Volume 118 | Issue 2 Article 11

December 2015

The Stored Communications Act: Property Law Enforcement Tool or Instrument of Oppression?

Raymond Boyce
West Virginia University College of Law

THE STORED COMMUNICATIONS ACT: PROPER LAW ENFORCEMENT TOOL OR INSTRUMENT OF OPPRESSION?

I. INTRODUCTION

Alan battles multiple sclerosis,[1] the unpredictable and often debilitating disease that disrupts the flow of information within the brain and body.[2] Bill worries whether his cardiac monitoring device will actually control his heart arrhythmia and keep him alive.[3] Charles considers buying the same kind of assault rifle[4] used to mow down 20 children and 6 adults in a Newtown, Connecticut, elementary school and 12 moviegoers in an Aurora, Colorado, theater.[5] Dylan begins growing marijuana.[6] And Erica, after turning to her sister

---

1 *What is MS?*, NAT'L MULTIPLE SCLEROSIS SOC'Y, http://www.nationalmssociety.org/What-is-MS (last visited Nov. 5, 2015) (defining multiple sclerosis as "an unpredictable, often disabling disease of the central nervous system that disrupts the flow of information within the brain, and between the brain and body").

2 Jonathan Mayer, *MetaPhone: The Sensitivity of Telephone Metadata*, WEB POL'Y (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

3 *Id.*

4 *Id.*

5 Erica Goode, *Popular AR-15 Style Rifle Used in Mass Killings*, SEATTLE TIMES (Dec. 17, 2012, 6:13 AM), http://www.seattletimes.com/nation-world/popular-ar-15-style-rifle-used-in-recent-mass-killings/.

for guidance, has an abortion.[7] How do we know this? We know this based on simple analysis of the non-content information, or "metadata," that these people inadvertently produced while using their cell phones.[8]

Despite not revealing communication content, metadata created by cell phone usage—even "over a short time window"[9]—creates an "unambiguously sensitive"[10] mosaic of the user's personal life.[11] Numbers dialed, the unique serial number of a called phone, and the time and duration of calls are but a few of the metadata records cell phone usage generates.[12] Perhaps the most invasive metadata record generated by cell phone usage is cell site location information ("CSLI").[13] CSLI creates a definitive record of a cell phone user's actual physical movements.[14] A functioning[15] cell phone automatically generates CSLI by relaying its location to its user's service provider every seven seconds,[16] creating a real time record of the cell phone's movements with enough specificity to pinpoint an individual's location on a specific floor of a particular building.[17] Cell phone service providers, in turn, archive CSLI.[18]

---

6 Mayer, *supra* note 2.

7 *Id.*

8 *Id.*

9 *Id.*

10 *Id.*

11 *Id.*

12 Dan Albright, *What Can Government Agencies Tell from Your Phone's Metadata?*, MAKEUSEOF (Feb. 2, 2015), http://www.makeuseof.com/tag/can-government-security-agencies-tell-phones-metadata/#.

13 *See, e.g.*, United States v. Guerrero, 768 F.3d 351, 358 (5th Cir. 2014) (describing CSLI stored by third-party cell phone service providers as "revealing [to government officials] 'the antenna tower and sector to which the cell phone sends its signal'" (quoting *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013))); *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006) (explaining that CSLI "reveal[s] the general location—and, in some circumstances, permit[s] law enforcement agents to track the precise movements—of a particular cellular telephone on a real-time basis").

14 *See Guerrero*, 768 F.3d at 358; *In re Prospective*, 460 F. Supp. 2d at 450.

15 Steven M. Harkins, *CSLI Disclosure: Why Probable Cause Is Necessary to Protect What's Left of the Fourth Amendment*, 68 WASH. & LEE L. REV. 1875, 1881 n.29 (2011) (noting that cell phones must be turned on in order to communicate with the network of the service provider).

16 *Id.* at 1877 (indicating that this process, known as registration, is the once-every-seven-seconds communication between your cell phone and the nearest cell phone tower, which is done to find the tower with the strongest reception).

17 Evan Perez & Siobhan Gorman, *Phones Leave a Telltale Trail*, WALL ST. J. (June 15, 2013, 12:24 PM), http://www.wsj.com/articles/SB10001424127887324049504578545352803220058.

Moreover, in addition to the historical tracking capability enabled by CSLI, today's cell phones can show authorities the "geographic movements of the phone . . . as they occur,"[19] contrary to Hollywood's frequent depiction that police must keep a caller on the line for a specified length of time to successfully trace the phone's location.[20] Realizing the utility of such information in fighting crime, law enforcement has begun using CSLI in criminal prosecutions to circumstantially demonstrate that a particular defendant was in the same general area as a crime when it occurred.[21] It comes as little surprise that in the last five years, four federal circuits—the Third, Fourth, Fifth, and Eleventh—have considered challenges to the constitutionality of the statute the government uses to obtain CSLI,[22] the Stored Communications Act ("SCA").[23]

---

[18] *See, e.g.*, United States v. Davis, 754 F.3d 1205, 1217 (11th Cir.), *vacated*, 573 F. App'x 925 (11th Cir. 2014), *aff'd on reh'g*, 785 F.3d 498 (11th Cir. 2015); *In re Historical*, 724 F.3d at 611.

[19] *See In re Prospective*, 460 F. Supp. 2d at 451. The court provided a comprehensive explanation of this process, commonly known as triangulation:

> [T]he process of determining the coordinates of a point based on the known location of two other points. If the direction (but not distance) from each known point to the unknown point can be determined, then a triangle can be drawn connecting all three points. While only the length of one side of the triangle is known at first (the side connecting the two known points), simple trigonometry reveals the lengths of the other sides and so the position of the third point. In the context of cell site information, the two known points are the antenna towers, the third point is the cellular telephone, and the direction from each tower to the phone is discerned from the information about which face of each tower is facing the phone.
>
> Another method of tracking the location of cellular telephones, which also is sometimes called triangulation, is possible when a phone transmits signals to three antenna towers at once. Based on the strength of a phone's signal to a tower, and the time delay for the signal to reach the tower, one can determine the distance between the phone and the tower. One can then draw around the tower a circle, the radius of which is the distance from that tower to the phone. The location of the phone can be pinpointed by drawing circles around three of more towers and seeing where the circles intersect.

Id. at 451 n.3.

[20] *See, e.g.*, IRON MAN 2 (Paramount Pictures 2010). Billionaire, genius, playboy Tony Stark, fighting crime as Iron Man, receives a phone call from his arch nemesis, Ivan Vanko, at which time Stark immediately utilizes his high-tech in-home computer system to initiate a call trace that is ultimately unable to identify Vanko's location with any more specificity than the general New York City area before Vanko hangs up. *Id.*

[21] *See, e.g.*, United States v. Graham, 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, Nos. 12-4659(L), 12-4825, 2015 WL 6531272 (4th Cir. Oct. 28, 2015); United States v. Davis, 785 F.3d 498 (11th Cir. 2015).

[22] *Graham*, 796 F.3d at 338; *Davis*, 785 F.3d at 500; *In re Historical*, 724 F.3d at 602; *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 305 (3d Cir. 2010).

[23] Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2013).

These four cases—two of which involved the opinions of federal magistrates,[24] and two of which involved the appeal of criminal defendants[25]—raised Fourth Amendment challenges to the collection and admission in court of CSLI obtained from cell phone service providers, pursuant to § 2703(d) of the SCA.[26] Section 2703(d) of the SCA allows the government to obtain a warrant compelling cell phone providers to produce CSLI upon a demonstration of "*specific and articulable facts* showing that there are reasonable grounds to believe that [CSLI records] are relevant and material to an ongoing criminal investigation."[27] In contrast, the Fourth Amendment requires that "no Warrants shall issue, but upon *probable cause*"[28]—a higher standard than what § 2703(d) of the SCA requires.

Because the burden necessary to issue a warrant under § 2703(d) of the SCA is in conflict with the burden necessary to issue a warrant under the Fourth Amendment, this Note argues that § 2703(d) of the SCA is unconstitutional.[29] The reasonable suspicion requirement of § 2703(d) directly conflicts with the plain language of the Fourth Amendment, thereby creating a constitutional loophole the Founders would have never permitted.[30] Further, persons maintain a subjective expectation of privacy in their historical CSLI that society is prepared to recognize as objectively reasonable, notwithstanding the third-party exception.[31] Finally, the privacy interest of cell phone users in their CSLI outweighs law enforcement's typical need to obtain such records.[32]

In making this argument, this Note will first detail the history, evolution, and modern application of Fourth Amendment jurisprudence.[33] Next, Part III provides an overview of the SCA and its utilization by government officials. Then, Part IV analyzes the circuit split created by the decisions of the

---

24 *In re Historical*, 724 F.3d at 602 (concluding that the SCA lessens the government's burden of proof below what is required by the Fourth Amendment); *In re Provider*, 620 F.3d at 308 (concluding that a warrant for CSLI may not be authorized absent a showing of probable cause).

25 *See Graham*, 796 F.3d at 338 (holding that "the government's warrantless procurement of . . . CSLI was an unreasonable search in violation of Appellant's Fourth Amendment rights"); *Davis*, 785 F.3d at 500 (holding that a court order authorized by the SCA compelling the production of a third-party telephone company's CSLI business records does not violate the Fourth Amendment).

26 18 U.S.C. §§ 2701–2712 (2013); *Davis*, 754 F.3d at 1210; *In re Historical*, 724 F.3d at 605–15; *In re Provider*, 620 F.3d at 308–19.

27 18 U.S.C. § 2703(d) (emphasis added).

28 U.S. CONST. amend. IV (emphasis added).

29 *See infra* Part V.

30 *See infra* Part V.C.1.

31 *See infra* Part V.C.2–3.

32 *See infra* Part V.C.4.

33 *See infra* Part II.

Third, Fifth, and Eleventh Circuits, which affirm the constitutionality of reasonable suspicion warrants of § 2703(d) of the SCA, and the vacated panel decision of the Fourth Circuit,[34] which held that such warrants violate the Fourth Amendment. Finally, in Part V, this Note argues that § 2703(d) of the SCA violates the Fourth Amendment because individuals have a legitimate expectation of privacy in their historical CSLI, and thus the government must first obtain a warrant supported by probable cause—the burden necessitated by the Fourth Amendment—to access historical CSLI.

II. THE FOURTH AMENDMENT PAST AND PRESENT

The American colonists endured British general warrants and writs of assistance, which "allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[35] Opposition to the practice was so intense that it played a pivotal role in motivating the Revolution itself.[36] John Adams once noted, after hearing an impassioned 1761 speech opposing the practice, that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance."[37]

Given their loathing of rampant governmental invasiveness, when the Founders codified the "rights of man"[38] to be forever preserved by the Constitution—the "supreme Law of the Land"[39]—they sought to limit the ability of the government to invade individual privacy.[40] Accordingly, since its 1791 ratification, the Fourth Amendment has safeguarded "[t]he right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and ensured that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[41] However, the Fourth Amendment's scope is limited to preclude government inspections of houses, persons, papers, and effects only if such examinations are deemed searches or seizures.[42]

---

34 *See infra* Part IV.D.1.

35 Riley v. California, 134 S. Ct. 2473, 2494 (2014).

36 *Id.*

37 *Id.* (quoting 10 WORKS OF JOHN ADAMS 247–48 (C. Adams ed., 1856)).

38 Adamson v. People of California, 332 U.S. 46, 51 (1947) (noting that "the rights of man . . . are listed in the Bill of Rights").

39 U.S. CONST. art. VI.

40 *See id.* amend. IV.

41 *Id.*

42 THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 4 (2d ed. 2014).

This Part outlines the evolution and modern application of the Supreme Court's Fourth Amendment jurisprudence. First, Section A examines the Supreme Court's definition of "search" under the Fourth Amendment and how it has changed over time. Next, Section B discusses the Supreme Court's definition of "seizure" under the Fourth Amendment. Finally, Section C reviews the reasonableness and warrant requirements of the Fourth Amendment, and the Supreme Court's interpretation of their applicability to law enforcement's use of cutting-edge investigative technology.

A. Searches

Prior to the 1950s,[43] traditional Supreme Court jurisprudence did not recognize the commission of a search unless a government officer committed a "common-law trespass."[44] This strict property-based trespass framework, epitomized in *Olmstead v. United States*,[45] holds that only the government's *physical* intrusion into constitutionally protected tangible objects—i.e., one's home, person, papers, and effects—implicates the Fourth Amendment.[46] The Court has accordingly held that governmental actions such as placing a drug dog on the porch of a suspect's home,[47] extracting an unwilling suspect's blood to determine his level of intoxication,[48] patting down an individual,[49] and attaching a GPS tracker to a vehicle[50] constitute Fourth Amendment searches.

However, by 1967, in the seminal case *Katz v. United States*,[51] the Court announced a significant Fourth Amendment paradigm shift. In *Katz*, the FBI "bugged," or implanted, a listening device in a public telephone booth to

---

43 United States v. Jones, 132 S. Ct. 945, 949 (2012).

44 *Id.*

45 277 U.S. 438, 457 (1928) (noting that because the actual wire taps used to monitor the conversations of and ultimately convict the defendants were placed along exterior telephone lines, "insertions were made without trespass upon *any property* of the defendants," and the Fourth Amendment was not violated (emphasis added)).

46 CLANCY, *supra* note 42, at 361.

47 Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (regarding "the area 'immediately surrounding and associated with the home'—what our cases call the curtilage—as 'part of *the home itself* for Fourth Amendment purposes'" (emphasis added) (quoting Oliver v. United States, 466 U.S. 170, 184 (1984))).

48 Schmerber v. California, 384 U.S. 757, 767–68 (1966).

49 *See, e.g.*, United States v. Robinson, 414 U.S. 218, 223–24 (1973) (pack of cigarettes containing heroin discovered after officer examined suspect's pockets); Sibron v. New York, 392 U.S. 40, 65 (1968) (envelopes of heroin discovered after officer examined suspect's pockets); Terry v. Ohio, 392 U.S. 1, 7 (1968) (gun discovered after exterior probe of suspect's clothing); Beck v. Ohio, 379 U.S. 89, 90 (1964) (envelope containing illegal municipal forms discovered after searching arrestee's socks).

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

51 389 U.S. 347 (1967).

catch a defendant placing illegal bets.[52] The Court held this search to be unconstitutional and, for the first time, the Court declared that the "Fourth Amendment protects people, not places."[53] The Court nevertheless tempered the scope of such a seemingly sweeping precedent by declaring that "[w]hat a person *knowingly* exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection."[54]

Thus, since 1967, the Supreme Court has recognized an alternative to strict physical trespass: any governmental search "violat[ing] a person's '*reasonable expectation of privacy*'"[55] is subject to Fourth Amendment scrutiny.[56] A reasonable expectation of privacy is established in those places, objects, or conversations in which (1) an individual has "exhibited an actual (subjective) expectation of privacy" that (2) "society is prepared to recognize as [objectively] 'reasonable.'"[57] Failure of an individual to satisfy either of the test's two prongs means a governmental intrusion is not a search, removing such intrusion from the scope of Fourth Amendment protection.[58]

In addition to protecting against unreasonable searches, the Fourth Amendment also protects against unreasonable seizures. Accordingly, the following section elaborates on what is considered a seizure for Fourth Amendment purposes.

B. Seizures

The Supreme Court first explicitly defined seizures under the Fourth Amendment[59] in the 1968 landmark case *Terry v. Ohio*.[60] In *Terry*, a police officer stopped, or "seized," and patted down two individuals that he suspected were planning to rob a store.[61] The *Terry* Court announced that "[w]henever a police officer accosts an individual and restrains his freedom to walk away, he has 'seized' that person."[62] Thus, law enforcement officers execute a personal seizure both by physically restraining someone[63] and by showing authority,[64] a

---

52 *Id.* at 348.

53 *Id.* at 351.

54 *Id.* (emphasis added).

55 *Jones*, 132 S. Ct. at 950 (emphasis added).

56 *Katz*, 389 U.S. at 360–62 (Harlan, J., concurring).

57 *Id.* at 361.

58 *Id.* (noting that "the rule that has emerged . . . is that there is a twofold requirement").

59 CLANCY, *supra* note 42, at 5.

60 392 U.S. 1 (1968).

61 *Id.* at 5–7.

62 *Id.* at 16.

