Can You Hear Me Now? Time To Consider Whether Cell Phone Providers Are State Actors

I cannot imagine a more "indiscriminate" and "arbitrary invasion" than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on "that degree of privacy" that the Founders enshrined in the Fourth Amendment.[1]

I. INTRODUCTION

A study of smartphone users found that seventy-nine percent of respondents have their phones on or near them for almost their entire waking day.[2] By 2017, an estimated 67.8% of the U.S. population will use smartphones.[3] The increased adoption of smartphones changed the detail and frequency of how people interact with each other and within their communities, yielding intimate information about the individual user's relationships.[4] In June 2013, Edward Snowden, a former National Security Agency (NSA) contractor, became notorious for leaking classified information detailing a government program to collect cell phone metadata, also known as transactional information, and location information on virtually every U.S. citizen.[5] Transactional information is data individual users generate when their cell phones interact with outside entities, including businesses, organizations, and websites.[6] Snowden admits that he leaked the information to start a public debate about privacy and the morality of the government collection program.[7] The leaked

1. Klayman v. Obama, 957 F. Supp. 2d 1, 42 (D.D.C. 2013) (admonishing government collection effort).

2. IDC, ALWAYS CONNECTED: HOW SMARTPHONES AND SOCIAL KEEP US ENGAGED 9 (2013), http://www.nu.nl/files/IDC-Facebook%20Always%20Connected%20%281%29.pdf [http://perma.cc/CKP4-GNQ6] (highlighting significant personal interaction with smartphones).

3. *See id*. at 3 (estimating future smartphone usage). By 2017, IDC projects 222.4 million people will use smartphones. *See id.*

4. *See id*. at 16-17, 23 (detailing evolving human interaction with technology).

5. *See Edward Snowden Was NSA Prism Leak Source-Guardian*, BBC NEWS (June 10, 2013), http://www.bbc.com/news/world-us-canada-22836378 [http://perma.cc/64R3-KJ3E] (reporting Edward Snowden leaked U.S. government information); 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 [http://perma.cc/YPR5-HHN6] (explaining scope of U.S. government collection effort).

6. *See* NAT'L RESEARCH COUNCIL OF THE NAT'L ACADEMIES, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 98 n.26 (2008), http://fsi.stanford.edu/sites/default/files/Protecting_Individual_Privacy.pdf [http://perma.cc/MA26-X479] (defining "transactional information").

7. *See* Barbara Starr & Holly Yan, *Man Behind NSA Leaks Says He Did It To Safeguard Privacy,*

information, however, may have created a new problem for cell phone service providers in forcing them to afford their subscribers constitutional privacy protections, a role usually reserved to the state.[8]

The Constitution applies almost exclusively to government conduct and not to the conduct of private actors.[9] This concept is known as the state action doctrine, meaning private actors do not need to comply with the Constitution.[10] Private citizens or corporations, however, must conform to the Constitution if their actions fit either the exclusive public function or significant state involvement exceptions to the state action doctrine.[11]

The Constitution guarantees the right to privacy under the Fourth Amendment.[12] In a mobile society, anchored by constant communication and social connection with our communities, the privacy rights secured by the Constitution are increasingly important.[13] Cell phone providers are at the intersection of individual privacy interests and state collection programs; they are private actors that provide an estimated 181.4 million Americans with smartphone access.[14]

This Note will examine the history of the state action doctrine and the privacy protections afforded by the Constitution.[15] In Part II, this Note will

Liberty, CNN (June 23, 2013), http://www.cnn.com/2013/06/10/politics/edward-snowden-profile/ [http://perm a.cc/YCN5-Y2QL] (stating Snowden's intent leaking information).

8. *See* U.S. CONST. amend. IV (providing individual privacy rights). The Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." *Id.*

9. *See* Franz v. United States, 707 F.2d 582, 591 n.33 (D.C. Cir. 1983) (explaining "state action" refers to any government action at any level); Erwin Chemerinsky, *Rethinking State Action*, 80 NW. U. L. REV. 503, 507 (1985) (stating Constitution applies to governmental conduct, not private behavior). *But see* U.S. CONST. amend. XIII, § 1 (prohibiting both government and private actors from engaging in slavery or involuntary servitude). The Thirteenth Amendment is the only constitutional amendment that applies to both the government and private actors. *See* U.S. CONST. amend. XIII, § 1.

10. *See infra* Part II.B (explaining exceptions when Constitution applied to private citizens); Chemerinsky, *supra* note 9, at 507-09 (asserting private citizens' and corporations' infringement on constitutional values shielded from judicial action).

11. *See* Terry v. Adams, 345 U.S. 461, 469-70 (1953) (holding private organization must comply with Constitution). In *Terry*, a private organization fit the public function exception to the state action doctrine because it ran an election for public office—a responsibility traditionally and exclusively given to the state. *See id.*; *see also* Lombard v. Louisiana, 373 U.S. 267, 273-74 (1963) (holding state directed segregation of private restaurant unconstitutional). In *Lombard*, the Court held that Louisiana was significantly involved in the matters of a private entity by way of enforcing a statute compelling segregation in restaurants, thus making the private restaurant state actors subject to the Constitution. *See Lombard*, 373 U.S. at 273-74.

12. *See* U.S. CONST. amend. IV (establishing limit of government power to encroach on individual privacy rights).

13. *See* IDC, *supra* note 2, at 4-5 (noting personal nature of mobile phones important to social connection).

14. *See id.* at 3 (projecting in 2013, 57.3% of U.S. population will use smartphones).

15. *See* U.S. CONST. amend. IV (providing citizens with protections against unreasonable searches and seizures); U.S. CONST. amend. XIV, § 1 (establishing citizenship and privacy rights and outlining prohibitions on state action).

explore the purpose behind the state action doctrine's construction.[16] Next, this Note will describe the test for applying the state action doctrine to private conduct and identify exceptions to state action.[17] This Note will then explain cell phone carriers' technology, infrastructure, and data collection practices.[18] This Note will also discuss the applications of location data and will identify laws governing data collection of individual subscribers.[19] Also in Part II, this Note will consider the privacy protections guaranteed by the Constitution and the doctrinal approaches to analyzing privacy rights.[20] This Note will then argue why the state action doctrine must apply to cell phone carriers.[21] Finally, this Note will argue cell phone subscriber location data deserves constitutional protection under the Fourth Amendment.[22]

II. HISTORY

A. State Action Doctrine

State action is action conducted by a government entity at any level.[23] The state action doctrine prohibits a government entity from conducting a "state action" that infringes upon an individual's constitutional rights.[24] The state action doctrine thereby creates a distinction between government and private actions to protect individual rights from the unique danger of government power.[25]

The state action doctrine is a key component of the Fourteenth Amendment.[26] The Fourteenth Amendment creates "negative rights" or restraints on the power of the government over the people.[27] The constitutional

16. *See infra* Part II.A.
17. *See infra* Part II.B.
18. *See infra* Part II.C.1.
19. *See infra* Part II.C.2.
20. *See infra* Part II.D.
21. *See infra* Part III.A.
22. *See infra* Part III.B.
23. *See* Daphne Barak-Erez, *A State Action Doctrine for an Age of Privatization*, 45 SYRACUSE L. REV. 1169, 1171-72 (1995) (discussing origin of state action doctrine).
24. *See id.* (addressing constraint on government power).
25. *See id.* at 1171 (explaining purpose of state action doctrine).
26. *See* Wilson R. Huhn, *The State Action Doctrine and the Principle of Democratic Choice*, 34 HOFSTRA L. REV. 1379, 1380 (2006) (stating state action doctrine part of Fourteenth Amendment). A state action must infringe on a fundamental right to trigger constitutional protections. *See id.*
27. U.S. CONST. amend. XIV, § 1 (protecting citizens from state and governmental infringement on "life, liberty, or property"); Susan Bandes, *The Negative Constitution: A Critique*, 88 MICH. L. REV. 2271, 2273 (1990) (asserting Constitution provides negative rights—restraints on government power rather than affirmative government duties).

