise guidance from the founding era").

3. Application of partial search theory

The creation of partial search theory, in conjunction with mosaic theory, has huge ramifications for government surveillance, and for Fourth Amendment analysis generally.[181] It can be assumed that, since the NSA collects so many different types of information from people, the number of pieces, notwithstanding the probative weight of any piece of information, will lead to the NSA's warrantless surveillance programs being unconstitutional.[182] In order to avoid suppression, the government must either enact safeguards so that the level of intrusiveness reached by surveillance programs does not reach the level in *Katz* or get an individualized warrant for the surveillance of individuals.

Partial search theory does not completely distort Fourth Amendment analysis, but at the same time allows courts to adjust to the tactics the federal government has used to circumvent the Fourth Amendment. While still allowing the government to search those it suspects of committing serious crimes, especially terrorism, partial search theory protects the civil liberties of the American populace and requires the government to take steps to protect the privacy of its citizens rather than arbitrarily and unnecessarily trample on their rights.[183] Most importantly, partial search theory allows the Fourth Amendment, third-party doctrine, and mosaic theory to adjust to advancing technologies.[184] While there are other

---

181. This is due to the extensive amount of data captured by the agency. In 2010, the *Washington Post* estimated that the NSA collected 1.7 billion communications. Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST (July 19, 2010), http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control.

182. *Cf.* Gentithes, *supra* 9, at 38 ("More plausibly, mosaic theory's supporters might claim that there is a collective Fourth Amendment interest shared by a group as large as all citizens using telecom services, one that is infringed by a program as broad as the NSA's. That collective interest is not based upon privacy, but is instead derived from the ideal of tranquility woven into the structure of the Constitution and implicit in Justice Brandeis's expression of the Fourth Amendment's primary goal—to protect citizens' 'right to be let alone.'" (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting))); Kayyali, *supra* note 58.

183. *Cf.* Steele, *supra* note 2 (outlining the vastness of the information collected by the NSA); Kayyali, *surpa* note 58.

184. *See* United States v. Jones, 132 S. Ct. 945 (2012); United States v. Maynard, 615 F.3d 544, 562–63 (D.C. Cir. 2010) (discussing the need to adopt mosaic theory in light on modern technology), *aff'd in part sub nom.*

issues, which still persist even in the presence of partial search theory, this theory realizes that accumulated information can reach the level of a search, and that the populous has a reasonable expectation of privacy in these highly descriptive bits of information.[185] The population may assume that government surveillance only affects the criminal, and thus the issue is not of concern, but this thinking is misguided and dangerous, as, when analyzing modern surveillance, "every person is the victim, for the technology we exalt today is everyman's master."[186]

The passage of the USA Freedom Act offers a unique perspective to the future of third-party doctrine and mosaic theory, as it offers more protections for citizens than the Patriot Act did.[187] However, these protections are statutory only, not constitutional.[188] Legislative measures may in fact be the proper way to address surveillance, and "raise[s] the possibility that the third party doctrine should simply be left alone."[189] Third party doctrine is flawed, as highlighted by Justice Sotomayor in *Jones*,[190] and because of this imperfection, "legislatures, rather than courts, may be the proper agents to calibrate law enforcement needs with privacy concerns."[191] Legislative solutions allow for the more flexibility than constitutional safeguards, and the tradeoff between privacy and security is arguably better suited to be determined by the democratic process.[192] Additionally, Orin Kerr argues that since the Fourth Amendment typically offers all or nothing protections, legislative solutions allow for "a middle ground not possible under the Fourth Amendment."[193]

---

185. *See Jones*, 132 S. Ct. at 945; *Maynard*, 615 F.3d at 562–63.

186. United States v. White, 401 U.S. 745, 757 (1971) (Douglas, J., dissenting).

187. *See* Chappell, *supra* note 4.

188. *See* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 996 (2016).

189. *Id*.

190. Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring).

191. Issacharoff & Wirshba, *supra* note 188, at 996 (noting the use of legislative protections such as the Right to Financial Privacy Act, the Pen Register Act, and the Electronic Communications Privacy Act of 1986).

192. *See id*.

193. Orin S. Kerr, *The Case for the Third Party Doctrine,* 107 MICH. L. REV. 561, 597 (2009).

Certain differences between the Freedom Act and Patriot Act may alleviate privacy concerns. Specifically, the Freedom Act requires "reasonable, articulable suspicion" that a "specific selection term" used to request telephone data is associated with terrorism before a FISC order is granted.[194] However, as there is a reasonable expectation of privacy in the accumulation of metadata,[195] probable cause is required to avoid a Fourth Amendment violation,[196] not simply reasonable suspicion. Nevertheless, it remains to be seen how the newly fashioned, legislative protections of the USA Freedom Act will operate in practice, due mainly to the act's infancy.

4. How can non-searches become a search?

The issue of where an accumulation of non-searches becomes a search also requires examining how a non-entity, namely a non-search, can become an entity, namely a search.[197] However, the response to this becomes clear by following the analysis of the proceeding section. It is inaccurate to characterize NSA's intrusions as non-searches, instead they are partial searches that in isolation do not warrant constitutional protections, but once added together do reach the level of a search.[198] If the intrusions are characterized in this manner, the logical impossibility of non-searches becoming a search is no longer present and the second chronicled issue with mosaic theory disappears.

III. CONCLUSION

With the advantages of modern technology come new challenges to individual privacy. The government's capacity to surveil individuals, as well as the ability of citizens to store their entire lives in electronic devices, has created a perfect storm for substantial government surveillance. After Edward

---

194. USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101, 129 Stat. at 270 (codified at 50 U.S.C.A. § 1861 (West 2015)).

195. *See See* Klayman v. Obama, 957 F. Supp. 2d 1, 29–42 (D.D.C. 2013). *Cf.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd in part sub nom. Jones*, 132 S. Ct. 945.

196. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

197. *See* Gentithes, *supra* note 9, at 37.

198. *Cf. Jones*, 132 S. Ct. 945. *Maynard*, 615 F.3d at 562–63, *aff'd in part sub nom.*

Snowden's disclosure of the extent of the NSA's surveillance, the American people have become more aware, and arguably less accepting, towards government surveillance.[199] One aspect of these realizations, which received extra attention, was the metadata collection program taken part in by the NSA. The attention this program drew was largely due to the amount of information it collects.

Each piece of information captured by the government is wrongly characterized as a non-search by third-party and mosaic theorists. Instead, they are partial searches—each not deserving Fourth Amendment safeguards in isolation. However, each of these partial searches, when added together, eventually reach the level of intrusiveness of a search, as viewed through the reasonable expectations of privacy test put forth in *Katz*.[200] Thus, at this point a warrant is required. So, the government must put in place safeguards to keep the level of intrusiveness below that point, or get a warrant in fear of suppressing all the information it has gathered.

This analysis also responds to the second critique of mosaic theory, as the intrusions should not be categorized as non-searches, but as partial searches that accumulate into a search. Government surveillance and modern technology offer new challenges to traditional Fourth Amendment analysis. Mosaic theory attempts to remedy these issues, but brings issues of its own. However, characterizing third-party data collection as partial searches, rather than non-searches addresses those issues, does not result in total upheaval of the third-party doctrine, and promotes new oversight into government surveillance.

199. *See* Gao, *supra* note 1.

200. *Katz*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

***