63 *Id.* at 19 n.16 (defining a seizure as "[w]hen the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen").

common example of which is brandishing a firearm.[65] Ultimately, "the proper inquiry 'is whether a reasonable person would feel free to decline the officers' requests or otherwise terminate the encounter.'"[66]

The most common examples may involve persons, but the Fourth Amendment is not limited to the seizure of persons. Although it is often a highly fact-specific inquiry,[67] the Fourth Amendment also typically shields real property and other objects in which individuals possess a liberty interest.[68] Property is considered seized by the government "when there is some meaningful interference with an individual's possessory interests in that property";[69] seizure of objects in which individuals possess a liberty interest occurs, for example, upon the warrantless interception of electronic data or sound waves carrying communications.[70]

Building on these concepts, the following section interprets reasonableness as it pertains to Fourth Amendment searches and seizures, and expounds upon the warrant requirement therein.

C. *Reasonableness and the Warrant Requirement*

If an individual's privacy or liberty interests are implicated by a governmental search or seizure, "the ultimate touchstone of [that search or seizure under] the Fourth Amendment is 'reasonableness.'"[71] The Framers selected such an "imprecise and flexible term"[72] because they realized "that searches and seizures were too valuable to law enforcement to prohibit them entirely,"[73] but they knew that unfettered government power might become an instrument of tyranny.[74]

Modern Supreme Court jurisprudence has done little to clarify the definition of Fourth Amendment reasonableness. Not only is Fourth

---

64 *Id.*

65 *See, e.g.*, United States v. Drayton, 536 U.S. 194, 203–04 (2002) (citing Florida v. Bostick, 501 U.S. 429, 432 (1991)).

66 *Id.*

67 *See* Ohio v. Robinette, 519 U.S. 33, 39 (1996).

68 *See* CLANCY, *supra* note 42, at 7–11.

69 United States v. Jacobsen, 466 U.S. 109, 113 (1984). "[M]eaningful interference with an individual's possessory interests" constitutes a seizure of such property. *Id.* at 113 n.5.

70 United States v. Davis, 754 F.3d 1205, 1213 (11th Cir.), *vacated*, 573 F. App'x 925 (11th Cir. 2014), *aff'd on reh'g*, 785 F.3d 498 (11th Cir. 2015).

71 Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

72 Berger v. New York, 388 U.S. 41, 75 (1967) (Black, J., dissenting).

73 *Id.*

74 *See* discussion *infra* Part V.A.

Amendment analysis highly fact-specific,[75] but concretely defining reasonableness is complicated by the Supreme Court's recognition of both the trespass and the *Katz* reasonable expectation of privacy theories as legitimate grounds upon which a search or seizure may be found unreasonable.[76] In addition to the confusion created by the application of multiple tests, the *Katz* test is highly malleable because it is predicated on the subjective beliefs of individuals and whether an ever-evolving society is willing to recognize their beliefs as reasonable. Thus, "no clearly articulated standard exists as to what constitutes an 'unreasonable search' under the Fourth Amendment,"[77] and the potentially "subjective and unpredictable" nature of the Fourth Amendment is simply compounded by the perpetual advancement of technology.[78]

What has remained constant, however, is a general confidence in the validity of a search or seizure authorized by a judicial warrant. The Framers believed that the "formal processes associated with specific warrants, including the judicial assessment of whether there was adequate cause for the intrusion, provided the best means of preventing violations" of liberty.[79] The Supreme Court has similarly maintained that the Fourth Amendment's guarantee of "reasonableness generally requires the [government's] obtaining of a judicial warrant" supported by probable cause prior to its execution of a search or seizure.[80]

According to the Supreme Court, warrants ensure that the inferences necessary to support a search are "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime,"[81] while also providing "fair leeway for enforcing the law in the community's protection."[82] Accordingly, absent "a few

---

75 Ohio v. Robinette, 519 U.S. 33, 39 (1996).

76 *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 952 ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, but not *substituted for*, the common-law trespassory test.").

77 Jeremy Derman, *Constitutional Law: Maryland District Court Finds Government's Acquistion of Historical Cell Site Data Immune from Fourth Amendment:* United States v. Graham, *846 F. Supp. 2d 384 (D. Md. 2012)*, 46 SUFFOLK U. L. REV. 297, 299 (2013).

78 Kyllo v. United States, 533 U.S. 27, 33–34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens . . . [is] unaffected by the advance of technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.").

79 Thomas Y. Davies, *Recovering the Original Fourth Amendment*, *in* THE FOURTH AMENDMENT: SEARCHES AND SEIZURES: ITS CONSTITUTIONAL HISTORY AND THE CONTEMPORARY DEBATE 32, 34 (Cynthia Lee ed., 2011).

80 Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

81 Riley v. California, 134 S. Ct. 2473, 2482 (2014) (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).

82 Maryland v. Pringle, 540 U.S. 366, 370 (2003) (quoting Brinegar v. United States, 338 U.S. 160, 176 (1949)).

specifically established and well-delineated exceptions"[83]—such as searches incident to arrest,[84] hot pursuit of a felony suspect,[85] or some other set of exigent circumstances rendering obtaining a warrant objectively impractical[86]—warrantless searches or seizures by the government are per se unreasonable under the Fourth Amendment.[87]

The following subsection examines another exception to the warrant requirement: the third-party exception doctrine. Among the many warrant requirement exceptions, this exception is most applicable to the questions of the constitutionality of the SCA's § 2703(d).

1. General Third-Party Exception Doctrine

The Fourth Amendment exception perhaps most applicable to the question of the protection of CSLI is the third-party exception doctrine, established in *United States v. Miller*.[88] The third-party exception allows government officials to obtain information initially revealed to a third-party "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in a third-party will not be betrayed."[89]

In *Miller*, federal law enforcement officials in the Treasury Department's Alcohol, Tobacco, and Firearms Bureau ("ATFB") suspected Miller of participating in the operation of an illegal whiskey distillery.[90] In its investigation, the ATFB obtained copies of Miller's checks and other bank records,[91] pursuant to subpoenas issued by a United States Attorney rather than a judge.[92] The records were ultimately admitted at Miller's trial and used

---

83 Katz v. United States, 389 U.S. 347, 357 (1967).

84 Chimel v. California, 395 U.S. 752, 762–63 (1969) (holding that officers are able to search an arrestee both to detect weapons that may be used to harm the officer or effect the arrestees escape, as well as to detect any evidence on the arrestee's person in order prevent its concealment or destruction).

85 *See* Warden v. Hayden, 387 U.S. 294, 298 (1967) (citing McDonald v. United States, 33 U.S. 451, 456 (1948)).

86 *See* Mincey v. Arizona, 437 U.S. 385, 394 (1978).

87 *Katz*, 389 U.S. at 357.

88 425 U.S. 435, 438–47 (1976).

89 *Id.* at 443.

90 *Id.* at 437.

91 *Id.* at 437–38.

92 *Id.* at 438–39.

against him as proof of his participation in the distillery.[93] Miller appealed their admission.[94]

The Court held that Miller maintained no reasonable expectation of privacy in his subpoenaed bank records because they were not his "private papers," and he could not assert ownership or possession of them.[95] Rather, they were the third-party bank's business records.[96] The obtained documents contained information "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," further supporting the Court's conclusion that Miller's financial records were the unprotected business records of his bank.[97] The Court accordingly cautioned that an individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government."[98]

Thus, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[99] The government implicates "no Fourth Amendment interests of the depositor" by coercing the bank to produce its records, "even if a criminal prosecution is contemplated at the time" the records are acquired.[100]

Whereas the third-party doctrine has typically been applied with ease to tangible objects, such as bank records, its application to modern technology—and the intangible—is not that easy. The following subsection discusses Supreme Court cases that address the inherent conflict between the individual privacy rights outlined in the Fourth Amendment and law enforcement's use of increasingly sophisticated technology.

2. Technology, the Reasonable Expectation of Privacy, and the Third-Party Doctrine

The Supreme Court's Fourth Amendment jurisprudence is frequently difficult to reconcile with modern technological processes employed by law enforcement. Consequently, courts have relied on such disparate cases as *Smith v. Maryland*,[101] *Kyllo v. United States*,[102] *United States v. Jones*,[103] *Riley v.*

---

93 *Id.* at 438.

94 *Id.* at 437.

95 *Id.* at 440.

96 *Id.*

97 *Id.* at 442.

98 *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)).

99 Katz v. United States, 389 U.S. 347, 351 (1967) (citations omitted).

100 *Miller*, 425 U.S. at 444.

101 442 U.S. 735 (1979).

California,[104] *United States v. Knotts*,[105] and *United States v. Karo*[106] to determine the Fourth Amendment's application to CSLI and other technologies. The *Smith*, *Knotts*, and *Karo* opinions rule against individual privacy;[107] whereas, *Kyllo*, *Jones*, and *Riley* invalidate various governmental actions on Fourth Amendment grounds.[108] The following subsections will provide a brief synopsis of each case.

i. Smith v. Maryland*: Warrantless Use of a Pen Register to Obtain Dialed Numbers Is Not an Unreasonable Search*

In *Smith*, the Court held that telephone users "can claim no legitimate [subjective] expectation of privacy" in the numbers they dial.[109] While investigating Smith for robbery, police requested that a telephone company install a pen register[110] to record the numbers dialed from his home telephone.[111] The pen register was authorized by neither warrant nor court order.[112] It ultimately confirmed that Smith was the robber,[113] and he was subsequently convicted of the crime.[114]

The Court stated that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through

---

102 533 U.S. 27 (2001).

103 132 S. Ct. 945 (2012).

104 134 S. Ct. 2473 (2014).

105 460 U.S. 276 (1983).

106 468 U.S. 705 (1984).

107 *See Karo*, 468 U.S. at 718; *Knotts*, 460 U.S. at 285; Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

108 *See Riley*, 134 S. Ct. at 2495; *Jones*, 132 S. Ct. at 948–49; Kyllo v. United States, 533 U.S. 27, 40–41 (2001).

109 *Smith*, 442 U.S. at 744 (noting that when the defendant used his phone, he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business").

110 *Id.* at 736 n.1. *Smith* defines a pen register as

> "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." A pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached.

Id. (alteration in original) (citations omitted).

111 *Id.* at 737.

112 *Id.*

113 *Id.*

114 *Id.* at 738.

telephone company switching equipment that their calls are completed."[115] Accordingly, the warrantless use of a pen register at the behest of the police did not violate the Fourth Amendment because people were likely to not "entertain any actual expectation of privacy in the numbers they dial."[116]

ii. United States v. Knotts *and* United States v. Karo*: Items Are Not Searched When Viewed with the Naked Eye from a Lawful Vantage Point*

Knotts and *Karo* involved the constitutionality of homing devices placed in personal property by law enforcement to track the property's location.[117] In *Knotts*, with the consent of a chloroform manufacturer, the police placed a tracking device in a drum of chloroform to be sold to persons suspected of using it to produce methamphetamine.[118] When visual surveillance failed, the police used the tracker to follow the drum to a cabin in the woods, which they lawfully observed for three days in order to obtain a search warrant.[119] A subsequent search uncovered the cabin's methamphetamine lab.[120] The Court upheld the device's use because, despite enhancing the senses of law enforcement by maintaining a virtual visual of the drum even when the physical tail was lost, it merely revealed what *could* have been seen with the naked eye: the driver's movements on a public highway.[121]

The next year, in *Karo*, as in *Knotts*, the Court dealt with the constitutionality of the use of a tracking device by law enforcement;[122] however, the Court in *Karo* reached the opposite decision.[123] In *Karo*, with the consent of a chemical dealer, law enforcement placed a tracking beeper in a drum of ether.[124] Police suspected the ether had been ordered to produce illegal drugs.[125] Relying on the tracking device, police followed the drum to a private home.[126] In the ensuing days, police used the device to track the drum between

---

115 *Id.* at 742.

116 *Id.*

117 *See* United States v. Karo, 468 U.S. 705, 707 (1984); United States v. Knotts, 460 U.S. 276, 277 (1983).

118 *Knotts*, 460 U.S. at 277–78.

119 *Id.* at 278–79.

120 *Id.* at 279.

121 *Id.* at 285.

122 *Karo*, 468 U.S. at 714.

123 *Id.* at 705.

124 *Id.* at 708.

125 *Id.*

126 *Id.*

three private homes and a commercial storage facility.[127] The Court held that monitoring a tracking device within a private residence, which grants police insight into an area not open to visual surveillance, violates the Fourth Amendment rights of those with a reasonable expectation of privacy in the home.[128]

iii. Kyllo v. United States*: Use of a Thermal Imaging Device to See Within a Home Constitutes a Search*

In *Kyllo*,[129] law enforcement officials suspected Kyllo of growing marijuana in his home but lacked sufficient probable cause to obtain a warrant to search the premises.[130] Nonetheless, police were aware that indoor marijuana production typically requires many high-intensity lamps that generate a significant amount of heat.[131] Accordingly, police scanned Kyllo's home with a thermal imaging device, revealing such a signature.[132] Based on the thermal imaging and other corroborating information, the agents obtained a warrant to search the home and uncovered a marijuana growing operation containing over 100 marijuana plants.[133]

The Court held that the use of a thermal imager to gain information undetectable with natural senses constituted a search, particularly when such technology is "not in general public use."[134] Criticized by the dissent as creating a malleable rule that is "unnecessary, unwise, and inconsistent with the Fourth Amendment,"[135] *Kyllo* requires continual reevaluation of advances in technology[136] to determine whether the new technology is sufficiently in the public use so as to erode the Fourth Amendment's protections.[137]

---

127 *Id.*

128 *Id.* at 716, 718.

129 Kyllo v. United States, 533 U.S. 27 (2001).

130 *See id.* at 29.

131 *See id.*

132 *Id.*

133 *Id.*

134 *Id.* at 34 (holding that "obtaining by sense-enhancing technology any information . . . that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use" (citation omitted)).

135 *Id.* at 41 (Stevens, J., dissenting).

136 *See, e.g.*, *FLIR One*, FLIR, http://www.flir.com/flirone/ (last visited Nov. 5, 2015). The advanced investigative technology at issue in *Kyllo* can now be utilized on cell phones.

137 Harkins, *supra* note 15, at 1892.

iv. United States v. Jones*: Warrantless Application of a GPS Tracking Device to Property Constitutes an Unreasonable Search*

Over a decade after *Kyllo*, the Court decided *Jones*,[138] which pertained to the constitutionality of the warrantless application of a tracking device to the vehicle of a man suspected of trafficking illegal drugs.[139] Reviving the traditional Fourth Amendment trespass theory but not thereby disposing of the reasonable expectation of privacy theory,[140] the Court held that warrantless use of a GPS tracker on Jones's personal property was a common law trespass that invalidated any evidence cultivated from it.[141] Justices Sotomayor[142] and Alito[143] filed separate concurrences in *Jones*, applying the reasonable expectation of privacy standard, with three other Justices joining Alito's opinion.[144]

Justice Sotomayor held that GPS tracking of Jones's whereabouts over time was an unreasonable search.[145] She argued that it might be necessary to reconsider the fundamental premise of the third-party doctrine, particularly as manifested in a digital context, because it "is ill suited for the digital age."[146] Similarly, Justice Alito held that it was the length of time Jones was monitored that established a search under the Fourth Amendment.[147] Taken together, the Sotomayor and Alito concurrences create what has been called the "mosaic" theory of Fourth Amendment interpretation,[148] which allows courts to assess

---

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

139 *Id.* at 948. Police possessed a properly obtained warrant, however, the warrant authorized the GPS tracker to be applied within ten days and within the District Columbia, and it was applied on the 11th day in Maryland. *Id.* Twenty-eight days of data were compiled and used against Jones at trial to obtain his conviction for conspiracy to traffic illegal substances. *Id.*

140 *Id.* at 952. "[T]he *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for*, the common-law trespassory test." *Id.*

141 *Id.* at 949.

142 *Id.* at 955. "I agree with Justice ALITO that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Id.* (Sotomayor, J., concurring) (quoting *id.* at 964 (Alito, J., concurring)).

143 *Id.* at 958. "I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id.* (Alito, J., concurring in the result).

144 *Id.* at 957. Justices Ginsburg, Breyer, and Kagan joined Justice Alito's concurrence.

145 *Id.* at 954–56 (Sotomayor, J., concurring).

146 *Id.* at 957.

147 *Id.* at 964 (Alito, J., concurring).