> No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

restraints apply only to government entities—the Constitution does not protect against private citizen or corporate action.[28] Seven years after the Fourteenth Amendment's ratification, the Supreme Court solidified the requirement for state action through the holding that the Constitution applies only to government entities, not private citizens.[29] Four years after this initial decision, the Court held that private citizens may deny other citizens basic constitutional protections, such as equal protection, without violating the Constitution.[30] The Constitution is, therefore, limited because courts have no authority to stop private actions that infringe on constitutionally protected values.[31] The prohibition on slavery is the only provision in the Constitution that applies directly to private citizens as well as the government.[32]

The state action doctrine may apply to private parties when the relationship between the government and the private action is so significant that the government is effectively responsible for the activity.[33] In *Marsh v. Alabama*,[34] an Alabama deputy sheriff arrested private citizens for distributing religious material on the sidewalk of a company-owned town.[35] The Court held that Alabama allowed a private corporation to oversee a community like a government entity, and, therefore, that private corporation could not restrict private citizens' constitutional rights.[36] *Marsh* carved out an exception to the state action doctrine for private entities conducting a "public function" to

U.S. CONST. amend. XIV, § 1.

28. *See* Chemerinsky, *supra* note 9, at 507-08 (explaining Constitution applies to state action, or governmental actions).

29. *See* United States v. Cruikshank, 92 U.S. 542, 554 (1875) (holding Fourteenth Amendment prohibits states from violating Constitution, not citizens violating rights of other citizen); *see also Primary Documents in American History: 14th Amendment to the U.S. Constitution*, LIBR. CONG., http://www.loc.gov/rr/program/bib/ourdocs/14thamendment.html (last visited Nov. 19, 2015) [http://perma.cc/77S2-XZYE] (stating Fourteenth Amendment ratified July 9, 1868, seven years before *Cruikshank* decision).

30. *See* Virginia v. Rives, 100 U.S. 313, 318 (1879) (holding private citizens may deny other citizens equal protection because citizens not state entities). The Supreme Court held, "The provisions of the Fourteenth Amendment . . . have reference to State action exclusively, and not to any action of private individuals." *Id.*

31. *See* Chemerinsky, *supra* note 9, at 508-09 (noting inability to protect individuals against constitutional rights infringements by private actors). The Constitution cannot stop private entities from engaging in discriminatory or inappropriate conduct. *See id.*

32. *See* U.S. CONST. amend. XIII, § 1 (prohibiting private citizens from engaging in slavery). "Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction." *Id.*

33. *See* Chemerinsky, *supra* note 9, at 508 (explaining exception to state action doctrine requiring private-entity compliance with Constitution).

34. 326 U.S. 501 (1946).

35. *See id.* at 502 (describing characteristics of company-owned town).

36. *See id.* at 509 (holding Constitution applied to private entity). As a result of treating the corporation as a governmental entity, the Constitution applies, and the corporation cannot deny First Amendment rights. *See id.*

comply with the Constitution.[37] In *Shelley v. Kraemer*,[38] the state government enforced a racially restrictive covenant on the sale of real property.[39] A private citizen sued to restrict an African-American couple from taking possession of a home in a neighborhood subject to a racially restrictive covenant.[40] The Court reasoned that there is state action when private parties employ the "full coercive power of government," or "state powers in all forms," to deny other parties rights guaranteed by the Constitution.[41] The Supreme Court held that when the government, like in *Shelley*, is substantially "entangled" with a private actor or action that denies constitutional protections, there is state action requiring the private actor to comply with the Constitution.[42]

B. Test To Apply State Action Doctrine to Private Conduct

There is no universally accepted test for determining when the connection between government and private action is sufficient to establish state action.[43] Determining whether an action constitutes state action requires a case-by-case analysis to decide if there is a sufficient government connection to a private entities' activity.[44] That fact-specific analysis often yields unpredictable results because it requires courts to sort through details and weigh them in the context of case-specific circumstances.[45] The Supreme Court, however, held that state action might come in two forms—public function and entanglement—when the

37. *See id.* (recognizing public function exemption for private conduct). The Court reasoned that there is no significant constitutional difference between prohibiting a corporation that operates a public road from interfering with the public use of the road and allowing a corporation to use its property as a "business block," or town, open to the public from interfering with public use of the town. *Id.* at 507. The Court identified the public nature of the town's operation and held it to be a public function, requiring the corporation to comply with the Constitution. *See id.* at 506.

38. 334 U.S. 1 (1948).

39. *See id.* at 19-20 (examining private action, sanctioned by state, violated Constitution). The Court found that judicial enforcement of a racially restrictive covenant is state action because the "full panoply of state power" actively prevented a qualified purchaser from taking legal possession of property because of race. *Id.* at 19.

40. *See id.* at 6 (detailing commencement of suit to uphold restrictive covenant). A racially restrictive covenant prevented the conveyance of land in a residential community to a purchaser of the "Negro or Mongolian race" for a period of fifty years beginning in 1911. *Id.* at 4-5.

41. *Id.* at 19-20. Courts must uphold constitutional demands when private parties employ state power to resolve disputes. *See id.* at 20.

42. *See* Chemerinsky, *supra* note 9, at 508 n.19 (identifying entanglement exception to state action when substantial state involvement in private action). Courts analyze the magnitude of the connection between state and private action that implicates a liberty interest. *See* Dilan A. Esper, Note, *Some Thoughts on the Puzzle of State Action*, 68 S. CAL. L. REV. 663, 682-83 (1995). There is no clear standard for how much government entanglement in private action constitutes state action. *See id.* at 687. A "traditionally well-protected" constitutional interest, however, is more likely to succeed as a state action claim. *Id.*

43. *See* Robert J. Glennon, Jr. & John E. Nowak, *A Functional Analysis of the Fourteenth Amendment "State Action" Requirement*, 1976 SUP. CT. REV. 221, 221 (1976) (observing limitation on state action analysis).

44. *See id.* at 224 (highlighting critical criteria to find state action).

45. *See id.* at 221-22 (focusing on Court's difficult task of applying subjective evaluations consistently).

relationship between government and private actions are essentially actions of the government.[46] The public function exception exists when a private entity performs a function traditionally and exclusively reserved to the state.[47] Government tolerance of a private party's actions to conduct a public function is indicative, but not determinative, of state action.[48] The second exception, entanglement, occurs when the government encourages, authorizes, or facilitates a private entity to violate the Constitution.[49] The entanglement exception requires more than the involvement of the government to license, regulate, or fund the private actor or action.[50]

In *Edmonson v. Leesville Concrete Co.*,[51] the Supreme Court discussed a two-part test to determine what constitutes state action.[52] First, the private party's action that caused the deprivation of a constitutional right or privilege must have its source in government authority.[53] Second, the private party must be able to be described as a state actor.[54] To evaluate the second part of this test, a court considers "the extent to which the [private] actor relies on governmental assistance and benefits; whether the actor is performing a traditional government function," and if government authority aggravated the injury.[55]

C. Cell Phone Carriers and Data Collection

1. Cell Phone Technology

Three-quarters of the world's population can acquire cell phone service.[56]

46. *See* Chemerinsky, *supra* note 9, at 508 n.19 (evaluating different cases establishing public function and entanglement exceptions to state action). *Compare* Brentwood Acad. v. Tennessee Secondary Sch. Athletic Ass'n, 531 U.S. 288, 290 (2001) (holding public school athletic association's imposition of sanctions constituted state action), Jackson v. Metro. Edison Co., 419 U.S. 345, 351 (1974) (asserting necessary inquiry when government and state action sufficiently close), *and* Lombard v. Louisiana, 373 U.S. 267, 273-74 (1963) (holding state action when city officials upheld racially restrictive custom in local restaurant), *with* Moose Lodge No. 107 v. Irvis, 407 U.S. 163, 177 (1972) (holding state-issued liquor license used in lodge not sufficient entanglement for state action).

47. *See* 16C C.J.S. *Constitutional Law* § 1845 (2015) (identifying public function exception to state action).

48. *See id.* (articulating tolerance aids in determining state action).

49. *See* John L. Watts, *Tyranny by Proxy: State Action and the Private Use of Deadly Force*, 89 NOTRE DAME L. REV. 1237, 1239 (2014) (defining entanglement exception to state action).

50. *See* MARCY STRAUSS, LOYOLA LAW SCH.,THE FIRST AMENDMENT: AN INTRODUCTION TO THE LAW, 337, 340 (2002) (noting interpretation requirements for entanglement exception).

51. 500 U.S. 614 (1991).

52. *See id.* at 620 (listing two prongs of test for existence of state action); *see also* Lugar v. Edmondson Oil Co., 457 U.S. 922, 936 (1982) (outlining approach for determining whether violation of constitutional right "fairly attributable" to state).

53. *See Edmonson*, 500 U.S. at 620 (stating private conduct must exercise state authority).

54. *See id.* (indicating private party's actions must be objectively similar to government actions).

55. *Id.* at 621-22 (citations omitted) (listing three-factor analysis to determine state action for second part of test).

56. *See* Naomi Canton, *Cell Phone Culture: How Cultural Differences Affect Mobile Use*, CNN (Sept.

One of the distinguishing features of cell phones is that they allow people to be readily available at any time or location.[57] To enable cell phone service, cellular phone providers must apply to the Federal Communications Commission (FCC) for licenses to operate on specific electromagnetic radio frequencies (spectrum).[58] The FCC allocated spectrum licenses to 734 geographic markets in the United States; cell phone providers can purchase a spectrum license in one of those geographic markets to operate its cellular networks.[59] Cell phone providers' cellular networks use spectrum licenses to allow cell phones to transmit sound, data, and video information wirelessly to nearby cellular towers.[60] Cell phones must relay their location data to nearby cellular towers to facilitate persistent and reliable wireless service.[61] An exchange of location data between cell phones and towers, or registration, occurs approximately every seven seconds when a phone is on, without any action needed by the cell phone user.[62]

Cell phone carriers divide a service area or city into individual cells to provide a reliable cell phone signal.[63] Each cell is usually ten square miles and serviced by a base station that includes a cell tower and radio equipment.[64] As a cell phone user moves within and between the different cells in a service area, the user's cell phone continuously registers with the nearest cell's base station to access the cell phone carrier's network.[65] While the phone is on, the information provided to the cell's base station yields an accurate picture of the user's past and present locations.[66] Cell phone carriers determine a cell phone user's location by using the cell phone's global positioning system (GPS) technology or by triangulating the physical distance of the cell phone from the

28, 2012), http://www.cnn.com/2012/09/27/tech/mobile-culture-usage/index.html [http://perma.cc/6XPG-ZDWA] (detailing world-wide access to cell phone service).

57. *See* Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 422 (2007) (noting cell phones' pervasive existence in daily life).

58. *See* 47 U.S.C. § 303(y) (2012) (granting FCC statutory authority to manage U.S. spectrum).

59. *See Cellular Service*, FED. COMM. COMM'N, http://www.fcc.gov/encyclopedia/cellular-service (last visited Nov. 20, 2015) [http://perma.cc/B9F4-D399] (describing cell phone spectrum license background and process for cell providers to purchase licenses).

60. *See* Michael Harris, *How Cell Towers Work*, UNISON 2 (2011), http://www.unisonsite.com/pdf/resource-center/How%20Towers%20Work.pdf [http://perma.cc/FS4B-88AQ] (detailing cell tower operations); *Spectrum Dashboard API*, FED. COMM. COMM'N, http://www.fcc.gov/developers/spectrum-dashboard-api (last visited Nov. 20, 2015) [http://perma.cc/P66Q-E2DU] (listing electromagnetic spectrum uses by private companies).

61. *See* McLaughlin, *supra* note 57, at 426 (explaining cell phones automatically interact with cell towers to provide service).

62. *See id.* (describing cell phone registration process).

63. *See* Marshall Brain et al., *How Cell Phones Work*, HOWSTUFFWORKS, http://electronics.howstuffworks.com/cell-phone.htm (last visited Nov. 20, 2015) [http://perma.cc/G68A-CZ7Z] (outlining cell phone service technology and infrastructure).

64. *See id.* (describing cell phone service technology).

65. *See id.* (noting continuous data exchange between cell phone and cellular network).

66. *See* McLaughlin, *supra* note 57, at 426-27 (explaining cell phone registration process to determine location).

base stations in each cell.[67] During triangulation, the base station's radio equipment intercepts the registration signals from active cell phones and measures the time and angle of the signal when it arrives at the base station.[68] Each base station in contact with a cell phone compares time and angle measurements to approximate the location of the cell phone user and create a "virtual map of [a user's] movements."[69]

2. Application of Location Services

Cell phone carriers use customer location data for a variety of purposes—both governmental and commercial.[70] Cell phone carriers share cell phone data with the government during emergencies to ensure public safety.[71] Local governments leverage cell phone location data to improve city administration and traffic planning efforts.[72] One commercial use for cell phone data includes utilizing a cell phone subscriber's location data to tailor advertising through location-based services.[73] In 2013, Verizon became the first company to sell customer location data to third parties, providing tailored location-based

67. *See* President & Fellows of Harvard Coll., *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308-09 (2004) (articulating cell phone triangulation process).

68. *See id.* (describing cell phone base station process to determine cell phone location).

69. *Id.* at 309.

> When a cell phone connects with a provider's tower . . . the tower measures the amount of time it takes for the signal to leave one location and reach the other . . . . [T]he tower measures the time it takes for the signal to get from the tower to the phone. These time measurements make it possible to estimate the distance between the tower and the phone . . . . [A]n algorithm allows the system [base station] to determine . . . the phone's latitude and longitude . . . [and] angle-of-arrival technology uses signals between the cell tower and wireless phone to determine location.

Id. at 308-09.

70. *See AT&T Privacy Policy*, AT&T, http://www.att.com/gen/privacy-policy?pid=2506 (last visited Jan. 3, 2015) [http://perma.cc/UNT9-HWU2] (explaining customer data used to improve cell phone networks, cell service, and tailor services); *Privacy Policy: Full Privacy Policy*, VERIZON, https://www.verizon.com/about/privacy/policy/ (last updated Dec. 2015) [https://perma.cc/Z98K-HRM7] (maintaining service provider uses customer data to tailor service and improve network); *Sprint Corporation Privacy Policy*, SPRINT, http://www.sprint.com/legal/privacy.html (last updated May 2, 2014) [http://perma.cc/827Y-ZRTF] (advising customer's data used to improve service, respond to legal processes, and personalize advertising); *T-Mobile Privacy Policy*, T-MOBILE, http://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy (last updated Nov. 25, 2015) [http://perma.cc/E99W-ENFE] (stating customer data used to provide service and data analysis and to personalize advertising).

71. *See* McLaughlin, *supra* note 57, at 422 (noting 911 emergency tracking uses cell phone location data).

72. *See* Emily Badger, *You Already Own the Next Most Important Transportation Planning Tool*, CITYLAB (Feb. 3, 2012), http://www.citylab.com/tech/2012/02/you-already-own-next-most-important-transportation-planning-tool/1124/ [http://perma.cc/ZK9M-28U2] (announcing North Carolina Capital Area Metropolitan Planning Organization employing cell phone location data).

73. *See* McLaughlin, *supra* note 57, at 422 (describing cell phone location tracking beneficial for marketing purposes).

advertising to cell phone subscribers.[74] Major cell phone providers—AT&T, Sprint, T-Mobile, and Verizon—retain user location data ranging from four months to two years, making commercialization of cell phone transactional information possible.[75]

Law enforcement agencies recognize the value of location data and utilize the information to enhance investigations.[76] In 2012, government investigators requested cell phone data from cell carriers approximately 1.1 million times.[77] Not all of the 1.1 million requests were for location data; some included requests for text messages, voicemails, call history, and other information.[78] While law enforcement agencies can obtain location data from cell carriers, some agencies purchased technology to collect cell phone location data independently.[79] One such technology local police departments employ is the Stingray.[80] The Stingray is a mobile device installed in a police vehicle that

74. *See* Alexis Kleinman, *Verizon Selling Customers' Cell Phone Data: Report*, HUFFINGTON POST (May 22, 2013), http://www.huffingtonpost.com/2013/05/22/verizon-selling-customer-data_n_3320680.html [http://perma.cc/KK5K-6YUF] (reporting cell phone carrier monetizes user phone data). Verizon sells user data through a product called Precision Market Insights. *See id.* Precision Market Insights associates a unique identifier to a Verizon user's cell phone, and that unique identifier correlates a user's demographic, interest, and geographic information to create a composite picture of that cell phone user. *See* Precision Mkt. Insights, *Precision Market Insights—the Precision ID-HD*, VIMEO, http://vimeo.com/109847536 (last visited Jan. 2, 2015). Third-party advertisers buy this precise information from carriers to tailor subscriber-specific advertising. *See id.*

75. *See Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU (Aug. 2010), https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart [https://perma.cc/9RWF-HUMY] (explaining commercial data retention policies). The American Civil Liberties Union (ACLU) acquired the data retention information from a document the Department of Justice produced to advise law enforcement officers seeking data from cell phone providers. *See id.*

76. *See Cell Phone Location Tracking Public Records Request*, ACLU, https://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request (last updated Mar. 25, 2013) [https://perma.cc/XQF5-FUFL] (reporting virtually all police departments responding to request for information use location data). The ACLU filed 380 public record requests with law enforcement agencies for information on cell phone location tracking policies, procedures, and practices. *See id.* The ACLU reported that approximately 250 police departments responded, and nearly all of the departments utilized cell phone location data. *See id.* The ACLU noted that only a minority of the responding departments obtained a warrant and demonstrated probable cause to acquire location data. *See id.* The released documents that the ACLU obtained indicate the legal standards to obtain location data vary. *See id.* The ACLU explained that some departments demonstrate probable cause to obtain a warrant, while others obtain data when it is "relevant and material." *Id.*

77. *See* Kashmir Hill, *This Is How Often Your Phone Company Hands Data Over to Law Enforcement*, FORBES (Dec. 10, 2013), http://www.forbes.com/sites/kashmirhill/2013/12/10/this-is-how-often-your-phone-company-hands-data-over-to-law-enforcement/ [http://perma.cc/8CHH-9MCV] (reporting records request from law enforcement to cell phone companies).