148 *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012). Kerr offers the following definition:

> Under the mosaic theory, searches can be analyzed as a collective sequence of steps rather than as individual steps. Identifying Fourth Amendment

the constitutionality of government searches and seizures by viewing them collectively rather than by viewing them sequentially in isolated steps.[149]

v. Riley v. California: *Warrantless Searches of a Cell Phone Incident to Arrest Are Impermissible Under the Fourth Amendment*

Finally, in 2014, the Court decided *Riley*,[150] a consolidation of two similar cases,[151] holding that police may not search an arrestee's cell phone without a warrant.[152] In *Riley*, police searched the contents of the defendant's cell phone upon its discovery during a lawful arrest, extracted evidence from it, and later used that evidence against him at trial to obtain a conviction.[153] The Court found that law enforcement's need to obtain the contents of an arrestee's cell phone satisfied none of the exceptions to the Fourth Amendment.[154] Accordingly, the Court held that the Fourth Amendment requires law enforcement to obtain a warrant before examining the contents of an arrestee's cell phone.[155]

The Court additionally stated that the data stored on a cell phone is unique from tangible objects both quantitatively and qualitatively.[156] Not only did the Court recognize that cell phones can contain vast amounts of information utterly impossible to be carried physically,[157] but also that they can

---

> 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.

Id. (citations omitted).

149 *Id.* at 320.

150 Riley v. California, 134 S. Ct. 2473 (2014).

151 *Id.* at 2480.

152 *Id.* at 2495.

153 *Id.* at 2480–82.

154 *Id.* at 2485. The Court held that the contents of an arrestee's cell phone pose no risk to officer safety. *Id.* Officer safety motivated the search incident to arrest exception to the Fourth Amendment. *See* Chimel v. California, 395 U.S. 752, 763 (1967). The Court also held that the contents of an arrestee's cell phone are not so susceptible to destruction as to render obtaining a warrant before examining them objectively unreasonable. *Riley*, 134 S. Ct. at 2486–88. Preventing imminent destruction of evidence motivated the exigent circumstances exception to the Fourth Amendment. *Id.* at 2494.

155 *Riley*, 134 S. Ct. at 2495 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is . . . simple—get a warrant.").

156 *Id.* at 2489.

157 *Id.* The Court distinguished the information storage capacity of a cell phone from that of traditional tangible objects typically used to carry information on one's person:

> One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only

reconstruct years of an individual's private life.[158] Finally, the Court noted that cell phones are unique in that they can uncover one's specific movements down to the minute, not only around town but also within a particular building.[159] Confronted with the facts in *Riley*, the Court was forced to educate itself on the nuances of cell phone technology and—for the first time—make a substantive ruling based on these nuances.[160]

The next Part discusses the SCA, the federal statute currently being utilized by law enforcement to obtain historical CSLI. The discussion includes a brief overview of both how the SCA came to be, and its subsections authorizing law enforcement's acquisition of CSLI.

III. THE SCA AND ITS REASONABLE SUSPICION WARRANTS

Law enforcement currently uses the SCA to obtain CSLI from cell phone service providers as circumstantial evidence demonstrating that a criminal defendant was in a particular location at the same time a crime was committed.[161] This Part provides a brief history of that statute, as well as an examination of its subsections authorizing the practice.

Signaling the Legislature's recognition that cell phone technology is a rapidly changing and important component of modern society, Congress passed

---

> a narrow intrusion on privacy. . . . Most 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. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in *Chadwick* . . . rather than a container the size of the cigarette package in *Robinson*.

Id. (citations omitted).

158 *Id.* The Court demonstrated how the data contained on a cell phone is qualitatively different than vessels traditionally carried on one's person for storage purposes such as wallets:

> The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Id.

159 *Id.* at 2490.

160 *See* R. Craig Curtis, Michael C. Gizzi & Michael J. Kittleson, *Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment*, 4 U. DENV. CRIM. L. REV. 61, 75 (2014).

161 *See, e.g.*, United States v. Davis, 754 F.3d 1205, 1213 (11th Cir.), *vacated*, 573 F. App'x 925 (11th Cir. 2014), *aff'd on reh'g*, 785 F.3d 498 (11th Cir. 2015).

the Electronic Communications Privacy Act ("ECPA") in 1986.[162] The intent of the ECPA was to update and clarify federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.[163] Within the larger statutory scheme of the ECPA was the SCA. Eight years later, in 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA") in part to amend and update the SCA.[164]

The SCA "create[d] a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and [cell phone as well as Internet] service providers in possession of users' private information."[165] These purported safeguards are achieved in two ways. First, the SCA restricts the government's ability to compel disclosure by service providers of customer data in its possession by establishing specific procedures that the government must follow to obtain CSLI data.[166] Second, the SCA generally limits the ability of service providers to voluntarily release such information—although numerous exceptions exist.[167]

One such protection takes shape in § 2703(c)(1)(A), which requires the government to obtain a warrant supported by probable cause[168] in order to compel service provider production of records in "temporary 'electronic storage' for 180 days or less."[169] Another, more lenient, SCA provision protecting records "in electronic storage for greater than 180 days"[170] is found

---

162 *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

163 S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

164 *In re* Application of U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 306 (3d Cir. 2010). "In 1994, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103–414, 108 Stat. 4279, 4292 (1994) (codified in relevant part at 18 U.S.C. § 2703 (2010)), in part to amend the SCA." *Id.*

165 Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1212 (2004).

166 *See id.* (citing Stored Communications Act, 18 U.S.C. § 2703 (2000 & Supp. I 2001)).

167 *Id.* at 1213 (citing 18 U.S.C. § 2702 (2013)). Customer records, such as CSLI, may be divulged by a service provider storing such records in the following situations: (1) when a warrant is obtained pursuant to § 2703(d) of the SCA, (2) with the customer or subscriber's consent, (3) when necessary to render service or to protect the provider's rights or property, (4) to a government entity based upon good faith belief of an emergency in which someone is in danger of death or serious physical harm requiring the information, (5) to the National Center for Missing and Exploited Children, and (6) to any person other than a government entity. *Id.* at 1221.

168 18 U.S.C. § 2703(c)(1)(A) (2013) (requiring the police to obtain a warrant by utilizing the procedure laid out in the Federal Rules of Criminal Procedure).

169 *See* Kerr, *supra* note 165, at 1218–19.

170 *Id.* at 1219.

in § 2703(d).[171] Section 2703(d) requires the government to obtain a court order outlining "specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation."[172] This more relaxed standard is essentially a reasonable suspicion standard.[173]

Reasonable suspicion[174] permits a "brief, investigatory stop, when the officer has a reasonable, articulable suspicion that criminal activity is afoot"[175] based upon the totality of the circumstances.[176] An officer must possess "a minimal level of objective justification"[177] amounting to more than inchoate, unparticularized hunches of criminal activity[178] in order to briefly detain or seize an individual or his constitutionally protected property. Although not "readily, or even usefully, reduced to a neat set of legal rules,"[179] properly placed on a proof continuum, "'reasonable suspicion' is a less demanding standard than probable cause and requires a showing considerably less than preponderance of the evidence."[180]

Thus, under the SCA, the government has at its disposal numerous mechanisms by which it may compel cell phone service providers to turn over CSLI, only one of which complies on its face with the Fourth Amendment's requirement that no warrant shall issue absent a governmental presentation and judicial finding of probable cause.[181] Therefore, the central inquiry regarding the government's acquisition of CSLI must be whether the Fourth Amendment "covers not only content [of electronic communications], but also the transmission itself when it reveals information about the personal source of the transmission, specifically his location."[182] Debate over the proper adjudication

---

171 *See* 18 U.S.C. § 2703(d).

172 *Id.*

173 *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 287 (4th Cir. 2013).

174 *See supra* Part II.B.

175 Illinois v. Wardlow, 528 U.S. 119, 123 (2000).

176 *See* Terry v. Ohio, 392 U.S. 1, 21–22 (1968).

177 *Wardlow*, 528 U.S. at 123 (citing United States v. Sokolow, 490 U.S. 1, 7 (1989)).

178 *Id.* at 124 (citing *Terry*, 392 U.S. at 27).

179 *Sokolow*, 490 U.S. at 7 (quoting Illinois v. Gates, 462 U.S. 213, 232 (1983)).

180 *Wardlow*, 528 U.S. at 123.

181 U.S. CONST. amend. IV.

182 United States v. Davis, 754 F.3d 1205, 1213 (11th Cir.), *vacated*, 573 F. App'x 925 (11th Cir. 2014), *aff'd on reh'g*, 785 F.3d 498 (11th Cir. 2015).

of this issue has been a recent focus of the federal judiciary, and the following Part outlines the principal cases in this discussion.[183]

IV. THE SPLIT: *PROVIDER*, *HISTORICAL*, *DAVIS*, AND *GRAHAM*

The U.S. Supreme Court has never addressed the constitutionality of § 2703(d) of the SCA.[184] Similarly, the federal appellate judiciary has developed minimal Fourth Amendment jurisprudence governing challenges to governmental obtainment of CSLI pursuant to the Act.[185] Furthermore, the plain language of the SCA, requiring reasonable suspicion for CSLI warrants, conflicts with the plain language of the Fourth Amendment, requiring probable cause for warrants to lawfully issue.[186] Consequently, no mandatory judicial paradigm exists that courts must consistently and coherently apply to SCA-based CSLI challenges.[187] As a result, the federal circuits are split on whether the reasonable suspicion threshold of § 2703(d) of the SCA satisfies the Fourth Amendment.[188] This Part discusses the split between the Third, Fifth, and Eleventh Circuits, which affirm § 2703(d)'s constitutionality, and the Fourth Circuit, which rejects § 2703(d)'s constitutionality.

A. The Third Circuit: Provider

In its 2010 decision, *In re Application of United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*,[189] the Third Circuit became the first court of appeals to address the constitutionality of the SCA's "specific and articulable facts"

---

183 There is also discord among the states on this exact issue. *See, e.g.*, Eric Lode, Annotation, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessor of Phone Under State Law*, 94 A.L.R. 6th 579 (2014).

184 *Davis*, 754 F.3d at 1211.

185 Curtis, Gizzi & Kittleson, *supra* note 160, at 80. Collecting cases, the article asserts that through 2013, eight federal appellate cases have addressed challenges to the constitutionality of CSLI. *Id.* An analysis of these cases, however, reveals that four cases do not challenge access of CSLI by the government pursuant to the SCA, one case was unreported, two are *Historical* and *Provider*, and one relied solely on *Provider* for guidance from the federal courts of appeals. *Id.*

186 U.S. CONST. amend. IV.

187 *See* Curtis, Gizzi & Kittleson, *supra* note 160, at 61. It should be noted, however, that the judges from the three circuits that have squarely dealt with the issue of the SCA's constitutionality have predominately employed the third-party exception to the Fourth Amendment warrant requirement as articulated in *Miller* and *Smith*. *Id.*

188 *See Davis*, 754 F.3d at 1205; *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

189 620 F.3d 304.

standard.[190] In *Provider*, federal law enforcement officials requested a § 2703(d) warrant to obtain the CSLI of a suspected drug dealer.[191] The federal magistrate judge denied the application chiefly on the ground that the SCA violated the probable cause requirement for warrants under the Federal Rules of Criminal Procedure.[192] The district court affirmed the magistrate judge's order, and the case was appealed to the Third Circuit.[193]

Focusing less on the requirements of the Fourth Amendment and more on the language of the SCA itself,[194] the *Provider* decision reversed the district court.[195] Largely ignoring the Fourth Amendment's probable cause requirement, the court concentrated both on the SCA's plain language requirement of reasonable suspicion and the absence of legislative history indicating a preference that the "Government . . . show probable cause as a predicate for a court order under § 2703(d)."[196] Accordingly, the court held that CSLI "is obtainable under a § 2703(d) order" not requiring "the traditional probable cause determination. Instead, the standard is governed by the text of § 2703(d) . . . [a] standard [that] is a lesser one than probable cause, a conclusion that . . . is supported by the legislative history."[197] Thus, the Third Circuit generally sidestepped a detailed, critical analysis of the Fourth Amendment altogether[198] and ultimately endorsed the SCA.

B. The Fifth Circuit: Historical

In 2013, *In re Application of the United States for Historical Cell Site Data*[199] arose from federal § 2703(d) applications for CSLI relevant to three separate criminal investigations.[200] In *Historical*, the federal magistrate judge rejected the applications after determining that "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment."[201] The district court issued an order affirming the magistrate judge's determination and concluding that CSLI "may be acquired only by a warrant issued on probable

---

190 *Id.* at 305–07.

191 *Id.* at 307–08.

192 *Id.* at 308.

193 *Id.* at 305.

194 *See* Curtis, Gizzi & Kittleson, *supra* note 160, at 69.

195 *In re Provider*, 620 F.3d at 313.

196 *Id.* at 315.

197 *Id.* at 313.

198 *See* Curtis, Gizzi & Kittleson, *supra* note 160, at 69.

199 724 F.3d 600 (5th Cir. 2014).

200 *Id.* at 602.

201 *Id.* (quoting *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010)).

cause" and, accordingly, that the "standard under the Stored Communications Act is below that required by the Constitution."[202] The government appealed the district court order to the Fifth Circuit.[203]

In overturning the district court, the Fifth Circuit rejected the ACLU's contention that the SCA's constitutionality is properly reviewed under the Supreme Court's tracking devices precedent. Rather, the Fifth Circuit adopted the government's position that the Supreme Court's business records precedent controls[204] and proceeded with such analysis.[205]

In *Historical*, the Fifth Circuit recited the basic premise of the third-party exception to the Fourth Amendment: the information an individual voluntarily conveys to others enjoys no reasonable expectation of privacy, whether digital or tangible.[206] Accordingly, the Fifth Circuit held that the Fourth Amendment does not protect a cell phone user's CSLI because he "understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call."[207] The *Historical* court further held that cell phone users enjoy no expectation of privacy in CSLI because cell service contracts "expressly state that a provider uses a subscriber's location information to route his cell phone calls"[208] and "that the providers not only use the information, but collect it."[209]

The court then turned to the next step in the Supreme Court's third-party exception jurisprudence—whether such disclosure is voluntary.[210] The Fifth Circuit observed that "[t]he Government does not require a member of the public to own or carry a phone."[211] Further, the *Historical* decision observed that because telephone monopolies are a past phenomenon, "the Government does not require [a cell phone user] to obtain his cell phone service from a particular service provider that keeps historical cell cite records for its

---

202 *Id.* at 603.

203 *Id.*

204 *Id.* at 615. "Using the proper framework, the SCA's authorization of § 2703(d) orders for historical cell site information if an application meets the lesser 'specific and articulable facts' standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional." *Id.*

205 *Id.*

206 *Id.* at 613 (citing United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012)). "There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone." *Id.*

207 *Id.* (citing United States v. Madison, No. 11–60285–CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012)).

208 *Id.*

209 *Id.*

210 *Id.* at 612–14.

211 *Id.* at 613.

subscribers, either."[212] Nor does the government "require him to make a call, let alone to make a call at a specific location."[213]

Finally, the court acknowledged that although many citizens "may reasonably want their location information to remain private," it ultimately rejected the temptation to unilaterally extend the protections of the Fourth Amendment to historical CSLI.[214] Instead, the court deferred to Congress to remediate the law by enacting appropriate legislation.[215] The Fifth Circuit noted that during periods of "dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[216] The *Historical* court therefore concluded that the "Fourth Amendment . . . protects only reasonable expectations of privacy," and that the proper avenue of recourse for those desiring reform of the SCA "is in the market or the political process."[217] Thus, in upholding the validity of § 2703(d) of the SCA, the Fifth Circuit approved the practice of law enforcement obtaining warrants for historical CSLI upon a showing of reasonable suspicion, even though the Fourth Amendment requires a higher standard—probable cause.

C. The Eleventh Circuit: Davis

In 2014, in *United States v. Davis*, the Eleventh Circuit created a split by diverging from the decisions of the Third Circuit in *Provider* and the Fifth Circuit in *Historical*.[218] *Davis* arose when a criminal defendant appealed his conviction because it was secured, in part, by the government's use at trial of CSLI that it obtained pursuant to the SCA.[219] On appeal, Davis principally alleged that the district court's admission of his CSLI pursuant to the SCA violated his Fourth Amendment rights.[220] The Eleventh Circuit panel agreed, holding that § 2703(d)'s reasonable suspicion warrants violate the Fourth Amendment.[221] Applying the "good faith"[222] exception to the Fourth

---

212 *Id.*

213 *Id.*

214 *Id.* at 615.

215 *Id.* at 614–15.

216 *Id.* at 614 (quoting United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring)).

217 *Id.* at 615.

218 United States v. Davis, 754 F.3d 1205, 1213 (11th Cir.), *vacated*, 573 F. App'x 925 (11th Cir. 2014), *aff'd on reh'g*, 785 F.3d 498 (11th Cir. 2015).