78. *See id.* (listing types of information law enforcement requests from phone companies).

79. *See* Letter from Kate Weiby & Tim Dorn, Gilbert, Ariz. Police Dep't, to Dan Pochoda, ACLU (Sept. 6, 2011), https://www.aclu.org/files/cellphonetracking/20120328/celltrackingpra_gilbertpd_gilbertaz.pdf# [https://perma.cc/CY56-C33N] (noting police department purchased cell phone tracking equipment).

80. *See* Drew Mikkelsen, *Tacoma, Wash., Police Use Cell-Phone Tracking Device*, USA TODAY (Aug. 28, 2014), http://www.usatoday.com/story/news/nation-now/2014/08/28/cell-phone-tracking-stingray/14751105/ [http://perma.cc/54QZ-QTBC] (detailing Tacoma police's Stingray collection system).

mimics a cell phone tower.[81] Nearby cell phones connect to the Stingray's mimicked cell tower signal and pass user data directly to the police, bypassing the need for more expensive traditional police tracking techniques.[82]

Use of the cell carrier's network is critical to providing government entities with the ability to track suspects affordably.[83] Location tracking costs police departments as little as $0.04 per hour compared to approximately $250 per hour for traditional, covert foot pursuit.[84] Given the economic incentive to use cell phone tracking technologies, government use of location data is likely to increase.[85]

3. Laws Governing Cell Phone Providers

During the early 1970s, the U.S. government conducted covert domestic spying programs on its citizens.[86] In response, Congress created the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee) to investigate domestic spying operations.[87] The Church Committee discovered a range of programs collecting information on U.S. citizens.[88] To limit the power of the intelligence community, Congress passed the Foreign Intelligence Surveillance Act (FISA), which adopted numerous protections for citizen's privacy.[89] Before collection, FISA required the government to show the electronic intercept's association

81. *See id.* (explaining Stingray operates as cell tower to determine location of phones nearby).

82. *See id.* (describing how cell phones connect to Stingray).

83. *See* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 349 tbl.1 (2014) (calculating per hour cost for different surveillance techniques).

84. *See id.* (presenting economic incentive for police departments to use tracking technologies). Sprint charges the lowest cost to the government, $0.04 per hour for twenty-eight days, to track an individual user through cell phone location data. *See id.* The monetary difference between covert foot pursuit and using Sprint is $249.96 per hour. *See id.*

85. *See id.* at 349 (demonstrating large financial disparity expected to increase, as tracking rates likely to decrease over time).

86. *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL'Y 757, 766 (2014) (detailing history of government surveillance of its own citizens).

87. *See id.* (explaining domestic spying consequences and legislative reaction). Senator Frank Church led the Church Committee to discover the scope of the domestic spying programs. *See id.*

88. *See id*. at 770 (declaring Church Committee report found surveillance compromised privacy rights). The Church Committee took testimony from intelligence agencies, the Internal Revenue Service, the Post Office, and other federal agencies. *See id.* at 769. The Church Committee discovered that the government conducted domestic spying operations under the pretense of foreign intelligence collection. *See id*. at 770. During the course of the investigation, the Church Committee discovered numerous concerning programs collecting large amounts of U.S. citizens' communications, including Project MIRANET, which focused on U.S. citizens traveling to Cuba, and Operation SHAMROCK, which is an agreement by major telegraph operators to disclose international telegraphs to the Department of Defense. *See id.* at 772-74.

89. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-1813 (2012)) (providing procedures for electronic surveillance and punishments for violations); Donohue, *supra* note 86, at 766 (stating congressional intent to create FISA).

with a specific person or agent of a foreign power.[90] The legislation also incorporated electronic surveillance minimization procedures and created the Foreign Intelligence Surveillance Court (FISC) to oversee collection requests.[91]

Today, two laws directly influence the data disclosure requirements of cell phone providers.[92] The first law is the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act (USA FREEDOM Act), which replaced the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) that expired in 2015.[93] The second law is the Stored Communications Act.[94] The government may compel production of cell phone subscribers' records that are relevant to a foreign intelligence threat investigation.[95] Also, the government requires cell phone providers to maintain records of phone data and location information for emergency responses.[96] From the repository of stored cell phone communication data, the government may order disclosure of a subscriber's records and location data.[97]

a. USA FREEDOM Act

After the terrorist attacks on September 11, 2001, Congress passed the USA PATRIOT Act to improve intelligence collection.[98] In 2005, Congress amended Section 215 of the USA PATRIOT Act (Section 215) to become more consistent with the FISA provisions established in 1978.[99] Since 2006, the

90. *See* Donohue, *supra* note 86, at 766 (inferring target must have tie to foreign threat or entity to satisfy FISA). Specifically, the government may not use an electronic intercept to target a U.S. person if justification is based solely on a First Amendment-protected activity. *See id.*

91. *See* 50 U.S.C. § 1801(h) (2012) (establishing minimization procedures for electronic surveillance); Donohue, *supra* note 86, at 766-67 (stating court created to oversee process). The legislation adopted the following actions to minimize electronic surveillance: the Attorney General has the authority to adopt procedures that minimize or prohibit acquiring, retaining, or circulating information on unconsenting U.S. persons that is not publicly available; the government may not disseminate information on unconsenting U.S. persons unless the "[U.S.] person's identity is necessary to understand foreign intelligence information"; and the government may not disclose or retain contents of a U.S. person's electronic communications for longer than seventy-two hours unless under court order or the Attorney General determines the electronic information suggests there is a threat of death or serious bodily injury to any person. 50 U.S.C. § 1801(h).

92. *See* Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2012) (stating requirement to disclose customer communications and records); USA FREEDOM Act, Pub. L. No. 114-23, § 101, 129 Stat. 268 (2015) (creating procedures and safeguards in regards to acquiring communication information).

93. *See* USA FREEDOM Act, Pub. L. No. 114-23, § 101, 129 Stat. 268 (2015).

94. *See* Stored Communications Act, 18 U.S.C. §§ 2701-2712 (2012) (stating requirement to disclose customer communications and records).

95. *See* USA FREEDOM Act § 101 (authorizing *government* collection of telephone metadata).

96. *See* 47 C.F.R. § 20.18 (2015) (listing cell phone location tracking requirements).

97. *See* 18 U.S.C. § 2703(a) (2009) (listing required disclosure for customer communications or records).

98. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272 (2001) (establishing tangible goods provision allowing government to require production of records).

99. *See* Donohue, *supra* note 86, at 801 (asserting Section 215 closely aligned to FISA provisions). Section 215 requires that an application include reasonable grounds that the "tangible things" requested are

government interpreted Section 215 to authorize the bulk collection of phone metadata.[100] In 2015, the Second Circuit ruled that the bulk collection of metadata exceeded the scope of Section 215.[101] After the Second Circuit's decision, on June 1, 2015, Congress allowed the USA PATRIOT Act to expire; on June 2, 2015, the President signed the USA FREEDOM Act into law as a comprehensive reform of the telephone metadata bulk collection program.[102]

The USA FREEDOM Act curtails the government's authority to collect data and provides more transparency into FISC decisions.[103] To reduce government authority, the USA FREEDOM Act requires the Federal Bureau of Investigation (FBI)—before receiving daily production of telephone metadata—to demonstrate reasonable grounds that the requested data is relevant to an investigation and a reasonably articulable suspicion that the requested data is tied to a foreign agent or power.[104] If the FBI successfully receives a FISC order for daily production of cell phone data, the USA FREEDOM Act limits the cell phone metadata production to 180 days, with an extension available upon an additional application and court approval.[105] Additionally, to increase FISC transparency, the USA FREEDOM Act requires the Director of the Administrative Office of the United States Courts to report the total number of production applications and approved orders to Congress annually.[106]

relevant to the investigation and the purpose of the foreign intelligence threat investigation. *Id.* at 801-02. In addition, the government may not direct the request at a U.S. person solely based on First Amendment-protected activity. *See id.* at 802.

100. *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 796 (2d Cir. 2015) (stating government permitted bulk collection of metadata from phone service providers according to Section 215).

101. *See id.* at 826 (holding government's interpretation of Section 215 erroneous; bulk collection violates Section 215). *Clapper* did not address Section 215's constitutional issues; instead, the court ordered the district court to reconsider the case based on the holding that the telephone bulk collection program exceeded the scope of the law. *See id.*

102. *See* Bruce Zagaris, *U.S. Congress Limits Surveillance with Passage of the USA FREEDOM Act*, 31 No. 6 INT'L ENFORCEMENT L. REP. 214 (2015) (outlining history of USA PATRIOT Act and passage of USA FREEDOM Act).

103. *See id.* (explaining overarching goals of USA FREEDOM Act).

104. *See* USA FREEDOM Act § 101. Under the USA FREEDOM Act, if the government applies for an ongoing production of phone records to protect the United States against international terrorism, it must provide:

> a statement of facts showing that—
> (i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term . . . are relevant to [an] investigation; and (ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities . . . or an agent of a foreign power . . . .

Id.

105. *See* USA FREEDOM Act § 101 (authorizing collection for 180 days before requiring additional application and judicial finding).

106. *See* USA FREEDOM Act § 603(a) (listing information required in report, including number of applications and orders granted, modified, or denied).

b. Stored Communications Act

In 1996, the FCC finalized Enhanced 911 (E911) rules.[107] The E911 rules require cell phone providers to institute technology to allow government approximation of a cell phone user's location.[108] Cell phone providers instituted network and handset-based technologies to meet the FCC requirements regarding the location of cell phone users.[109] Cell phone providers store the user's location information for billing purposes and to respond to future government inquiries.[110] The Stored Communications Act allows the government to require cell phone providers to disclose a user's cell phone records upon receipt of a warrant, court order, or when a subscriber consents to disclosure of information.[111] To compel a service provider to disclose a cell phone subscriber's records—by court order—the government must offer specific facts showing reasonable grounds that the requested cell phone records are relevant to an ongoing criminal investigation.[112]

D. Privacy

1. Constitutional Privacy Protections

The Constitution guarantees the right to privacy through the Fourth Amendment.[113] The Fourth Amendment protects individual privacy by

107. *See* 47 C.F.R. § 20.18 (2015) (codifying 911 service regulations); Wireless E911 Location Accuracy Requirements, 79 Fed. Reg. 17,820 (proposed Mar. 28, 2014) (to be codified at 47 C.F.R. 20) (detailing E911 history).

108. *See* 47 C.F.R. § 20.18(e), (h) (listing cell phone location tracking requirements). Location accuracy standards for network-based technologies requires 100 meters accuracy for sixty-seven percent of calls and 300 meters accuracy for ninety percent of calls. *See id.* §§ 20.18(h)(1)(i)-(ii). By 2013, the regulations required location accuracy for handset-based technologies to be 50 meters for sixty-seven percent of calls and 150 meters for eighty percent of calls. *See id.* § 20.18(h)(2)(i).

109. *See* Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 384-86 (2003) (listing methods cell providers use to meet FCC requirements).

110. *See id.* at 381 (stating cell phone providers keep location data for business records and government information requests).

111. *See* 18 U.S.C. §§ 2703(b)(2)(c)(A)-(E) (2012) (listing cell phone provider's disclosure requirements). The government's standard from the Stored Communications Act to receive a court order requiring disclosure of cell phone location data is lower than the probable cause standard. *See* Katz v. United States, 389 U.S. 347, 357 (1967) (acknowledging warrantless search violates Fourth Amendment, subject to narrow circumstances); *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011).

112. *See* 18 U.S.C. § 2703(d) (stating requirement to obtain court order demanding disclosure). In 2008, a court considered whether the government may obtain prospective cell phone location data without showing probable cause. *See In re* U.S. for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices, 632 F. Supp. 2d 202, 204 (E.D.N.Y. 2008). The government argued that the combination of the Pen Register statute and the Stored Communications Act gave the government authorization to receive a prospective cell phone location under a "hybrid theory." *Id.* The majority of courts, including the one in that case, rejected this legal reasoning and denied the government prospective cell phone location data. *See id.* at 204-05.

113. *See* U.S. CONST. amend. IV (establishing constitutional right to privacy).

prohibiting the government from conducting "unreasonable searches and seizures."[114] The government must obtain a court order based upon probable cause before searching or seizing an individual's property to comply with the constitutionally protected right.[115] The Supreme Court defined a "search" in the Fourth Amendment context as an infringement of "an expectation of privacy that society is prepared to consider reasonable."[116] The Court then identified a "seizure," stating, "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[117]

Despite these two distinct elements of the Fourth Amendment, issues concerning whether a violation of an individual's constitutional privacy interest occurred often depend on whether the government's action constituted a search.[118] Courts apply the *Katz* test to determine if a form of investigation violates the unreasonable search provision of the Fourth Amendment.[119] The Court explained that the *Katz* test applies a two-part inquiry: whether an individual has a subjective expectation of privacy, and whether society recognizes the expectation of privacy as reasonable.[120] For example, *Katz* considered whether a telephone booth is a constitutionally protected area.[121] *Katz* held government eavesdropping on private conversations conducted inside a telephone booth constitutes a search and seizure under the Fourth Amendment.[122]

The bar on unreasonable searches and seizures balances privacy and security.[123] Under this framework, the Constitution protects an individual's

114. U.S. CONST. amend. IV (stating Amendment's protections); Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 475 (2012) (outlining Fourth Amendment protections and exemptions).

115. *See* U.S. CONST. amend. IV (providing limitation on government authority by requiring probable cause before partaking in search or seizure).

116. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

117. *Id.* The Court acknowledged that case law does not fully discuss a seizure of property. *See id.* at 113 n.5. The Court adopts the definition of "seizure of property" from the definition of "seizure" related to an individual's freedom of movement. *Id.*

118. *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) (identifying video monitoring and vehicle tracking as Fourth Amendment considerations); Illinois v. Caballes, 543 U.S. 405, 407 (2005) (determining whether narcotics-detecting dog used during speeding stop violates Fourth Amendment); Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding scanning home with thermal imaging device violates Fourth Amendment).

119. *See* McAllister, *supra* note 114, at 475 (identifying *Katz* test as method to determine improper search).

120. *See id.* at 475-76 (explaining *Katz* test and subjectivity of its application).

121. *See* Katz v. United States, 389 U.S. 347, 349 (1967) (stating issue considered in case).

122. *See id.* at 353 (articulating government electronic surveillance of citizens' phone calls in phone booth violates Constitution). *Katz* determined government eavesdropping was an illegal search and seizure because the government did not obtain a warrant before conducting surveillance on a targeted individual using a telephone booth. *See id.* at 357. The Court reasoned that making a phone call from a private telephone booth creates an expectation of privacy for the caller. *See id.* at 352.

123. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 574 (2009) (framing Fourth Amendment's unreasonable search and seizure provision as compromise between privacy and security).

privacy from government intrusion, while also allowing the government reasonable access to activity conducted in public.[124] The distinction between public and private conduct is necessary because most crimes require parts of the offense to occur in public.[125] Without acknowledging the right of the government—or law enforcement—to observe public activity, the Fourth Amendment individual privacy protections may supersede the value of bringing criminals to justice.[126]

2. Doctrinal Approaches To Analyzing Privacy Rights

a. The Third-Party Doctrine

Two conventional approaches have emerged to analyze privacy rights: the Third-Party Doctrine (Doctrine) and the Mosaic Theory (Theory).[127] The Doctrine is a rule, rooted in the Fourth Amendment, which controls the collection of evidence from third parties.[128] The rule explains, "By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed."[129] Specifically, when an individual discloses information to a third party, there is no expectation of privacy, and the Fourth Amendment does not apply.[130] Many criticize the Doctrine as a misguided interpretation for three reasons: there may be a reasonable expectation of privacy when disclosing information to third parties, the Doctrine gives the government too much power, and the Fourth Amendment bars the government from collecting highly personal information in cell phones without cause.[131]

First, commenters question the basis of the Doctrine because many

124. *Compare* Payton v. New York, 445 U.S. 573, 586 (1980) (stating warrantless search inside home presumptively unreasonable), *with* California v. Ciraolo, 476 U.S. 207, 213 (1986) (stating Fourth Amendment does not require government to "shield eyes" from public activity).