219 *Id.* at 1210–11.

220 *Id.* at 1210.

221 *Id.* at 1217.

Amendment, however, the *Davis* court nevertheless upheld Davis's conviction.[223]

1. The Majority Opinion

Following the Eleventh Circuit's *Davis* panel decision, both the government and Davis filed motions for rehearing en banc.[224] The government's motion was granted and the panel's ruling was thereby vacated.[225] Then, in May 2015, the Eleventh Circuit ruled nine to two that the government's warrantless acquisition of historical CSLI pursuant to the SCA is constitutional.[226] Thus, the federal circuit split created by the *Davis* panel decision was erased by the Eleventh Circuit's en banc *Davis* decision.

In affirming the constitutionality of the SCA, the Eleventh Circuit remarked that although the evidentiary standard of the SCA falls below the probable cause mandate of the Fourth Amendment, the SCA nevertheless contains privacy safeguards[227] more strenuous than those required of the government to issue subpoenas compelling third-party production of other business records.[228] Davis nevertheless contended that the court order compelling production of his historic CSLI records violated his Fourth Amendment rights, as the order was supported by reasonable suspicion rather

---

222 *Id.* The "good faith" exception to the typical exclusionary rule of the Fourth Amendment, established in *United States v. Leon*, dictates that evidence of a government search or seizure should not be suppressed unless the officer knew, or should have known, that the search or seizure was unconstitutional under the Fourth Amendment. 468 U.S. 897 (1984). The *Davis* court concluded that "[a]t that time, there was no governing authority affecting the constitutionality of this application of the [SCA]. There is not even [an] allegation that any actor in the process evidenced anything other than good faith." *Davis*, 754 F.3d at 1218.

223 *Davis*, 754 F.3d at 1218.

224 United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015).

225 *Id.*

226 *See id.* at 500.

227 *Id.* at 505–06 (noting that (1) the SCA demands that specific and articulable facts demonstrating that there are reasonable grounds to believe the requested information is relevant to an ongoing criminal investigation; (2) the SCA exceeds the constitutional requirements for compulsory subpoenas; (3) judicial review by a magistrate is a pre-condition to § 2703(d) order issuance; (4) the SCA prohibits cell phone service providers from voluntarily providing CSLI to government entities; and (5) the SCA provides remedies and penalties—including monetary penalties and disciplinary proceedings against the offending federal officers—for violations of the anti-disclosure privacy provisions).

228 *Id.* at 506 (noting that subpoenas are routinely used to compel production of such business records as credit card statements, bank statements, hotel bills, purchase orders, and billing invoices).

than probable cause.[229] Accordingly, the Eleventh Circuit began *Davis* with a review of applicable Fourth Amendment precedent.[230]

Summarizing the jurisprudence set forth in *Katz*, *Smith*, *Miller*, and *Historical*, the Eleventh Circuit turned to the particular facts of Davis's case.[231] First, the court concluded that they were not his to withhold.[232] Rather, Davis's CSLI records neither contained the contents of Davis's private communications, nor were they owned or possessed by Davis.[233] Thus, because Davis's cell phone service provider maintained his CSLI records in the ordinary course of business for legitimate business purposes, the Eleventh Circuit concluded that Davis's CSLI records were the business records and property of his service provider.[234]

The *Davis* court also determined that, assuming Davis had ownership or possessory rights in his historical CSLI, he had neither a subjective nor objective expectation of privacy in such records, likening Davis to the bank customer in *Miller* and the phone customer in *Smith*.[235] Specifically, Davis was found to have no subjective expectation of privacy because, as a cell phone user, he knew that (1) he must transmit signals to nearby cell towers, (2) making or receiving calls necessarily conveys his general location to his cell phone provider, and (3) cell phone companies record such usage.[236] Likewise, the Eleventh Circuit determined that whatever subjective expectation of privacy Davis might have had, it was objectively unreasonable because, under *Smith*, cell phone users are presumed to know of "uncontroverted and publicly available facts about technologies and practices" applied by phone companies.[237] The Eleventh Circuit was also unpersuaded that advances in technology enabling the determination of a cell phone's location alter the Fourth Amendment calculus established in *Smith*.[238] Rather, the Eleventh Circuit noted that the landlines at issue in *Smith* were arguably even more revealing than modern, imprecise CSLI because landlines correspond to fixed

---

229 *Id.*

230 *Id.* at 506–11.

231 *Id.* at 507–11.

232 *Id.* at 511 (deciding that "*non-content evidence*, lawfully created by a third-party telephone company for legitimate business purposes does not belong to Davis, even if it concerns him").

233 *Id.*

234 *Id.*

235 *Id.*

236 *Id.* at 510 (citing *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 613–14 (5th Cir. 2013)). "Users are aware that cell phones do not work when they are outside the range of the provider company's cell tower network." *Id.*

237 *Id.* at 511 (citing Smith v. Maryland, 442 U.S. 735, 742–43 (1979)).

238 *Id.*

physical addresses.[239] The Eleventh Circuit therefore reasoned that there is no reason to deviate from "the longstanding third-party doctrine [set forth in *Smith*, which] plainly controls the disposition of this case."[240]

The Eleventh Circuit then directly addressed Davis's principal argument that *United States v. Jones*, not *Smith* and *Miller*, controlled the adjudication of his appeal.[241] The argument gained little traction, however, as the court declared that *Jones* turned on the government physically trespassing by placing a GPS tracker on a private citizen's vehicle and, therefore, was "wholly inapplicable" to the CSLI at issue in Davis's case.[242] Additionally, the *Davis* court found that historical CSLI is distinguishable from the "precise, real-time GPS tracking in *Jones*" because CSLI "does not identify the cell phone user's location with pinpoint precision" and, therefore, "does not paint the 'intimate portrait of personal, social, religious, medical, and other activities and interactions' that Davis claims."[243]

The Eleventh Circuit also dismissed Davis's "intimate picture" argument by noting that reasonable expectations of privacy do not turn on the quantity of non-content information.[244] The court reasoned that if Davis had no expectation of privacy in his CSLI records, then a Fourth Amendment violation could not occur when the government acquired them, regardless of the duration of the CSLI records or whether those records created a mosaic of his activities.[245] Thus, the Eleventh Circuit concluded that the "judicial system does not engage in monitoring or a search when it compels the production of preexisting documents from a witness."[246]

Finally, the *Davis* court noted that the touchstone of Fourth Amendment analysis is reasonableness and, therefore, examined, *arguendo*, the reasonableness of the government's acquisition of Davis's CSLI.[247] The Eleventh Circuit began its reasonableness inquiry by observing that the

---

239 *Id.* at 511–12.

240 *Id.* at 512.

241 *Id.* at 513.

242 *See id.* at 514 (stating that in Davis's case, the government obtained records from the cell phone service provider without any physical intrusion on private property, and that such records belonged to a private company, were obtained through a court order authorized by federal statute, could be collected as the result of private action—the construction of the service provider's cell towers—and were collected for legitimate business purposes).

243 *Id.* at 515. The court conceded, however, that close analysis of Davis's CSLI for the 67-day period the government obtained could reveal patterns with regard to his physical location. *Id.* However, the Eleventh Circuit still found that 67 days of CSLI does not yield "anything close to the 'intimate portrait' of Davis's life that he now argues." *Id.* at 516.

244 *Id.* at 515.

245 *Id.*

246 *Id.* at 516.

247 *Id.* at 516–18.

Supreme Court applies a strong presumption of constitutionality to an act of Congress, especially when the act turns on what is reasonable within the meaning of the Fourth Amendment.[248] The Eleventh Circuit acknowledged, however, that despite the favorable presumption congressional legislation enjoys, reasonableness of a search or seizure is ultimately based "on the one hand, [by] the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[249]

In balancing such competing interests, the Eleventh Circuit first addressed and rejected any claim that Davis possessed a privacy interest in his CSLI.[250] The court reiterated that Davis had no reasonable expectation of privacy in his CSLI records, as they were his service provider's business records.[251] The Eleventh Circuit next reasoned that to whatever extent Davis did have a privacy expectation in his CSLI, it was negligibly intruded by the government.[252] Not only were none of Davis's conversations recorded, he was not tracked real-time with GPS.[253] Moreover, Davis's liberties were protected by the SCA's requirement that a neutral and detached magistrate be presented with specific and articulable facts that the sought CSLI be material and reasonably relevant to an ongoing criminal investigation.[254] Thus, the Eleventh Circuit found that "any intrusion on Davis's alleged privacy expectation . . . was minimal."[255]

The Eleventh Circuit next considered the interests of the government in obtaining CSLI in criminal investigations.[256] The court observed that historical CSLI "serve[s] compelling governmental interests" in many criminal cases because they are "routinely used to investigate the full gamut of state and federal crimes, including child abductions, bombings, kidnappings, murders, robberies, sex offenses, and terrorism-related offenses."[257] Additionally, the Eleventh Circuit recognized that CSLI is valuable to law enforcement during the early stages of investigations to "help build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources."[258]

---

248 *Id.* at 516–17 (quoting United States v. Watson, 423 U.S. 411, 416 (1976)).

249 *Id.* at 517 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

250 *Id.*

251 *Id.*

252 *Id.*

253 *Id.*

254 *Id.*

255 *Id.*

256 *See id.* at 518.

257 *Id.*

258 *Id.*

In its summation, the Eleventh Circuit concluded that "Davis had at most a diminished expectation of privacy" in his historical CSLI; production of his CSLI was not "a serious invasion of any such privacy interest"; the disclosure of CSLI pursuant to a § 2703(d) order "served substantial governmental interests"; and, therefore, a "strong presumption of constitutionality" applied to his case.[259] Thus, in its en banc *Davis* decision, the Eleventh Circuit agreed with the Third and Fifth Circuits, declaring that § 2703(d) of the SCA "comports with applicable Fourth Amendment principles and is not constitutionally unreasonable," despite not satisfying the probable cause requirement of the Warrant Clause.[260]

2. The Pryor Concurrence[261]

Despite joining the majority opinion in full, Judge William Pryor wrote separately to argue that strict application of the third-party doctrine demands that a court order compelling disclosure of CSLI would not violate a person's Fourth Amendment rights, even if the protections of the SCA did not exist.[262] Because a person has no legitimate expectation of privacy in information he voluntarily discloses to third-parties, and because "[t]here is no doubt that Davis voluntarily disclosed his location to a third party by using a cell phone to place or receive calls," Judge Pryor declared that "this appeal is easy."[263]

Comparing Davis's appeal to the facts of *Smith* and *Miller*, Judge Pryor saw no distinction between the records of dialed numbers created through the use of landlines in *Smith* and the records of historical CSLI created through the use of cell phones.[264] Judge Pryor dismissed the argument that CSLI is created less voluntarily than records of dialed numbers simply because the latter involves affirmative action.[265] "[I]n neither case is a phone user coerced to reveal anything."[266] If a telephone user wishes not to reveal the numbers he dials to the telephone company, "he has another option: don't place a call."[267] Likewise, if a cell phone user wishes not to reveal his physical movements to his cellular carrier, he has "another option: turn off the cell phone."[268]

---

259 *Id.*

260 *Id.*

261 Judge William Pryor filed a concurrence, not to be confused with Judge Jill Pryor who joined the *Davis* dissent.

262 *Davis*, 785 F.3d at 519 (Pryor, J., concurring).

263 *Id.*

264 *Id.*

265 *Id.* at 520.

266 *Id.*

267 *Id.*

268 *Id.*

Moreover, Judge Pryor found Davis's disclosure of his location to his cell phone provider was "no less 'knowing' than the disclosure at issue in *Smith*."[269] In *Smith*, the Supreme Court ruled that telephone users know they convey phone numbers to the telephone company because it is through the telephone company's switching equipment that calls are completed.[270] Similarly, Judge Pryor found that although "most people may be oblivious to the 'esoteric functions' of a technology," it cannot be believed that "cell phone users lack 'some awareness' that they communicate information about their location to cell towers."[271] Therefore, Judge Pryor concluded that the third-party rule of *Smith* defeats Davis's appeal, irrespective of the SCA and its reasonable suspicion warrants.[272]

Judge Pryor also cautioned that even if the rapid advancement of technology implicates proper interpretation of the Fourth Amendment, the courts must exercise restraint because Congress, not the judiciary, has the ability to adequately address complex and evolving technologies.[273] "Simply put, we must apply the law and leave the task of developing new rules for rapidly changing technologies to the branch most capable of weighing the costs and benefits of doing so."[274]

Finally, Judge Pryor commented that the Eleventh Circuit, as an inferior court, has "no business . . . anticipating the future decisions of the Supreme Court."[275] "If the third-party doctrine results in an unacceptable 'slippery slope,' the Supreme Court can tell us as much."[276] Thus, if such decisions as *Jones* have "given reasons to doubt the rule's breadth," Judge Pryor concluded that the Supreme Court "alone must decide the exceptions to its rule."[277]

3. The Jordan Concurrence[278]

Adopting a more circumspect approach, Judge Adalberto Jordan predicted that Davis's case would be not only about the present, "but . . . also potentially about the future."[279] Judge Jordan remarked that as technology becomes more sophisticated, CSLI "will undoubtedly become more precise and

---

269 *Id.*

270 *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 742 (1979)).

271 *Id.* (quoting *Smith*, 442 U.S. at 742) (citations omitted).

272 *See id.* at 519.

273 *See id.* at 520.

274 *Id.*

275 *Id.* at 521.

276 *Id.* (citations omitted).

277 *Id.*

278 Judge Wilson joined Judge Jordan's concurrence.

279 *Davis*, 785 F.3d at 521 (Jordan, J., concurring).

easier to obtain, and if there is no expectation of privacy here, I have some concerns about the government being able to conduct 24/7 electronic tracking (live or historical) in the years to come without an appropriate judicial order."[280] As a result, Judge Jordan contended that the Eleventh Circuit should decide *Davis* on reasonableness grounds and leave broader expectation of privacy issues for another case.[281] The Supreme Court did so in *City of Ontario v. Quon*[282] when it simply assumed that a police officer had a privacy expectation in text messages he sent from his city-issued pager, despite those messages being routed through a third-party service provider.[283] Accordingly, Judge Jordan assumed that Davis had a diminished expectation of privacy in his CSLI, but found that the government nevertheless satisfied the Fourth Amendment's reasonableness requirements by using § 2703(d) of the SCA to obtain such records.[284]

Judge Jordan contended that the third-party doctrine diminished whatever privacy expectation Davis had in his CSLI, and that in such cases warrantless searches and seizures may still satisfy the reasonableness requirement of the Fourth Amendment.[285] In Davis's case, Judge Jordan determined that whatever search occurred when the government obtained Davis's CSLI, it was reasonable, first, because the protocol of the SCA was followed, and second, because "temporal scope of the [CSLI] request . . . was reasonable."[286] The government only requested a period spanning from six days before the first robbery to six days after the last robbery in order to determine Davis's location at the time of the robberies and whether and to what extent he communicated with the other suspects.[287] Finally, Judge Jordan noted that there was no passive tracking in *Davis* that occurred by virtue of Davis simply carrying a cell phone; the CSLI used against him at trial contained solely the calls he placed or received.[288] Thus, Judge Jordan concluded the government's use of § 2703(d) of the SCA to obtain Davis's CSLI was constitutionally reasonable.[289]

---

280 *Id.* (citations omitted).

281 *See id.*

282 560 U.S. 746, 759–60 (2010).

283 *See Davis*, 785 F.3d at 521–22 (citing *Quon*, 560 U.S. at 759–60).

284 *Id.*

285 *Id.* at 522–23 (quoting Maryland v. King, 133 S. Ct. 1958, 1969 (2013)).

286 *Id.* at 524.

287 *Id.*

288 *Id.*

289 *See id.* at 522.

4. The Rosenbaum Concurrence

Judge Robin S. Rosenbaum, while concurring in the judgment of the Eleventh Circuit, wrote separately to give additional discussion to the third-party doctrine in the context of modern technology because "unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life."[290] Judge Rosenbaum continued, "the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling."[291] Recalling the "problem" identified by Justice Marshall in his *Smith* dissent, Judge Rosenbaum reminded the Eleventh Circuit that the third-party doctrine forces "a person . . . to forgo use of what for many years has become a personal or professional necessity, . . . [or] accept the risk of surveillance."[292] Despite her reservations regarding the practical effect of third-party doctrine, Judge Rosenbaum joined the majority opinion of the Eleventh Circuit because "we are not the Supreme Court and . . . we must apply the third-party doctrine where appropriate."[293]

Judge Rosenbaum deemed that the third-party doctrine was appropriate in *Davis* because there is no specific historically protected privacy interest analogous to CSLI, and because the privacy interest implicated by CSLI "is materially indistinguishable" from the privacy interests at issue in *Smith*.[294] Therefore, Judge Rosenbaum concluded that *Smith* must govern the case and the Eleventh Circuit's approval of the § 2703(d) order compelling disclosure of Davis's CSLI could not be avoided.[295] Finally, Judge Rosenbaum's concurrence concluded with the forewarning that if historically protected privacy interests are subordinated by courts to the third-party doctrine, "then with every new technology, we [will] surrender more and more of our historically protected Fourth Amendment interests to unreasonable searches and seizures."[296]

---

290 *Id.* at 524–25 (Rosenbaum, J., concurring).

291 *Id.* at 525.

292 *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting)).

293 *Id.*

294 *Id.* at 531–32.

295 *Id.* at 531.

296 *Id.* at 532–33.

5. The Dissent

Judge Beverly B. Martin, with Judge Jill Pryor joining, filed the dissent to the Eleventh Circuit's en banc *Davis* opinion.[297] Challenging the majority's position that the third-party doctrine is dispositive of the case, Judge Martin indicated that her "reading of Supreme Court precedent suggests that things are not so simple."[298] Rather, Judge Martin maintained that the Fourth Amendment prohibits the government from subjecting the citizenry "to constant location tracking of their cell phones without . . . a warrant" supported by probable cause.[299]

First, Judge Martin contended that not only was the third-party doctrine formulated nearly 40 years ago in the context of manually dialed phone numbers and bank records, but also that dialed numbers are "readily distinguishable" from the precedent of *Smith*.[300] Judge Martin argued that *Smith* turned on the idea that phone users voluntarily convey the numbers they dial by affirmatively entering a desired number when placing a call, whereas cell phone users do not affirmatively enter their location in order to place a call, and therefore do not voluntarily disclose their CSLI.[301] Additionally, Judge Martin asserted that the majority's emphasis on *Smith* was misguided because in that case phone users were "required . . . to recite phone numbers out loud to a phone operator in order to make a call," and therefore knew that they conveyed numerical information to the phone company.[302] Conversely, there is no similar "knowing" disclosure of CSLI because cell phone users have never had to provide their location in order to place a call.[303] Thus, Judge Martin concluded that *Smith* does not control *Davis*.[304]

Second, Judge Martin noted that although the third-party doctrine appears to allow government access to "*all* information that *any* third-party obtains," Supreme Court precedent has given reasons to "doubt the rule's breadth."[305] As evidence, Judge Martin called the Eleventh Circuit's attention to a number of contexts in which the Supreme Court found a privacy right in information despite its disclosure to third-parties, including the results of diagnostic medical tests,[306] letters and other sealed packages,[307] and hotel

297 *Id.* at 533 (Martin, J., dissenting).

298 *Id.*

299 *Id.* at 544.

300 *Id.* at 534.

301 *Id.*

302 *Id.* (citing Smith v. Maryland, 442 U.S. 735, 743 (1979)).

303 *Id.* at 534–35.

304 *Id.* at 535.

305 *Id.*

306 *Id.* (citing Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001)).

rooms.[308] Judge Martin conceded that such contexts are distinguishable from *Davis*, but argued that they no less demonstrate that "the third-party doctrine may not be as all-encompassing as the majority seems to believe."[309]

Third, Judge Martin determined that the majority's "blunt application" of the third-party doctrine "threatens to allow government access to a staggering amount of information that surely must be protected under the Fourth Amendment," such as our e-mail accounts and online browsing history.[310] Judge Martin argued that the majority's application of the third-party doctrine would result in the absolute forfeiture of any privacy interest in, among other things, our search-engine history, what we watch online, whom we "friend," what we buy, what we research, and whom we date, simply because such records are necessarily routed through and maintained by third parties for legitimate business purposes.[311] Judge Martin posited that the "enormous impact of this outcome is probably why at least one Circuit has held that a person's Fourth Amendment rights are violated when the government compels an internet service provider to turn over the contents of e-mails without a warrant."[312] If e-mails are protected despite their being surrendered to the control of a third party, then the third-party doctrine has its limits, Judge Martin reasoned.[313]

Fourth, Judge Martin criticized the majority's distinction between "content" and "non-content" data as being without a "coherent definition of the terms."[314] Moreover, Judge Martin recalled that even if a rational distinction between the two varieties of information can be drawn, at oral argument the government conceded that the majority's conception of the third-party doctrine would permit its acquisition of such records as the sender and recipient of e-mails, the time e-mails are sent, the number of e-mails a person sends, the websites a person visits, and "maybe even the connections a person communicates with on a dating website and whom she meets in person—all without a warrant."[315]

Judge Martin next suggested the Supreme Court has "insisted" that technological advances require the judiciary to sometimes reconsider the scope of "decades-old Fourth Amendment rules," because a "wooden application" of the third-party doctrine would result in a slippery slope in such information

---

307 *Id.* (citing United States v. Jacobsen, 466 U.S. 109, 114 (1984)).

308 *Id.* (citing Stoner v. California, 376 U.S. 483, 487–88, 490 (1964)).

309 *Id.*

310 *Id.* at 535–37.

311 *Id.* at 537.

312 *Id.* at 536.

313 *Id.* at 537.

314 *Id.*

315 *Id.*

technology contexts as CSLI.[316] As evidence, Judge Martin cited *Riley v. California*,[317] in which the Supreme Court decided the continued vitality of its 41-year-old decision in *United States v. Robinson*,[318] which previously governed the search-incident-to-arrest exception to the Fourth Amendment.[319] Although "mechanical application of *Robinson* might well support the warrantless searches at issue," Judge Martin noted that the *Riley* Court nonetheless unanimously rejected *Robinson*, recognizing that "cell phones are based on technology nearly inconceivable" when *Robinson* was decided.[320] Similarly, Judge Martin contended that the third-party doctrine is outdated because the degree with which individuals convey information to third-parties has increased by "orders of magnitude" since *Smith* and *Miller*.[321] Judge Martin observed that society's deep reliance on third-party technology providers enables, as in *Davis*, the government to obtain months of "near-constant" CSLI—a "technological feat impossible to imagine" when the Supreme Court decided *Smith* and *Miller*.[322]

Fifth, and finally, Judge Martin rejected the majority's reliance on the third-party doctrine to uphold the SCA's constitutionality and instead analyzed *Davis* employing the traditional objective and subjective expectation of privacy tests set forth in *Katz*.[323] Judge Martin declared that, "the answer to the subjective inquiry is easy" because individuals do not expect "the government to track them" because they use "what amounts to a basic necessity of twenty-first century life—the cell phone."[324] Conversely, Judge Martin determined that the "more difficult question" is whether Davis's expectation of privacy was one society recognizes as objectively reasonable.[325] Applying the opinions of five Justices in *Jones*—which established that long-term location monitoring generally violates reasonable expectations of privacy—Judge Martin determined that Davis's subjective expectation of privacy in the amount of CSLI the government used against him at trial was likely one society would recognize as objectively reasonable.[326] Judge Martin thus concluded that because the 67 days of CSLI collected in *Davis* more than doubled the 28 days of tracking that five Justices decided was unconstitutionally long-term in

316 *Id.*

317 134 S. Ct. 2473 (2014).

318 414 U.S. 218 (1973).

319 *Davis*, 785 F.3d at 537 (Martin, J., dissenting).

320 *Id.* (quoting *Riley*, 134 S. Ct. at 2484, 2488–89).

321 *Id.* at 538.

322 *Id.*

323 *Id.*

324 *Id.* at 538–39.

325 *Id.* at 539.

326 *Id.* at 539–41.

Jones,[327] the SCA's temporally limitless § 2703(d) reasonable suspicion warrants violate the Fourth Amendment.[328]

D. The Fourth Circuit: Graham

Exactly three months after an en banc Eleventh Circuit upheld the constitutionality of the reasonable suspicion warrants of § 2703(d) of the SCA—which eliminated the federal circuit split on the issue—in August 2015 the split was revived by the Fourth Circuit's panel decision in *United States v. Graham*.[329] In *Graham*, a panel of Fourth Circuit judges considered the appeal of two criminal defendants challenging the constitutionality of the district court's admission at trial of 221 days of their CSLI.[330] Specifically, Graham and his co-defendant[331] challenged the district court's denial of their motion to suppress their historical CSLI, arguing that the government's acquisition of such records without a warrant supported by probable cause was an unreasonable search in violation of the Fourth Amendment.[332] The Fourth Circuit panel agreed, resurrecting the federal circuit split on the constitutionality of § 2703(d) of the SCA.

On October 28, 2015, however, the *Graham* panel decision was vacated when the Fourth Circuit granted the government's petition to rehear the case en banc.[333] Thus, presently, the Third, Fifth, and Eleventh Circuits affirm the constitutionality of the SCA's reasonable suspicion warrants, and the en banc Fourth Circuit is determining whether to accept or reject them. Though nullified, the *Graham* panel decision remains valuable to the extant discussion of the SCA's constitutionality and will therefore be examined below.

---

327 *See id.* at 540.

328 *See id.* at 544–45.

329 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, Nos. 12-4659(L), 12-4825, 2015 WL 6531272 (4th Cir. Oct. 28, 2015).

330 *Id.* at 338.

331 For ease of readability, hereinafter this Note will refer solely to Graham, rather than to Graham and his co-defendant.

332 *Graham*, 796 F.3d at 342–43.

333 796 F.3d 332 (4th Cir. 2015), *reh'g en banc granted*, Nos. 12-4659(L), 12-4825, 2015 WL 6531272 (4th Cir. Oct. 28, 2015).

1. The Majority Opinion[334]

i. Fourth Amendment Introduction

First, after detailing the particular facts of Graham's underlying case, the Fourth Circuit delivered a brief review of essential Fourth Amendment principles.[335] The court recalled that the Fourth Amendment protects persons from unreasonable searches and seizures[336] and that Fourth Amendment searches occur where the government invades a matter in which a person possesses a subjective expectation of privacy that society is willing to recognize as objectively reasonable.[337] A person's subjective expectation of privacy is objectively reasonable, the court explained, when it is derived from "understandings that are recognized and permitted by society."[338] Finally, the Fourth Circuit concluded by mentioning that, absent a few specific exceptions, warrantless searches are "*per se* unreasonable" under the Fourth Amendment.[339]

ii. Cell Phone Privacy Agreements

Second, the Fourth Circuit rejected the district court's determination that Graham lacked a subjective expectation of privacy in his CSLI because he waived it by agreeing to his service provider's privacy policy.[340] Rather, the *Graham* court demonstrated that although Graham's service provider's privacy policy indicated that his CSLI would be collected, there was no disclosure of the fact that Graham's CSLI would be disclosed to the government or any other third-party.[341] Furthermore, the court noted that recent studies show users of electronic communications services frequently "do not read or understand their

---

334 Judge Thacker also filed a concurrence to the majority opinion in which she expressed generalized "concern about the erosion of privacy in this era of rapid technological development." *Id.* at 377 (Thacker, J., concurring). Judge Thacker cautioned that as "technological progress continues to advance upon our zone of privacy, each step forward should be met with considered judgment that errs on the side of protecting privacy and accounts for the practical realities of modern life." *Id.* at 378. Finally, Judge Thacker praised the majority's decision as one that "continues a time-honored American tradition—obtaining a warrant is the rule, not the exception." *Id.*

335 *Id.* at 345 (majority opinion).

336 *Id.* at 344 (citing Katz v. United States, 389 U.S. 347, 353 (1967)).

337 *Id.* (citing *Katz*, 389 U.S. at 353).

338 *Id.* (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1988)).

339 *Id.* (quoting United States v. Davis, 690 F.3d 226, 241–42 (4th Cir. 2012)).

340 *Id.* at 345.

341 *Id.*

providers' privacy policies."[342] The Fourth Circuit therefore concluded that the district court erroneously decided that Graham either read or understood his cell phone service provider's privacy policy.[343]

iii. Fourth Amendment Case Review

Third, the Fourth Circuit concluded that the Supreme Court has recognized an individual's privacy interest in comprehensive accounts of the movements of both her person and her personal property within private spaces, particularly when such information may be gleaned only through technological means not in use by the general public.[344] To support that conclusion, the *Graham* court then analyzed the major cases applicable to the issue of whether CSLI is constitutionally protected.[345]

Turning first to *United States v. Karo*,[346] the Fourth Circuit noted that law enforcement's surreptitious use of a radio transmitter to track a container within a private residence violated the Fourth Amendment rights of those persons with a justifiable privacy interest in the home.[347] Such invasive, warrantless tracking was deemed unconstitutional because the government could not have otherwise learned whether an item "is actually located at a particular time in [a] private residence" or whether it is in the possession "of the person or persons whose residence is being watched."[348] Next summarizing *Kyllo v. United States*,[349] the Fourth Circuit observed that warrantless government use of technology not in general public use to explore a home's interior to a degree previously unknowable without physical intrusion is a presumptively unreasonable Fourth Amendment search.[350]

Despite their general relevance to *Graham*, the Fourth Circuit found reason to distinguish *Karo* and *Kyllo*.[351] Unlike a cell phone, the *Graham* court reasoned, the tracking device in *Karo* was not carried on anyone's person and

---

342 *Id.* (citing FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 10 (Feb. 2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf; Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 544 (2008)).

343 *Id.*

344 *Id.*

345 *Id.* at 345–50.

346 468 U.S. 705 (1984).

347 *Graham*, 796 F.3d at 346 (citing *Karo*, 468 U.S. at 709–10, 714–15).

348 *Id.*

349 533 U.S. 27 (2001).

350 *Graham*, 796 F.3d at 346 (citing *Kyllo*, 533 U.S. at 40).

351 *Id.* at 347.

therefore could not track anyone's location.[352] Additionally, the Fourth Circuit noted that Graham's CSLI records used against him at trial covered a 221-day period, potentially placing him at home on dozens of specific occasions, far more than the single intrusions of *Karo* and *Kyllo*.[353] Thus, the Fourth Circuit concluded that long-term inspection of CSLI invades a greater Fourth Amendment privacy interest than the searches challenged in both *Karo* and *Kyllo*.[354]

The Fourth Circuit then addressed *United States v. Jones*[355]—and its underlying case, *United States v. Maynard*[356]—the most recent Supreme Court case pertaining directly to long-term electronic location surveillance.[357] In *Jones*, five Justices applied the traditional two-pronged reasonable expectation of privacy test of *Katz* to the government's warrantless GPS tracking of a vehicle over a 28-day period, holding that the surveillance impinged on Jones's reasonable expectation of privacy.[358] Despite acknowledging that *Jones* left unresolved how long government surveillance must occur before the protections of the Fourth Amendment are triggered, the *Graham* court observed that Justice Sotomayor's *Jones* concurrence expressed concerns about the implications of the government's ability to aggregate an individual's location information.[359] Specifically, Justice Sotomayor realized that such ability enables authorities to ascertain "more or less at will," many private, and presumably constitutionally protected, facts about a person's life.[360]

The *Graham* court concluded that the privacy interests associated with the long-term GPS tracking in *Jones* apply "with equal or greater force to historical CSLI for an extended time period," because both long-term GPS monitoring and long-term CSLI monitoring can reveal "a comprehensive view and specific details of [an] individual's daily life."[361] Moreover, the Fourth Circuit remarked that long-term monitoring of CSLI has the potential to be far more invasive than the *Jones* GPS monitoring because a cell phone, unlike an automobile, is not limited to traveling on roadways.[362] Rather, a cell phone is a small, hand-held device that seldom leaves its owner's possession and

---

352 *Id.*

353 *Id.* (citing *Kyllo*, 533 U.S. at 30; *Karo*, 468 U.S. at 709, 714).

354 *Id.*

355 132 S. Ct. 945 (2012).

356 615 F.3d 544 (D.C. Cir. 2010).

357 *Graham*, 796 F.3d at 347.

358 *Id.*

359 *Id.* at 347–48 (citing *Jones*, 132 S. Ct. at 955–56).

360 *Id.* (citing *Jones*, 132 S. Ct. at 955–56) (noting that such tracking capability allows law enforcement to discern one's "political and religious beliefs, sexual habits, and so on").

361 *Id.* at 348.