125. *See* Kerr, *supra* note 123, at 574-75 (offering criminals normally must leave private spaces to commit crimes). Kerr notes that allowing governmental access to publicly visible activity may lead to warranted searches of private spaces to solve crimes in the public interest. *See id.* at 575.

126. *See id.* (positing balance between privacy and security important to society).

127. *See* Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1810 (2014) (discussing Theory after *United States v. Jones*); Kerr, *supra* note 123, at 563 (discussing Doctrine).

128. *See* Kerr, *supra* note 123, at 563 (stating Doctrine's Fourth Amendment origin).

129. *Id.*

130. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining conversations "in plain view" of public not protected). In his concurrence, Justice Harlan noted that the Doctrine requires the speaker to exhibit an actual expectation of privacy and society to recognize the speaker's expectation as reasonable. *See id.*

131. *See* Kerr, *supra* note 123, at 564, 572 (observing academics' critiques of Doctrine); Devon Ombres, *NSA Domestic Surveillance from the PATRIOT Act to the FREEDOM Act: The Underlying History, Constitutional Basis, and the Efforts at Reform*, 39 SETON HALL LEGIS. J. 27, 38-39 (2015) (explaining technological changes requiring more interaction with third parties does not diminish fundamental liberties). Kerr states that commentators, as well as many state court judges, almost unanimously opine the Doctrine is incorrect. *See* Kerr, *supra* note 123, at 564.

disclosures to third parties occur with the reasonable expectation of privacy required by the Fourth Amendment.[132] The Supreme Court justified the Doctrine by remarking that people who disclose communications to a third party "assume[] the risk" that their information will end up with the police.[133] The Court made "risk analysis dispositive," meaning individuals communicating private information through means they expect the government may monitor, assumes the risk of government monitoring, which limits their reasonable expectation of privacy.[134] As Justice Marshall noted in *Smith*, a problem with the Doctrine is that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[135] Consequently, for many subscribers, cell phones are arguably a vital piece of personal and professional life, and, under the Doctrine, the mere use of cell phone technology constructively constitutes consent to government surveillance.[136]

Second, commentators note the Doctrine is functionally inconsistent with a free society because it places too much power in the government.[137] In modern society, people must interact with third-party vendors for cell phone services and other technologies; therefore, if the Fourth Amendment does not protect information given to third-party vendors, the resulting harm of unchecked government surveillance will frustrate the expression of ideas.[138]

Third, the Fourth Amendment bars the government from collecting highly

132. *See* Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1314-15 (1981) (arguing modern society requires telephone use, and individual should not assume risk numbers dialed disclosed); Kerr, *supra* note 123, at 571 (declaring Justices' failure to see privacy expectation in third-party records as "out of touch"). Furthermore, Ashdown argues that people have a reasonable expectation that the contents of telephone communication are private and should be free from uncontrolled government seizure. *See* Ashdown, *supra*, at 1315.

133. Smith v. Maryland, 442 U.S. 735, 744 (1979).

134. *Id.* at 750 (Marshall, J., dissenting). *Smith* held there is no reasonable expectation of privacy when dialing phone numbers because it conveyed the information to a third party—the phone company. *See id.* at 745 (majority opinion). The Fourth Amendment does not protect the information conveyed to a third party; thus, the government's use of a pen register is constitutional. *See id.* at 745-46. Justice Marshall, in his dissent, posited that the majority's emphasis on assumption of the risk defines the scope of the Fourth Amendment. *See id.* at 750 (Marshall, J., dissenting). If the government stated its intent to intrude on a person's privacy, the individual could not have a reasonable expectation of privacy because the person assumed the risk. *See id*. at 749 (Marshall, J., dissenting).

135. *Id*. at 750 (Marshall, J., dissenting).

136. *See id.* (discussing problem with Doctrine). Analogizing between Justice Harlan's comments on landline telephones and cell phones leads to a logical conclusion that, under the Doctrine, using a cell phone constitutes a user's tacit consent for government monitoring of activity. *See id.*

137. *See* United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting) (suggesting Doctrine threatens liberty to communicate freely); Kerr, *supra* note 123, at 572 (exploring critique of Doctrine's function in free society). Specifically, with respect to the Doctrine in the context of undercover informants, Justice Harlan states, "[T]hird-party bugging . . . undermine[s] that confidence and sense of security . . . between citizens in a free society." *White*, 401 U.S. at 787 (Harlan, J., dissenting).

138. *See* Kerr, *supra* note 123, at 572-73 (articulating Doctrine's functional criticism in modern communication regarding third parties).

personal information contained in metadata without cause.[139] The Doctrine allows the government, however, to bypass Fourth Amendment protections by compelling third parties to disclose personal data the government could otherwise not collect.[140] A strict application of the Doctrine in the cell phone context means there is no reasonable expectation of privacy in cell phone use because subscribers must disclose metadata, location data, and actual contents of communication to third parties—cell phone providers—to utilize modern communication technology.[141]

b. The Mosaic Theory

The Theory is the second approach to analyzing the Fourth Amendment's privacy protections.[142] The Theory argues that long-term monitoring of an individual can violate the Fourth Amendment.[143] Specifically, long-term GPS surveillance, or location tracking, creates an aggregate total picture of the monitored person's daily activities and is tantamount to an unreasonable

139. *See* City of Ontario, Cal. v. Quon, 560 U.S. 746, 759 (2010) (acknowledging changes in technology do not limit constitutional protections). "Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy." *Id.* at 760; *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 39 (D.D.C. 2013) (discussing reasonable expectation of privacy in telephone metadata; stating bulk data collection likely violates Constitution).

140. *See* Brad Turner, *When Big Data Meets Big Brother: Why Courts Should Apply* United States v. Jones *To Protect People's Data*, 16 N.C. J.L. & TECH. 377, 423 (2015) (identifying Doctrine as government work-around to Fourth Amendment privacy protections). The Doctrine is poorly suited for the digital age because people share personal information with third parties to complete daily tasks. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (stressing information voluntarily shared with third parties may deserve constitutional protections); *see also* Turner, *supra*, at 423. The Doctrine allows the government to obtain highly intrusive personal data without Fourth Amendment scrutiny. *See* Turner, *supra*, at 423.

141. *See* Kerr, *supra* note 123, at 563 (stating no expectation of privacy with information disclosed to third parties); McLaughlin, *supra* note 57, at 426 (explaining cell phones interact with third-party-owned cell towers to provide continual service).

142. *See* Bedi, *supra* note 127, at 1810-11 (articulating Supreme Court introduced Theory to analyze Fourth Amendment). Bedi states the Court applied the Theory as a means to protect against long-term government surveillance. *See id.*

143. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (arguing Fourth Amendment search occurs when government monitors individual's locations over time). Traditionally, tracking an individual's movements through public areas was not considered a Fourth Amendment search. *See* United States v. Knotts, 460 U.S. 276, 282 (1983). *Knotts*, however, did not address dragnet style collection of an individual cell phone user's location data as a violation of Fourth Amendment privacy protections. *See In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 117 (E.D.N.Y. 2011). The public has a reasonable expectation of privacy in all of its movements collected over time because prolonged surveillance may reveal private information not obtainable from tracking a single or short trip. *See* United States v. Maynard, 615 F.3d 544, 561-63 (D.C. Cir. 2010). *Maynard*, for example, states aggregation of a person's movements reveals a detailed portrait that would be unknown if the government tracked only a single movement because the composition can indicate if the individual "is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband . . . or [associated with] political groups." *Id.* at 562. *Maynard* recognized that surveillance over one month sufficiently violates an individual's expectation of privacy because the movements are not constructively exposed to the public. *See id.* at 561-62.

search.[144] Justice Alito, in his concurrence in *Jones*, argued that society's expectation of privacy assumes protection against a government that is secretly monitoring a person's movements in the aggregate.[145] Commentators argue that even a single instance of surveillance can reveal private information that a monitored individual would want to remain secret.[146] Even though long-term monitoring may appear to be a privacy right violation, because these activities occur in public, the Public Disclosure Doctrine applies and limits the effectiveness of the Theory.[147] Under this Public Disclosure Doctrine, voluntary disclosure to the public forfeits Fourth Amendment protections, similar to disclosure to a third party under the Doctrine.[148] Thus, accepting the Theory as a viable approach to analyzing the Fourth Amendment requires the Supreme Court to alter or abandon the Public Disclosure Doctrine and the Doctrine.[149]

III. ANALYSIS

Cell phone carriers—private entities—must adhere to the Constitution if their conduct falls under an exception to the state action doctrine, and they violate a right that the Constitution protects.[150] Cell phone carriers' conduct fits an exception to the state action doctrine because they collect, store, and produce subscriber location data as the government requires.[151] Cell phone carriers also violate the right to privacy under the Fourth Amendment because carriers continuously collect cell phone subscriber location data, which deserves constitutional protection.[152] Consequently, cell phone carriers are state actors and must adhere to the Constitution.[153]

144. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (stating aggregating recorded movements violated reasonable privacy expectations).