362 *Id.*

frequently enters private locations.[363] Thus, the Fourth Circuit determined that CSLI "can permit the government to track a person's movements between public and private spaces, impacting at once her interests in both the privacy of her movements and the privacy of her home."[364]

Next, the Fourth Circuit cited numerous state and federal district court cases recognizing as objectively reasonable cell phone users' expectation of privacy in their long-term CSLI, commenting that "it is not surprising" so many courts have done so.[365] However, not only inferior courts, the court continued, have recognized a privacy expectation in CSLI.[366] In *Riley v. California*[367]—a case regarding the warrantless inspection of a cell phone confiscated by law enforcement following a search incident to a lawful arrest—the Supreme Court cited "'[h]istoric location information' as among the heightened privacy concerns presented in government inspection of cell phones, as such information details the user's 'specific movements down to the minute, not only around town but also within a particular building.'"[368] Accordingly, the Fourth Circuit held that, taken together, *Karo*, *Kyllo*, *Jones*, and *Riley* support the conclusion that the government invades a reasonable expectation of privacy when it utilizes technology not in general use to discover the movements of an individual over an extended period of time.[369] The Fourth Circuit thus ruled that the government engages in a Fourth Amendment search when it seeks to examine historical CSLI records pertaining to an extended period of time like 14[370] or 221 days.[371]

---

363 *Id.*

364 *Id.*

365 *Id.* at 349 ("[Commonwealth v.] Augustine, 4 N.E.3d [846,] 865–66 [(Mass. 2014)] (reasonable expectation of privacy in location information shown in historical CSLI records); [State v.] Earls, 70 A.3d [630,] 632 [(N.J. 2013)] (reasonable expectation of privacy in location of cell phones); Tracey v. State, 152 So.3d 504, 526 (Fla. 2014) (objectively reasonable expectation of privacy in 'location as signaled by one's cell phone'); *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 539 (D. Md. 2011) ('reasonable expectation of privacy both in [subject's] location as revealed by real-time [CSLI] and in his movement where his location is subject to continuous tracking over an extended period of time, here thirty days.'); *In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info. (In re Application (E.D.N.Y.)), 809 F. Supp. 2d 113, 120 (E.D.N.Y. 2011) ('reasonable expectation of privacy in long-term cell-location records')." (emphasis added)).

366 *Id.*

367 134 S. Ct. 2473 (2014).

368 *Graham*, 796 F.3d at 349 (quoting *Riley*, 134 S. Ct. at 2490).

369 *Id.*

370 *See id.* at 344 (explaining that two § 2703(d) orders were obtained by the government; the first order directed Sprint/Nextel to provide CSLI records for a total of 14 days, and the second order compelled production of 221 days of CSLI that included the previously-obtained 14-day span of records).

iv. CSLI Contemporaneousness and Precision

Fourth, the Fourth Circuit rejected as "constitutionally insignificant" the district court's distinction between *Graham* and *Karo* and *Jones* on the basis that the surveillance in those cases was continuous and real-time, whereas Graham's CSLI was historical and intermittent.[372] The *Graham* court observed that the government was unable to know before obtaining Graham's CSLI records how voluminous and detailed they would be.[373] Consequently, prior to obtaining a § 2703(d) order compelling production of Graham's CSLI by his service provider for the desired period, it would be impossible for the government to know whether no records existed, or whether, as was the actual case, Graham's CSLI would reveal "an impressive 29,659 location data points" amounting to an average of well over 100 daily location data points.[374] The court concluded that examination of such extensive CSLI records provided the government with a "reasonably detailed account" of Graham's movements—in public locations as well as the home—during the obtained 221-day time period.[375] The Fourth Circuit therefore rejected the district court's suggestion that Graham's CSLI was insufficiently continuous to raise Fourth Amendment privacy concerns.[376]

Next the Fourth Circuit countered the district court's conclusion that Graham's CSLI only revealed the general vicinity of his cell phone, and was insufficiently precise to invade his reasonable expectation of privacy.[377] The *Graham* court noted that although the precision of CSLI partly depends on size and coverage areas of cell phone service, there is "intense competition"[378] among providers to eliminate gaps in coverage and increase CSLI precision, and *Kyllo* requires the court to consider such advancements when determining

---

371 *Id.* at 350. In so ruling, the court recognized, but dismissed, the argument that CSLI may not be revealing because a cell phone may not be powered on or connecting with nearby towers. *Id.* at 349–50. Rather, the "government cannot know in advance of obtaining this information how revealing it will be or whether it will detail the cell phone user's movements in private spaces." *Id.* at 350 (citing State v. Earls, 70 A.3d 630, 642 (N.J. 2013)).

372 *Id.*

373 *Id.*

374 *Id.*

375 *Id.*

376 *Id.*

377 *Id.*

378 *Id.* at 350–51 (noting that service providers have "begun to increase network capacity and to fill gaps in network coverage by installing low-power cells such as 'microcells' and 'femtocells,' which cover areas as small as 40 feet").

the typical capability of a technology.[379] Accordingly, the Fourth Circuit assessed the precision of Graham's CSLI and decided that it was exact enough to provide at least "reasonable inferences" about his locations at specific points in time.[380] The court reasoned that Graham's CSLI would not have been relied upon if it were not sufficiently precise to establish his whereabouts.[381] The court also foreclosed any argument that Graham's CSLI is constitutionally too imprecise to be considered a Fourth Amendment search because examination of his CSLI may require the drawing of inferences to glean his exact location at particular times.[382] "Indeed, the Supreme Court, in *Kyllo*, specifically rejected 'the novel proposition that inference insulates a search'" from constitutional scrutiny.[383] The Fourth Circuit thus rejected the district court's argument that Graham's CSLI was insufficiently precise to infringe upon his expectations of privacy in his locations and movements.[384]

v. Third-Party Doctrine

Fifth, the Fourth Circuit disagreed with the conclusion of the dissent and the district court that Graham lacked a reasonable expectation of privacy in his CSLI because his cell phone service provider maintained them in the ordinary course of business.[385] Rather, to the *Graham* court, it was clear that "cell phone users do not voluntarily convey their CSLI to their service providers. The third-party doctrine of *Miller*[386] and *Smith*[387] is therefore inapplicable here."[388]

The Fourth Circuit began the third-party doctrine portion of the opinion by briefly summarizing cases in which voluntary disclosure of information to third-parties was held to constitute abandonment of privacy in the exposed information: *Smith*, *Miller*, and a similar Fourth Circuit case, *United States v. Bynum*,[389] in which a website user was deemed to have no expectation of privacy in his account information.[390] However, the court distinguished those

---

379 *Id.* ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001))).

380 *Id.* at 351.

381 *Id.*

382 *Id.*

383 *Id.* (quoting *Kyllo*, 533 U.S. at 36) (citing United States v. Karo, 468 U.S. 705 (1984)).

384 *Id.*

385 *Id.*

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

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

388 *Graham*, 796 F.3d at 352.

389 604 F.3d 161 (4th Cir. 2010).

390 *Graham*, 796 F.3d at 354.

cases from *Graham*.[391] In those cases, the Fourth Circuit held there was voluntary conveyance of the information to a third-party, whereas in *Graham* no such conveyance occurred because "a cell phone user does not 'convey' CSLI to her service provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement."[392]

Not only is CSLI automatically generated with or without the user's participation, the court noted, a cell phone user never submits any location information to complete a call.[393] Moreover, the CSLI in *Graham* detailed not only location information for outgoing communications, but also for incoming communications—even messages or calls that went unanswered.[394] The Fourth Circuit therefore refused to "impute to a cell phone user the risk that information about her location created by her service provider will be disclosed to law enforcement when she herself has not actively disclosed this information."[395]

The Fourth Circuit then directly addressed the contrary positions of the Fifth and Eleventh Circuits that general use of a cell phone demonstrates the user's voluntary conveyance of CSLI, notwithstanding that cell phone users "[do] not directly inform [their] service provider" of their whereabouts.[396] Observing that cell phone use is ubiquitous in society and essential to full cultural and economic participation for a growing segment of society, the Fourth Circuit reasoned that "[p]eople cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones."[397]

Furthermore, the *Graham* court argued that, despite assertions of the Fifth and Eleventh Circuits to the contrary, CSLI records are not of the same nature as those documents routinely stored by third-party businesses and obtained by the government by subpoena.[398] Rather, the Fourth Circuit classified CSLI records as "wholly unlike" other routine business records—such as credit card statements, hotel bills, and purchase orders—because the latter require overt and voluntary transactions to create, whereas CSLI is third-party recording of the location of cell phone users regardless of whether the user is an active and voluntary participant in the recording.[399]

---

391 *Id.*

392 *Id.*

393 *Id.*

394 *Id.* at 355.

395 *Id.*

396 *Id.* (citing United States v. Davis, 785 F.3d 498 (11th Cir. 2015); *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2014)).

397 *Id.* at 356.

398 *Id.* at 356–57.

399 *Id.* at 357.

The Fourth Circuit next agreed with the Fifth and Eleventh Circuits that a service provider's business interest in maintaining CSLI records is a relevant consideration in determining whether a cell phone user can maintain a reasonable expectation of privacy in such records.[400] However, the court noted that business interests are not the only interests to be weighed.[401] In addition to properly considering real and personal property law concepts, courts must consider the understandings recognized and permitted in society.[402] Mentioning again that society recognizes an individual's interest in maintaining privacy in her movements over an extended period as well as her movements in private places, the Fourth Circuit held that an individual maintains such an expectation in such records—even if a cell phone provider records and stores them—so long as the cell phone user does actively participate in their creation.[403] To hold otherwise, the court noted, would permit the government to "convert an individual's cell phone into a tracking device by examining the massive bank of location information retained by her service provider, and to do so without probable cause."[404]

Next the court commented that in the digital age courts routinely accord Fourth Amendment protections to digital information the creator intends to keep private but must route through third-parties.[405] For example, the Fourth Circuit noted that the Fourth Amendment has been held to apply to the content of e-mails, but not the e-mail address information used to transmit the e-mails.[406] The court distinguished CSLI from e-mail transmission data, however, noting that "CSLI is of course more than simple routing information; it tracks a cell phone user's location across specific points in time."[407] Furthermore, there is nothing a cell phone user can do to hide her location from her service provider, whereas an e-mail drafter can take reasonable steps to maintain her anonymity.[408] Thus, in the absence of evidence that Graham or cell phone users in general intend for CSLI to be open to inspection by others, the Fourth Circuit concluded that a cell phone user's Fourth Amendment interest in CSLI is not extinguished because CSLI is a tool used by third-parties to route communications.[409]

---

400 *Id.*

401 *Id.*

402 *Id.* (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1998)).

403 *Id.*

404 *Id.*

405 *Id.* at 358.

406 *Id.* (citing United States v. Warshak, 631 F.3d 266, 287–88 (6th Cir. 2010)).

407 *Id.*

408 *Id.* at 358–59.

409 *Id.* at 359.

Finally, the Fourth Circuit discussed the inherent conflict between the protections of the Fourth Amendment and the advancement of technology and provided its approach to deciding such cases.[410] The court resolved that, "even as technology evolves, protections against government intrusion should remain consistent with those privacy expectations society deems reasonable."[411] And although society's privacy expectations can change over time, the advent of new technology alone is not a sufficient basis to infer an immediate and equally dramatic shift in people's privacy expectations.[412] Moreover, "[t]he third-party doctrine is intended to delimit Fourth Amendment protections where privacy claims are not reasonable—not to diminish Fourth Amendment protections where new technology provides new means for acquiring private information."[413] The court rejected the temptation to apply the third-party doctrine to Graham's case, noting that if the modern Fourth Amendment is to be a "shrunken one," such a "solemn task" should be left to the "superiors in the majestic building on First Street."[414] Thus, the Fourth Circuit held that the relatively new technology of CSLI, which facilitates the eased tracking of individuals' movements, cannot by itself displace society's reasonable privacy expectations, nor can it justify governmental inspection of CSLI records by the government in absence of judicially-determined probable cause.[415] With its ruling in *Graham*, therefore, the Fourth Circuit declared that the reasonable suspicion warrants of § 2703(d) of the SCA violate the Fourth Amendment.[416]

2. Motz Dissent

Judge Diana G. Motz filed a dissent to the Fourth Circuit's *Graham* decision.[417] Advocating judicial restraint, Judge Motz argued that the "well-established"[418] third-party doctrine must be followed by inferior courts until overturned by the Supreme Court or revised by Congress or state legislatures,

---

410 *Id.* at 359–61.

411 *Id.* at 359.

412 *Id.*

413 *Id.* at 360.

414 *Id.* at 361.

415 *Id.*

416 Notwithstanding the fundamental holding of *Graham*, the Fourth Circuit affirmed Graham's conviction by applying the "good-faith exception" to the Fourth Amendment to the SCA. *Id.* at 361. "Prior to our ruling today, neither this Court nor the U.S. Supreme Court had deemed the government's conduct in this case unconstitutional." *Id.* at 363. The Fourth Circuit accordingly concluded that "the government reasonably relied on the SCA in exercising its option to seek a § 2703(d) order rather than a warrant." *Id.*

417 *Id.* at 378 (Motz, J., dissenting).

418 *Id.*

despite the temptation to remedy perceived Fourth Amendment deficiencies from the bench.[419]

Applying the third-party doctrine to *Graham*, Judge Motz determined that when Graham elected to use a cell phone he "unquestionably 'exposed'" his CSLI to his cell phone service provider and thereby assumed the risk that such records would be disclosed to the government.[420] Graham therefore lacked any basis to assert an expectation of privacy in his CSLI.[421] Accordingly, the government's acquisition of Graham's historical CSLI pursuant to § 2703(d) orders rather than warrants did not violate the Fourth Amendment, Judge Motz concluded.[422]

Finally, Judge Motz noted that although "[t]ime may show that [the majority has] struck the proper balance between technology and privacy[,] . . . it will only be because the Supreme Court revises its decades-old understanding of how the Fourth Amendment treats information voluntarily disclosed to third parties."[423] Judge Motz accordingly concluded that the *Graham* decision was inappropriate because the majority "endeavor[ed] to beat the Supreme Court to the punch."[424]

The next Part attempts to refute the prevailing federal appellate SCA jurisprudence and argues that the proper interpretation of § 2703(d)'s constitutionality is that of the Fourth Circuit: it violates the Fourth Amendment.

V. THE SCA CONTRADICTS THE FOURTH AMENDMENT

Section 2703(d) of the SCA violates the Fourth Amendment because individuals have a legitimate expectation of privacy in CSLI, and thus the government must first obtain a warrant supported by probable cause to access CSLI. To support this assertion, this Part will argue that (1) the Founders would likely have abhorred the nearly boundless nature of the SCA; (2) the SCA violates both the Warrant and Probable Cause Clauses of the Fourth Amendment; (3) cell phone users maintain a reasonable expectation of privacy in CSLI, notwithstanding the third-party doctrine; and (4) the needs of law enforcement do not justify warrantless access to CSLI.

---

419 *Id.* at 378, 388–89 (contending that the majority's decision "lacks support from all relevant authority and places us in conflict with the Supreme Court" and that not only are "Congress and state legislatures . . . far better positioned to respond to changes in technology than are the courts," but also the "very statute at issue here, the Stored Communications Act (SCA), demonstrates that Congress can—and does—make these judgments").

420 *Id.* at 380.

421 *Id.*

422 *Id.*

423 *Id.* at 390.

424 *Id.*

A. *Founders' Intent*

Records of the Fourth Amendment's pre-ratification debate among the Founders are sparse.[425] However, both an examination of history and an application of common sense indicate that in passing the Fourth Amendment, our forefathers could neither have anticipated nor approved of the massive constitutional loophole created by the reasonable suspicion requirement of § 2703(d) of the SCA.[426]

Although the Founders appreciated the necessity of a powerful and effective government, "they also feared what a powerful central government might bring, not only to the jeopardy of the states but to the terror of the individual."[427] The Founders "had known oppressive government,"[428] in the form of general warrants and writs of assistance, which gave British officers carte blanche to search homes for evidence of criminal activity.[429] Opposition to the government's unbridled ability to probe into citizens' affairs not only largely motivated the Fourth Amendment's passage[430] but "was in fact one of the driving forces behind the Revolution itself."[431]

The SCA, which allows the government to track virtually every American older than the age of 12, provides minimal judicial oversight and offers nearly no legal recourse.[432] The SCA is a modern permutation of the general warrants the crafters of the Fourth Amendment abhorred.[433] Accordingly, although the opinions of reasonable individuals may differ, contemporary understanding of the Founders' intent in drafting and enacting the protections of the Fourth Amendment strongly suggests that they would vehemently oppose the government's boundless surveillance capabilities under the SCA.[434] Beyond the historical motivations of our forefathers, the language of the Fourth Amendment itself demonstrates that the SCA is repugnant to the Constitution. The following section demonstrates the irreconcilability of the

---

425 Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 1047 (2011).