145. *See id*. at 964 (Alito, J., concurring) (stating long-term GPS monitoring infringes on privacy expectations).

146. *See* Bedi, *supra* note 127, at 1812 (noting brief surveillance impacts privacy). Bedi offers that a single instance of a monitored individual's trip to a religious gathering or political function could reveal compromising information. *See id.*

147. *See id*. at 1811 (stating public movements do not provide privacy expectation).

148. *See id*. at 1811, 1813 (stating limitation to Theory).

149. *See* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 402 (2013) (stating change in Supreme Court interpretation required to make Theory viable).

150. *See* Chemerinsky, *supra* note 9, at 507-08 (explaining state action doctrine occasionally requires private entities to comply with Constitution).

151. *See* 18 U.S.C. § 2703 (2012) (stating required disclosure of customer communications or records); USA FREEDOM Act § 101(a)(3)(C) (authorizing production of telephone records after demonstrating reasonable articulable suspicion of foreign threat); 47 C.F.R. § 20.18 (2015) (listing requirements for tracking cell phone user locations); *see also* Edmonson v. Leesville Concrete Co., 500 U.S. 614, 621-22 (1991) (establishing two-part test to find state action).

152. *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (arguing long-term location monitoring during government investigations impinges on privacy expectations).

153. *See* Chemerinsky, *supra* note 9, at 508 (stating private entity satisfying state action exemption must

A. Why the State Action Doctrine Should Apply to Cell Phone Carriers

Private entities must adhere to the Constitution if their conduct fits either the public function or entanglement exception.[154] Cell phone providers are private entities that collect and store cell phone subscriber metadata and, upon government direction, produce subscriber data to aid law enforcement activities.[155] Cell phone providers, therefore, fit both the public function and entanglement exceptions to the state action doctrine.[156]

Although the government does not traditionally and exclusively provide cellular phone service, carriers may qualify under the public function exception because law enforcement—a traditional government function—uses cellular service technologies.[157] Since carriers' cell phone networks and cell phone location tracking technologies assist the government in conducting law enforcement investigations—a role exclusively and traditionally the province of the state—cell phone carriers are state actors.[158] A private entity meets the entanglement exception to the state action doctrine if it employs the "full coercive power of government."[159] Cell phone carriers may qualify as state actors under the entanglement exception because the government went beyond licensing carriers to operate cellular networks through enacting statutes that encouraged, authorized, and facilitated cell phone carriers to encroach on subscribers' Fourth Amendment privacy rights.[160]

comply with Constitution).

154. *See id.* at 508 n.19 (listing differences between public function and entanglement exceptions).

155. *See* 18 U.S.C. § 2703 (requiring disclosure of customer communications or records); USA FREEDOM Act §§ 101-102 (authorizing government to require cell phone providers produce subscriber telephone records); 47 C.F.R. § 20.18 (listing 911 location tracking requirements); *see also Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, *supra* note 75 (explaining cell phone provider data retention policies).

156. *See* Chemerinsky, *supra* note 9, at 508 n.19 (discussing differences between state action doctrine exceptions).

157. *See Spectrum Dashboard API*, *supra* note 60 (listing spectrum licenses held by private entities); *see also supra* note 47 and accompanying text (describing public function exemption). Spectrum licenses are issued to private cell phone service providers, indicating the federal government does not operate commercial cell phone networks. *See Spectrum Dashboard API*, *supra* note 60.

158. *See* 16C C.J.S. *Constitutional Law* § 1845 (2015) (identifying public function as exclusive state prerogative); *Cell Phone Location Tracking Public Records Request*, *supra* note 76 (reporting government cell phone location tracking request activity).

159. Shelley v. Kraemer, 334 U.S. 1, 19-20 (1948) (holding state action when private entity employs state power to resolve disputes); *see also supra* note 49 and accompanying text (defining requirements of entanglement exception).

160. *See* U.S. CONST. amend. IV (establishing privacy rights); 18 U.S.C. § 2703 (2012) (codifying required disclosure of customer communications or records); 47 U.S.C. § 303(y) (2012) (authorizing cell phone providers to use spectrum); USA FREEDOM Act § 101(a)(3)(C) (authorizing production of telephone records after demonstrating reasonable articulable suspicion of foreign threat); 47 C.F.R. § 20.18 (2015) (listing requirements for tracking cell phone user locations). The government requires carriers to collect and maintain subscriber locations to facilitate government assistance during emergencies. *See* 47 C.F.R. § 20.18. Through the USA FREEDOM Act and the Stored Communications Act, government investigators can seek court orders compelling cell phone carriers to disclose customer transactional data, which they are required to collect and

Further, cell phone carriers that collect and maintain customer location data are state actors.[161] Federal laws are the source of government authority that requires cell phone providers to collect and store user location data, thereby turning cell phone providers into investigative agents for the government.[162] Cell phone carriers do not rely on government financial assistance to maintain cellular networks; however, carriers do rely on the government regulation of the licensing of spectrum to facilitate access to cell phone service.[163] Cell phone carriers collect, store, and produce records of cell phone subscribers' transactional data for law enforcement agencies, assisting the government in conducting a traditional and exclusive state function of law enforcement.[164] Carriers are state actors under both the public function and entanglement exception because they are legally obligated to collect subscriber information and, upon a valid request, to turn over the information for law enforcement activities, which encroaches on the privacy interests of individual subscribers.[165]

B. Subscriber Location Data Deserves Constitutional Privacy Protection

Cell phone subscribers have a reasonable expectation of privacy in their location data.[166] Under *Katz*, a reasonable expectation of privacy aids in determining whether there is a Fourth Amendment violation.[167] Therefore, cell

maintain to aid in ongoing investigations. *See* 18 U.S.C. § 2703; USA FREEDOM Act §§ 101-102; 47 C.F.R. § 20.18. Subscribers have a reasonable expectation of privacy that does not include long-term location monitoring. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

161. *See* Chemerinsky, *supra* note 9, at 508 (explaining government responsible for activity when nexus between government and private actors great). Cell phone carriers provide smartphone access to an estimated 181 million subscribers. *See* IDC, *supra* note 2, at 3.

162. *See* 18 U.S.C. § 2703 (requiring disclosure of electronic communications or records); 47 C.F.R. § 20.18 (listing requirements for tracking cell phone user locations).

163. *See* 47 U.S.C. § 303(y) (providing FCC with authority to manage spectrum); *Cellular Service*, *supra* note 59 (describing licensing process and management process).

164. *See* Greenwald, *supra* note 5 (reporting *Verizon* required to provide government with telephone records on "ongoing daily basis"); *Cell Phone Location Tracking Public Records Request*, *supra* note 76 (reporting government cell phone location tracking request activity).

165. *See* U.S. CONST. amend. IV (establishing individual privacy rights); 18 U.S.C. § 2703 (2012) (creating disclosure requirement for cell phone providers); USA FREEDOM Act § 101 (providing FBI with authority to order production of call records against international terrorism); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (noting long-term monitoring encroaches on privacy expectation); *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring) (stating Fourth Amendment search occurs when government monitors individual's location over time); 47 C.F.R. § 20.18 (2015) (listing requirements for tracking cell phone user locations); *see also* Chemerinsky, *supra* note 9, at 508 (explaining state action when government responsible for private activity); *Cell Phone Location Tracking Public Records Request*, *supra* note 76 (articulating cell phone location requests by law enforcement to providers).

166. *See* McLaughlin, *supra* note 57, at 426 (explaining cell phone continuously registers with cell towers without user interaction).