426 *See* Curtis, Gizzi & Kittleson, *supra* note 160, at 91 ("[I]t is hard to imagine that a nation founded on the principles of liberty and freedom would countenance a society in which the pre-condition for participation in the social and business life of the nation is to give to the government the ability to track your location at all times.").

427 THE FOURTH AMENDMENT: SEARCHES AND SEIZURES: ITS CONSTITUTIONAL HISTORY AND THE CONTEMPORARY DEBATE 54 (Cynthia Lee ed., 2011) [hereinafter THE FOURTH AMENDMENT].

428 *Id.* at 55.

429 Riley v. California, 134 S. Ct. 2473, 2494 (2014).

430 *Id.*

431 *Id.*

432 *See* Curtis, Gizzi & Kittleson, *supra* note 160, at 90.

433 *See Riley*, 134 S. Ct. at 2494.

434 *See, e.g.*, *supra* note 38–42 and accompanying text.

SCA with the Fourth Amendment's guarantee that searches and seizures will be authorized by warrants supported by probable cause.

B. Warrant and Probable Cause Clauses

Not only is the SCA inconsistent with the Founders' ideas of privacy, the SCA is unconstitutional because it violates both the Fourth Amendment's Warrant and Probable Cause Clauses. The Fourth Amendment explicitly mandates both that Americans are to be free from unreasonable searches and seizures and that no warrant shall be issued unless supported by probable cause.[435] If, however, a warrant lacking probable cause is issued, any search or seizure authorized by it is deemed warrantless,[436] and warrantless government searches or seizures are per se unreasonable.[437] The SCA attempts to legislate around these Fourth Amendment guarantees by authorizing the issuance of warrants supported by reasonable suspicion, and is therefore plainly unconstitutional.[438]

The Constitution is the "supreme [l]aw of the [l]and,"[439] and any congressional legislation inconsistent with it is by definition unconstitutional.[440] The Fourth Amendment to the Constitution unequivocally requires that no warrants shall issue but upon demonstration of probable cause.[441] Moreover, the Supreme Court has held, "[i]f times have changed, reducing everyman's scope to do as he pleases in [the modern] world, . . . the values served by the Fourth Amendment [are] more, not less, important."[442]

Section 2703(d) of the SCA, however, merely requires reasonable suspicion for CSLI warrant issuance, which is a far less stringent evidentiary standard than the Fourth Amendment's "substantially higher"[443] probable cause standard.[444] Consequently, § 2703(d) is constitutionally deficient and judicial reliance on its language is improper.[445] The Eleventh Circuit in the *Davis* panel

---

435 U.S. CONST. amend. IV.

436 CLANCY, *supra* note 42.

437 Katz v. United States, 389 U.S. 347, 357 (1967); *see also* Groh v. Ramirez, 540 U.S. 551, 559 (2004) (finding warrantless searches and seizures "presumptively unreasonable").

438 *See* U.S. CONST. amend. IV; Stored Communications Act, 18 U.S.C. § 2703(d) (2013).

439 U.S. CONST. art. VI, cl. 2.

440 Marbury v. Madison, 5 U.S. 137, 138 (1803) (holding that acts of Congress "repugnant to the constitution *cannot* become a law" (emphasis added)).

441 U.S. CONST. amend. IV.

442 Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971).

443 United States v. Graham, 796 F.3d 332, 344 (4th Cir. 2015), *reh'g en banc granted*, Nos. 12-4659(L), 12-4825, 2015 WL 6531272 (4th Cir. Oct. 28, 2015).

444 *See* 18 U.S.C. § 2703(d) (2013).

445 *See Marbury*, 5 U.S. at 138.

decision appropriately recognized that "obtaining . . . [CSLI] without a warrant [supported by probable cause] is a Fourth Amendment violation."[446] Likewise, because federal code is subordinate to the Constitution, the Third Circuit in *Provider*,[447] the Fifth Circuit in *Historical*,[448] and the Eleventh Circuit in its en banc *Davis* decision[449] were mistaken to place any stock in § 2703(d), as its plain language is clearly at odds with the Fourth Amendment—specifically its probable cause requirement.[450]

However, Supreme Court precedent holds that the protections of the Fourth Amendment against unreasonable governmental searches and seizures are triggered only if one maintains a reasonable expectation of privacy in the object intruded on by the search or seizure.[451] Accordingly, the next Section will address whether cell phone users possess a reasonable expectation of privacy in their CSLI.

C. *Reasonable Expectation of Privacy and the Third-Party Doctrine*

Every day, people utilize public thoroughfares while traveling to public locations to conduct affairs they nevertheless intend to keep private. Most persons intend to keep secret the fact that they are treating terminal cancer, considering an abortion, or seeking therapy for Post-Traumatic Stress Disorder after multiple combat deployments.[452] Society, in turn, would likely recognize as reasonable such subjective expectations of privacy.

However, if these individuals carried a powered cell phone during their trips, a CSLI record documenting the journey was created and archived by their cell phone service providers.[453] And so long as that information is simply relevant to an ongoing criminal investigation, the SCA enables law enforcement to compel cell phone service providers to turn the record over.[454]

---

446 United States v. Davis, 754 F.3d 1205, 1217 (11th Cir.), *vacated*, 573 F. App'x 925 (11th Cir. 2014), *aff'd on reh'g*, 785 F.3d 498 (11th Cir. 2015).

447 *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 315 (3d Cir. 2010).

448 *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013) (finding that the "reasonable grounds" requirement of the SCA is not "per se unconstitutional").

449 *Davis*, 785 F.3d at 505–06.

450 U.S. CONST. amend. IV.

451 *See* Katz v. United States, 389 U.S. 347, 351 (1967).

452 *See, e.g.*, *supra* notes 2–7 and accompanying text.

453 *See* Harkins, *supra* note 15, at 1877 (indicating that a new CSLI record is created approximately once every seven seconds through a process known as registration in which cell phones communicate with the nearest cell phone tower to find the tower with the strongest reception).

454 18 U.S.C. § 2703(d) (2013).

Once in the hands of law enforcement, historical CSLI records allow the government to retrace months of a cell phone user's past whereabouts regardless of their private or sensitive nature.[455]

The following subsections will explain why cell phone users have a subjective expectation of privacy in historical CSLI and why society is prepared to declare this expectation as objectively reasonable.[456] This analysis will also argue that the third-party exception doctrine is inapplicable to CSLI and that, even if the third-party doctrine applies to some information disclosed to third-parties, cell phone users do not voluntarily disclose their CSLI to third-party service providers.

1. Cell Phone Users Have a Subjective Expectation of Privacy in Historical CSLI Records

Under *Katz*, the first question to be answered when a law or action is challenged on the basis that it violates the privacy protections of the Fourth Amendment is whether the complainant has a subjective expectation of privacy in the information to be searched.[457] Whereas the courts have long made the home the heartland of an individual's subjective expectation of privacy against government searches,[458] in recent years the Supreme Court has signaled an increasing willingness to find a subjective expectation of privacy in location records generated by tracking devices.[459]

To establish a reasonable expectation of privacy, one must take "precautions customarily taken by those seeking privacy."[460] For example, in *United States v. Chadwick*,[461] the Supreme Court ruled that placing personal effects in a "double-locked footlocker," was sufficient to manifest an expectation of privacy that the contents would remain free from public examination.[462] Similarly, in *Katz*, the Supreme Court held that one who occupies a telephone booth, shuts the door behind him, and pays to connect his

---

455 *See, e.g.*, Brief for ACLU Found. et al. as Amici Curiae Supporting Appellant at 3, United States v. Davis, 785 F.3d 498 (11th Cir. 2015), 2014 WL 7006394, at *3 [hereinafter Amici Brief] (noting that "law enforcement obtained 67 days of [CSLI] for [Davis's] phone without a warrant").

456 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

457 *Id.*

458 *Id.*

459 *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945 (2012).

460 Rakas v. Illinois, 439 U.S. 128, 152 (1978) (Powell, J., concurring).

461 433 U.S. 1 (1977).

462 *Id.* at 11.

call "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[463]

In order for a cell phone user to assert a valid privacy interest in his CSLI, he must refuse to authorize his service provider's creation and preservation of CSLI records.[464] However, as society becomes more heavily reliant on the utility of the cell phone, the practicality of such a proposition becomes less tenable. Strict application of such a rule would require one to cut himself off from the most prevalent and effective communication device available.[465] Surely the Fourth Amendment does not require one to become a recluse in order to enjoy its protections.[466]

Moreover, strict application of the *Katz* jurisprudence dictates that as societal awareness of the existence and operation of CSLI increases, one day it will become impossible to successfully claim a subjective expectation of privacy in it. Ultimately, it would become impossible for one to assert his subjective expectation of privacy in even the most private of affairs simply because he carried a device so universal[467] "that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[468]

However, even if such an absurd outcome were to one day obtain, that day has likely not yet arrived. A 2014 poll revealed that 82% of adults "'feel as though the details of their physical location gathered over a period of time' is 'very sensitive' or 'somewhat sensitive.'"[469] Similarly, a 2008 study found that 73% of cell phone users surveyed supported "a law that required the police to convince a judge that a crime has been committed before obtaining [historical]

---

463 *Katz*, 389 U.S. at 352.

464 *See* United States v. Davis, 785 F.3d 498, 536 (11th Cir. 2015). Wooden adherence to the third-party doctrine dictates that cell phone users cannot maintain a privacy interest in their CSLI because service contracts and privacy policies typically warn of CSLI collection and possible disclosure to law enforcement. *Id.*

465 *See id.* at 525 (Rosenbaum, J., concurring) ("In our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life.").

466 *See* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (identifying the issue that "unless a person is willing to forego use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance").

467 Riley v. California, 134 S. Ct. 2473, 2490 (2014). Chief Justice Roberts noted that:

> Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.

Id.

468 *Id.*

469 *Davis*, 785 F.3d at 538 (quoting MARY MADDEN, PEW RESEARCH CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 34 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf).

location information from the cell phone company."[470] Nearly as many respondents supported a statute requiring law enforcement to provide notice to a cell phone user whose CSLI it sought from the service provider.[471] Moreover, as the government admitted in its closing argument in the trial that precipitated the Eleventh Circuit's *Davis* decision, Davis and his co-defendants "probably *had no idea* that by bringing their cell phones with them to these robberies, they were allowing [their cellular service provider] and now all of you to follow their movements on the days and at the times of the robberies."[472]

Accordingly, courts have, at times, accepted that the average cell phone user maintains a subjective interest of privacy in CSLI.[473] However, the protections of the Fourth Amendment are not effectuated unless both prongs of the *Katz* reasonable expectation of privacy test are satisfied.[474] Not only must the complainant have a subjective expectation of privacy, society must also be willing to recognize his expectation as objectively reasonable.[475]

2. Society Is Prepared to Recognize this Expectation as Objectively Reasonable

Under *Katz*, the second question to be answered by Fourth Amendment analysis is whether the subjective expectation of privacy established by a complainant is one society is willing to recognize as objectively reasonable.[476] Whether one's claim of privacy is objectively reasonable is determined in light of all the circumstances.[477] The Court has recognized that no one factor is determinative,[478] and that "[r]easonableness is determined by considering such factors as the precautions a person takes to maintain his privacy, the way he

---

470 JENNIFER KING & CHRIS JAY HOOFNAGLE, RESEARCH REPORT: A SUPERMAJORITY OF CALIFORNIANS SUPPORTS LIMITS ON LAW ENFORCEMENT ACCESS TO CELL PHONE LOCATION INFORMATION 16 (2008), https://www.ftc.gov/sites/default/files/documents/public_comments/beyond-voice-mapping-mobile-marketplace-534331-00005/534331-00005.pdf.

471 *Id.* (finding that 72% of respondents voted to receive notice when police sought the CSLI).

472 United States v. Davis, 754 F.3d 1205, 1217 (11th Cir.) (emphasis added), *vacated*, 573 F. App'x 925 (11th Cir. 2014), *aff'd on reh'g*, 785 F.3d 498 (11th Cir. 2015) (admitting that Davis "*could not have known*" his cell phone "was tracking his every movement").

473 *See, e.g.*, *Davis*, 785 F.3d at 539.

474 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

475 *Id.*

476 *Id.*

477 Rakas v. Illinois, 439 U.S. 128, 152 (1978) ("The ultimate question, therefore, is whether one's claim to privacy from government intrusion is reasonable in light of all the surrounding circumstances.").

478 *Id.*

uses a location, the history of the Fourth Amendment, the property interests involved, and society's recognition of customary behavior."[479]

Bearing qualities analogous to the modern CSLI-producing cell phone is yesterday's public telephone. As was true of a public telephone booth in the *Katz* era, today's cell phones are a "vital means of communications for many Americans,"[480] but to a far greater degree.[481] Whereas one previously had to locate a pay phone on a street corner, in a commercial establishment, or mass transit hub, now more than 90% of American adults own a cell phone.[482] Cell phones have become so pervasive that, as Chief Justice Roberts quipped, an alien might mistake it for an appendage,[483] and the voice and text conversations they facilitate are so inescapable that some may consider them to be "essential means or necessary instruments for self-expression, even self-identification."[484] Even today's average American youth is so attached to her cell phone that she sends upwards of 60 text messages per day.[485] The grip cell phones have on Americans of all ages and walks of life seemingly tightens daily.

Katz admittedly protected the content of a telephone call, not Katz's presence within the booth.[486] However, the Court protected the content of Katz's phone calls by explaining that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[487] Courts also should protect CSLI from warrantless government intrusion because to read the Constitution more narrowly is to ignore the vital role that cell phones play in modern life.

Moreover, although law enforcement interception of private conversation is unquestionably intrusive, such interception often captures little more than that—just talk. People say things they never intend to follow through

---

479 United States v. Smith, 621 F.2d 483, 487 (2d Cir. 1980) (citing *Rakas*, 439 U.S. at 143 n.12).

480 *See* THE FOURTH AMENDMENT, *supra* note 427, at 231.

481 *See* Michael Isikoff, *The Snitch in Your Pocket: Law Enforcement Is Tracking Americans' Cell Phones in Real Time—Without the Benefit of a Warrant*, NEWSWEEK, Mar. 1, 2010, at 40 (noting that, as of 2010, Americans owned 277 million cells phones); Christian Berg, *Pay Phones Reached Their Peak in "95*, THE MORNING CALL (Mar. 18, 2001), http://articles.mcall.com/2001-03-18/news/3340885_1_telephone-company-office-pay-bell-telephone (estimating that, at their height, there were 2.6 million pay phones in the United States).

482 *Mobile Technology Fact Sheet*, PEW RESEARCH CTR., http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited Nov. 5, 2015).

483 Riley v. California, 134 S. Ct. 2473, 2484 (2014).

484 City of Ontario v. Quon, 560 U.S. 746, 760 (2010).

485 United States v. Davis, 785 F.3d 498, 542 (11th Cir. 2015) (citing AMANDA LENHART, PEW RESEARCH CTR., TEENS, SMARTPHONES & TEXTING 2 (2012), http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_Teens_Smartphones_and_ Texting.pdf).

486 *See* Katz v. United States, 389 U.S. 347, 352 (1967) ("But what [Katz] sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear.").

487 *Id.*

with, intentionally bluff, boast, and outright lie. What does not lie is the CSLI created by your cell phone. As the prosecution emphasized in *Davis*, it places you in specific locations at specific times.[488] Were CSLI not demonstrative of the actual steps you took rather than those you merely said you would in the future, there is little doubt that government would not utilize CSLI as a key component of its prosecution strategy in many circumstantial cases.

Further, the indiscriminate nature of CSLI reveals one's movements and actions irrespective of how sensitive or private. As Justice Sotomayor noted in her *Jones* concurrence—the 2012 Supreme Court case striking down warrantless GPS tracking—"I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."[489]

CSLI is unquestionably more invasive than browsing history. Whereas one's browsing history may provide insight into desires, inclinations, and possibly physical activities, CSLI is far more telling. It reveals the next level of interest: the decision to actually travel to a given location, ostensibly to observe, participate in, experience, or otherwise satisfy such curiosities.[490] The D.C. Circuit observed the following:

> [One] who knows all of another's travels can deduce whether he is a weekly churchgoer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about [him], but all such facts.[491]

If Justice Sotomayor is correct, that society would be unwilling to accept warrantless access to simple internet history, there is little doubt that society would be significantly less willing to accept the modern practice of law enforcement successfully forcing millions of annual warrantless disclosures of one's CSLI records,[492] particularly for extended periods of time.[493] Further, an

---

488 *See Riley*, 134 S. Ct. at 2490; *Davis*, 785 F.3d at 541 ("Mr. Davis's phone [was] literally right up against the America Gas Station immediately preceding and after [the] robbery occurred." (citing Transcript of Record at 61, *Davis*, 785 F.3d 498 (No. 285))). Davis's cell phone was present "literally . . . right next door to the Walgreen's just before and just after the store was robbed." *Davis*, 785 F.3d at 541.