167. *See supra* notes 121-122 and accompanying text (detailing *Katz* inquiry into whether Fourth Amendment violation occurred).

phone subscribers' data deserves constitutional privacy protections.[168]

Individual cell phone subscribers have a subjective expectation of privacy in their location data.[169] Cell phones continuously register with nearby cellular towers to allow reliable cellular service.[170] It is unreasonable to infer that a cell phone subscriber surrenders an expectation of privacy because he or she carries a cell phone, regardless of whether the individual is actively using the device.[171] In 1981, scholars acknowledged that modern society requires telephone use.[172] Since 1981, cellular phones have replaced landline telephones, but the necessity of having a phone in modern society remains.[173] A cell phone that creates even a single location record without the subscriber's consent can reveal compromising information and violate a subscriber's reasonable expectation of privacy.[174] Therefore, carriers turning over subscriber data to the government cause injury to an individual's privacy interest, which the Constitution protects.[175] A subscriber's records contain location data and other transactional information that deserves protection under the Fourth Amendment.[176]

Society recognizes a reasonable expectation of privacy in location data.[177]

168. *See* Kerr, *supra* note 123, at 572-73 (highlighting criticism to Doctrine's application to modern communication). Both the Doctrine and the Public Disclosure Doctrine are ill suited for cell phone technologies because subscribers must share information, location data, and other transaction information with carriers (third parties) and, as a consequence, lose Fourth Amendment privacy protection. *See* Bedi, *supra* note 127, at 1811-13, 1841 (discussing Public Disclosure Doctrine and ubiquitous use of cell phones).

169. *See* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (stating reasonable expectation of privacy violated by aggregating recorded movements).

170. *See* President & Fellows of Harvard Coll., *supra* note 67, at 309 (explaining cell phone providers must determine phone location to enable call).

171. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (noting government monitoring "chills" personal expressive freedoms, and government data collection susceptible to abuse); McAllister, *supra* note 114, at 482-83 (reporting empirical survey results indicating individual respondents had privacy expectation in location data); McLaughlin, *supra* note 57, at 426 (explaining cell phones communicate with cell towers while powered on).

172. *See* Ashdown, *supra* note 132, at 1314 (noting necessity of phone communications).

173. *See id.* at 1314-15 (inferring landline telephone evolution to cell phone technology does not diminish phone importance to society); *see also* IDC, *supra* note 2, at 9 (noting survey respondents had phones nearby for all but two hours of waking day).

174. *See* U.S. CONST. amend. IV (establishing privacy rights); Bedi, *supra* note 127, at 1812 (noting brief surveillance impacts privacy).

175. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (noting long-term monitoring encroaches on privacy expectation); *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring) (stating Fourth Amendment search occurs when government monitors individual's location over time).

176. *See* Bedi, *supra* note 127, at 1812 (noting brief surveillance impacts privacy); *AT&T Privacy Policy*, *supra* note 70 (explaining customer data retained during cell phone network use); *Privacy Policy: Full Privacy Policy*, *supra* note 70 (describing customer data used for data analysis and personalized advertising); *Sprint Corporation Privacy Policy*, *supra* note 70 (acknowledging customer data collected during network use); *T-Mobile Privacy Policy*, *supra* note 70 (detailing customer data collected used for data analysis).

177. *See* Greenwald, *supra* note 5 (reporting government collection of call data). In a letter to Attorney General Eric Holder, United States Senators Wyden and Udall contend, "[T]here is now a significant gap between what most Americans *think* the law allows and what the government secretly *claims* the law allows." *Id*. (emphasis added). Greenwald notes that telephone records allow the government to identify every person

In *Jones*, the Court acknowledged that the government secretly monitoring a person's movement over a long period of time violates society's expectation of privacy.[178] The Doctrine and the Public Disclosure Doctrine are limiting the judicial branch from universal acceptance of a societal expectation of privacy in cell phone data.[179] Additionally, the Doctrine is poorly suited for the digital age because citizens must share personal information, such as location data, with third parties to conduct daily business.[180] A contemporary approach to analyzing privacy rights in a long-term context is the Theory.[181] Cell phone users have a reasonable expectation that their location data or transactional information is safe from continuous government monitoring, and given the pervasive presence of cell phones, society accepts this expectation as reasonable.[182]

As state actors, cell phone carriers must comply with the privacy protections guaranteed by the Fourth Amendment.[183] Cell phone carriers must adjust their policies on handling subscriber data.[184] Limiting collection of transactional data is not a viable solution because current cell phone technology requires a cell phone to register and pass transactional information with nearby cell towers continuously to enable service.[185] Cell phone carriers instead must seek to limit the retention of cell phone transactional information and location data to comply with a subscriber's right to privacy.[186] Carriers should adopt policies to retain user data for as short a time as possible unless court ordered to

who communicates, their location, and the time of their communication. *See id.*

178. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (recognizing long-term surveillance violates society's privacy expectations).

179. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979) (holding disclosing private information to third parties assumes government monitoring risk); United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting) (arguing Doctrine threatens liberty to communicate freely).

180. *See* Turner, *supra* note 140, at 423 (arguing Doctrine allows government to collect sensitive personal information without constitutional protection).

181. *See* Bedi, *supra* note 127, at 1810 (stating Court established Theory to analyze Fourth Amendment). Bedi comments that the Supreme Court established the Theory to protect against the potential of long-term government surveillance. *See id.*

182. *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (stating reasonable privacy expectation); IDC, *supra* note 2, at 9 (reporting smartphone users near cell phone almost entire day).

183. *See* U.S. CONST. amend. IV (establishing right to privacy from unreasonable searches and seizures); Chemerinsky, *supra* note 9, at 508 (explaining private actors must comply with Constitution if state actors).

184. *See Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, *supra* note 75 (listing carrier data retention timelines). Major cell phone carriers retain subscriber call records for eighteen months up to seven years. *See id.* The carriers retain records of cell towers used by subscribers ranging from four months to over two years. *See id.* The long-term data retention may create a mosaic of a subscriber's life, revealing intimate details that would otherwise remain private, thereby encroaching on Fourth Amendment-protected privacy rights. *See* United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring) (arguing Fourth Amendment search occurs when government monitors individuals locations over time).

185. *See* McLaughlin, *supra* note 57, at 426 (explaining cell phone registration process).

186. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (stating long-term GPS monitoring impinges privacy expectation).

extend the retention period to no longer than 180 days to aid law enforcement activities.[187] Limiting the data retention timeline creates an appropriate balance between government's law enforcement requirements and a subscriber's right to privacy.[188]

IV. CONCLUSION

Cell phone transactional information and location data have transformed the relationship between cell phone providers and the government. These data exponentially increase the government's ability to track individuals subjected to government investigations with precision. Cell phone providers are central to enabling this capability. The government compels cell phone providers to collect and disclose subscriber data to facilitate government investigations and thus transforms cell phone providers into state actors. As state actors, cell phone providers must provide their customers constitutional privacy protections over the use of cell phone data.

No one disputes that individuals use cell phones to share vast amounts of personal information with third parties voluntarily. While individuals choose to share this information, it is the transactional and location data, material unconsciously shared, that may provide the most intimate portrait of a person's identity. This reality implicates a privacy interest protected by the Fourth Amendment. In a modern world of constant connectivity, it is now time for courts to consider a new approach to protecting individual privacy interests in cell phone transactional information and location data.

Sean D.G. Camacho

187. *See* USA FREEDOM Act § 101(F) (authorizing collection for 180 days before requiring additional application and judicial findings). The recommendation to limit the retention of subscriber data to 180 days provides consistency between carrier policies and the USA FREEDOM Act. *See id.* *Compare Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (identifying privacy concern with long-term monitoring), *with Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, *supra* note 75 (listing carrier data retention timelines). Major carriers retain data from months to years. *See Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, *supra* note 75. Reducing data retention to less than one week would comply with concerns over long-term monitoring, while affording the government access to records. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (noting privacy concern with long-term monitoring).

188. *See* USA FREEDOM Act § 101(F) (attempting to respect privacy rights by limiting collection to 180 days). Limiting data retention will not prevent the government from seeking long-term monitoring of individual cell phone subscribers if it is necessary for law enforcement efforts. *See id.*; Donohue, *supra* note 86, at 766-67 (identifying FISC created to oversee order for production of "tangible goods"). *Maynard* acknowledged that tracking an individual's movements over the course of a month violates a reasonable expectation of privacy. *See* United States v. Maynard, 615 F.3d 544, 562-63 (2010). Prolonged retention of cell phone metadata is useful to the government but a threat to individual privacy; thus, limiting data retention time may protect the government's interest in law enforcement and respects an individual's right to privacy. *See* USA FREEDOM Act § 101; *Maynard*, 615 F.3d at 562.