489 United States v. Jones, 132 S. Ct. 945, 957 (2012).

490 *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

491 *Id.*

492 *See Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on Constitution, Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 2 (2010) (statement of Hon. Stephen W. Smith, U.S. Mag. J.) ("A reasonable estimate is that the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000.").

additional contingent of five *Jones* Justices subscribed to the notion that persons maintain a reasonable expectation of privacy in records of their physical movements obtained by the accumulation of tracking information.[494] Most recently, in the unanimous *Riley* decision—the 2014 Supreme Court decision prohibiting warrantless examination of an arrestee's cell phone pursuant to a lawful arrest—the Supreme Court unequivocally expressed a distinct respect for the sanctity of personal information contained on one's cell phone.[495]

Taken together, *Jones* and *Riley* clearly signal an increasingly potent and controlling sentiment on the Supreme Court that obtaining digitally conveyed tracking information is a violation of privacy under the Fourth Amendment.[496] Moreover, given that over five-eighths of adults deem extensive records of their physical movements to be sensitive or extremely sensitive,[497] and nearly three-quarters of individuals favor police being forced to obtain a warrant before accessing CSLI,[498] the assertion of privacy in historical CSLI is generally held by society to be objectively reasonable.

Accordingly, the average American cell phone user maintains a subjective expectation of privacy that society recognizes as objectively reasonable, satisfying the *Katz* reasonable expectation of privacy test. However, even if a person maintains a reasonable expectation of privacy, Supreme Court precedent holds that the attendant protections of the Fourth Amendment are destroyed if he voluntarily conveys that information to a third-party.[499] The following subsection discusses the third-party exception doctrine and argues that this exception to the Fourth Amendment's warrant requirement does not apply to CSLI.

3. CSLI Does Not Succumb to the Third-Party Exception Doctrine

The Fourth Amendment does not protect the information one knowingly exposes to a third-party, regardless of whether the location of exposure is itself private.[500] Many courts rely largely on this concept to validate

---

493 *See, e.g.*, *Jones*, 132 S. Ct. at 949 (invalidating 28 days of warrantless tracking of the defendant); Amici Brief, *supra* note 455, at 3.

494 *Jones*, 132 S. Ct. at 954, 957.

495 *See* Riley v. California, 134 S. Ct. 2473, 2494–95 (2014) (holding unanimously that "[m]odern cell phones . . . hold for many Americans the 'privacies of life'" (quoting Boyd v. United States, 116 U.S. 616, 630 (1886))).

496 *Id.* at 2495; *Jones*, 132 S. Ct. at 949.

497 United States v. Davis, 785 F.3d 498, 538 (11th Cir. 2015) (quoting MADDEN, *supra* note 469, at 34).

498 KING & HOOFNAGLE, *supra* note 470.

499 *See* Katz v. United States, 389 U.S. 347, 351 (1967).

500 *Id.*

the government's acquisition of historical CSLI, as did the Fifth Circuit in *Historical*[501] and the Eleventh Circuit in its en banc *Davis*[502] decision. The conclusion that exposure of CSLI to third-parties is voluntary is often rooted in the notions that (1) no one is forced to buy, carry, or use a cell phone,[503] and (2) cell service contracts typically include notice provisions making users aware that use of that company's cell service creates CSLI that is stored.[504] Both assumptions, when critically examined, prove to be unpersuasive as a basis to withhold the protections of the Fourth Amendment from CSLI.

First, as the Supreme Court noted in *Riley*, cell phones are now "a pervasive and insistent part of daily life."[505] If people wish to reasonably participate in society, they must "reveal a great deal of information about themselves to third-parties in the course of carrying out [even the most] mundane tasks."[506] For example, cell phone users convey such commonplace information as the phone numbers that they dial or text to their cell phone service 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.[507] Accordingly, as Judge Rosenbaum noted in her *Davis* concurrence, "unless a person is willing to 'live off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate personal life."[508]

Thus, although no one is literally forced by another to use a cell phone, its use has become practically unavoidable. Not only are cell phones ubiquitous, but for a growing segment of the population they are essential to

---

501 *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013) (concluding that "a user voluntarily conveys [CSLI] when he places a call, even though he does not directly inform his service provider of the location of the nearest cell phone tower"). Such disclosure is voluntary because

> a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call.

Id.

502 *Davis*, 785 F.3d 498.

503 *See id.* at 520 (Pryor, J., concurring) ("If a telephone caller does not want to reveal dialed numbers to the telephone company, he has another option: don't place a call. If a cell phone user does not want to reveal his location to a cellular carrier, he also has another option: turn off the cell phone.").

504 *In re Historical*, 724 F.3d at 613.

505 Riley v. California, 134 S. Ct. 2473, 2484 (2014).

506 United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

507 *Id.*

508 *Davis*, 785 F.3d at 525 (Rosenbaum, J., concurring).

cultural and economic participation.[509] Thus, full participation in modern society almost requires disclosure of certain digital information to third-parties.[510] As the Fourth Circuit noted in *Graham*, "[p]eople cannot be deemed to have volunteered to forfeit expectations of privacy [in CSLI] by simply seeking active participation in society through use of their cell phones."[511] CSLI cannot, therefore, be voluntarily conveyed in any real sense, as the cell phones that create it are virtually mandatory to today's existence. Any conclusion to the contrary fails to appreciate the cell phone's role as a centerpiece of contemporary life in this country.

Furthermore, the foundational third-party doctrine case relevant to CSLI was decided nearly 40 years ago in *Smith v. Maryland*[512] in the context of numbers manually dialed on a landline telephone. Society has significantly changed since *Smith*, however, as the degree with which the average citizen exposes information has increased in the last 40 years "by orders of magnitude."[513] Nevertheless, for nearly four decades, the Supreme Court has ignored the march of technology: if one uses a ubiquitous and vital tool like the cell phone, his Fourth Amendment rights are eliminated simply because the use of that tool is necessarily routed through third-parties.[514]

Today, strict application of the outmoded third-party doctrine renders the protections of the Fourth Amendment and the use of indispensable modern technologies, such as cell phones, mutually exclusive. Justice Marshall foresaw such an outcome in his *Smith* dissent, when he warned that the third-party doctrine forces "a person . . . to forgo use of what for many has become a personal or professional necessity . . . [or] accept the risk of surveillance."[515] Everyday life in today's world, however, is totally integrated with third-party-provided technological services and is nothing short of "a steroidal version of

---

509 United States v. Graham, 796 F.3d 332, 355–56 (4th Cir. 2015), *reh'g en banc granted*, Nos. 12-4659(L), 12-4825, 2015 WL 6531272 (4th Cir. Oct. 28, 2015).

510 *Davis*, 785 F.3d at 522 ("[P]ractical necessities now require individuals to share information about themselves 'with trusted individuals and institutions for limited purposes.'" (quoting STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 8 (2012))).

511 *Graham*, 796 F.3d at 356.

512 442 U.S. 735, 750 (1979).

513 *Davis*, 785 F.3d at 538 (Martin, J., dissenting).

514 *See* Matthew S. Adams, *Update: Eleventh Circuit En Banc Showdown Set for February 24th on Key Constitutional Issue Surrounding Cell Phone Tower Data*, FOX ROTHSCHILD LLP (Jan. 12, 2015), http://ediscoverystage.foxrothschild.com/2015/01/articles/evidence/update-en-banc-showdown-at-the-eleventh-circuit-court-of-appeals-set/ (noting that in its amicus brief AT&T argued that "[n]othing in *Smith* or *Miller* requires that individuals must choose between participating in the new digital world through use of their mobile devices and retaining the Fourth Amendment's protections").

515 *Davis*, 785 F.3d at 525 (Rosenbaum, J., concurring) (quoting *Smith*, 442 U.S. at 750 (Marshall, J., dissenting)).

the problems Justice[] Marshall . . . envisioned" nearly four decades ago.[516] Thus, with the advent of every new technology, the third-party doctrine forces Americans to "surrender more and more of our historically protected Fourth Amendment interests to unreasonable searches and seizures."[517]

Justice Sotomayor recognized this troubling truth when she argued in her *Jones* concurrence that it is therefore likely necessary for the Supreme Court to reconsider the fundamental premise of the third-party doctrine, particularly as manifested in the current digital context, because it "is ill suited to the digital age."[518] As the Fourth Circuit commented in *Graham*, the fact that a third-party indiscriminately records a person's movements over an extended period of time, both in public and in private, must not eliminate her expectation of privacy in her CSLI.[519] "Applying the third-party doctrine in this context would simply permit the government to convert an individual's cell phone into a tracking device by examining the massive bank of location information retained by her service provider, and to do so without probable cause."[520] Similarly, Congress needs to reexamine the wisdom of such provisions of the SCA as § 2703(d), as the SCA has not been significantly revised since it was passed into law in 1986. As the Supreme Court established in *Coolidge v. New Hampshire*,[521] "[i]f times have changed, reducing everyman's scope to do as he pleases in an urban and industrial world, . . . the values served by the Fourth Amendment [are] more, not less, important."[522]

Finally, the fact that cell phone contracts may contain provisions indicating that CSLI will be created and stored does not mean cell phone users actually give their consent to these practices.[523] Not only are cell phone service contracts typically incredibly voluminous,[524] they are pointless to read.[525] They are filled with pages of legal jargon that is meaningless to the average citizen, and are even pointless to read for "expert[s] in contract law," including "the

---

516 *Id.*

517 *Id.* at 532–33.

518 United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

519 United States v. Graham, 796 F.3d 332, 357 (4th Cir. 2015), *reh'g en banc granted*, Nos. 12-4659(L), 12-4825, 2015 WL 6531272 (4th Cir. Oct. 28, 2015).

520 *Id.*

521 403 U.S. 443 (1971).

522 *Davis*, 785 F.3d at 533 (Pryor, J., dissenting) (quoting *Coolidge*, 403 U.S. at 455 (alteration in original)).

523 *See Why Do We Blindly Sign Terms of Service Agreements?*, NPR (Sept. 1, 2014, 4:07 PM), http://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements.

524 *See, e.g.*, *id.* (noting that the 2014 Apple iTunes contract is 55 pages of eight-point font that reaches 30 feet when printed).

525 *See id.*

lawyers that drafted" them.[526] Further prohibiting comprehension of their terms is the fact that user agreements often contain so "many typos" that they appear to have gone unread by the disclosers themselves.[527]

Even if, however, the average cell phone user were able to penetrate the legalese of her cell phone service contract, its language may say nothing of the service provider disclosing her CSLI to third-parties.[528] In *Graham*, for example, the Sprint/Nextel service agreement "only state[d] that Sprint/Nextel *collects* information about the phone's location—not that it discloses this information to the government or anyone else."[529] Thus, if many cell phone contracts do not even mention potential disclosure of CSLI by the service provider to third-parties, and world-renowned contract attorneys cannot discern the intricacies of the content actually appearing in today's user agreements, then there is no way that the average citizen has such ability. Because cell phone users are forced to sign service contracts regardless of the privacy conditions contained therein, and such agreements are either silent on CSLI disclosure or unintelligibly dense to even the most seasoned contract attorney, agreeing to the terms of a cell phone service contract does not constitute anything approaching consent to disclosure of CSLI.

The rigid and decades-old third-party doctrine does not recognize the reality of the 21st century, however. Thus, as Justice Sotomayor appropriately appreciated in *Jones*, it has become abundantly clear that the traditional third-party doctrine is "ill suited" for "the digital age."[530] Individuals, therefore, maintain a subjectively reasonable expectation of privacy that society recognizes as objectively reasonable, notwithstanding the third-party doctrine of the Fourth Amendment.

4. The Needs of Law Enforcement Do Not Justify Warrantless Access to CSLI

Law enforcement officials argue that the balancing of Americans' liberty interest in individual privacy against the government's interest in conducting effective law enforcement dictates that § 2703(d) of the SCA should be upheld.[531] They contend that because § 2703(d) helps conserve

---

526 *Id.*

527 *Id.*

528 United States v. Graham, 796 F.3d 332, 345 (4th Cir. 2015), *reh'g en banc granted*, Nos. 12-4659(L), 12-4825, 2015 WL 6531272 (4th Cir. Oct. 28, 2015).

529 *Id.*

530 United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

531 Government's Petition for Rehearing En Banc at 14–15, United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (No. 12-12928-EE) (contending that striking § 2703(d) would constitute a "substantial burden" that "deprives law-enforcement authorities of an important investigative tool, without yielding any appreciable real-world privacy gains by way of compensation").

investigative resources and "deflect suspicions from the innocent,"[532] easy access to CSLI is extremely valuable during the early stages of criminal investigations before probable cause is cultivated.[533] Not only does acquisition of CSLI under § 2703(d) "come at a negligible cost to privacy," they say, to curtail such an effective investigative tool would constitute a substantial burden on law enforcement.[534] Accordingly, law enforcement officials maintain that courts should continue to accept the constitutionality of § 2703(d)'s reasonable suspicion CSLI warrants.[535]

However, based on the Supreme Court's unanimous ruling in its 2014 *Riley* decision, § 2703(d) of the SCA cannot survive simply because it is helpful to law enforcement.[536] In *Riley*, the Supreme Court held that warrantless searches of arrestees' cell phones are unconstitutional, notwithstanding the reality that the inability to conduct such searches "will have an impact on the ability of law enforcement to combat crime."[537] The Supreme Court also acknowledged that cell phones and the records they create are frequently troves of investigative information for law enforcement.[538] Nevertheless, the *Riley* Court dismissed such contentions by concluding that "[p]rivacy comes at a cost."[539]

The Supreme Court's decision in *Riley* further foreclosed such cost-benefit arguments of law enforcement.[540] The *Riley* decision held that "the [Fourth Amendment's probable cause] warrant requirement is 'an important working part of our machinery of government' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'"[541] Therefore, the Eleventh Circuit's balancing in its *Davis* decision, which held that the constitutionality of a search or seizure hinges on its reasonableness, and that reasonableness is based "on the one hand, [by] the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests,"[542] was squarely rejected by *Riley*.

---

532 *Id.*

533 *Id.*

534 *Id.*

535 *Id.* at 15.

536 *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014).

537 *Id.*

538 *Id.*

539 *Id.*

540 *Id.*

541 *Id.* (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

542 United States v. Davis, 785 F.3d 498, 517 (11th Cir. 2015) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

Additionally, in *Riley*, the Supreme Court raised the practical reality that, even if such balancing were proper, the difficulties imposed on law enforcement by forcing the acquisition of a warrant have largely been assuaged by the ability of police officers in many jurisdictions to quickly obtain warrants via e-mail.[543] Moreover, beyond often being able to obtain warrants in a matter of minutes, commentators have observed that the "[t]he Supreme Court has set the standard for the quality of information [supporting warrants] so low that judges can hardly be expected to uncover baseless requests."[544] Thus, any imposition suffered by police being forced to get a warrant is negligible.

Finally, in *Riley*, the government argued that because co-conspirators can destroy evidence stored on cell phones by remotely wiping the contents of an arrestee's cell phone, an arrest is a sufficiently exigent circumstance to necessitate obfuscation of the warrant requirement.[545] *Riley* addressed and dismissed such arguments as too remote and easily avoidable, particularly because law enforcement can place confiscated cell phones in signal-blocking protective cases.[546] CSLI is yet further removed from exigent circumstances because there is no reasonable basis to believe that cell phone service providers—engaged in the practice of routinely accumulating and storing CSLI to better serve their customers—will erase CSLI records before a warrant can reasonably be obtained.[547] No realistic argument can be made that law enforcement runs the risk of losing valuable CSLI evidence by adhering to the warrant requirement.[548]

Therefore, § 2703(d) of the SCA cannot be justified on the basis that its provision for the acquisition of CSLI upon showing of reasonable suspicion conveniences law enforcement. Expediency is not a basis upon which the Constitution may be discarded, notwithstanding that a more cumbersome process might inhibit the most effective law enforcement techniques.

---

543 *Riley*, 134 S. Ct. at 2493 (noting that in many jurisdictions police officers are able to e-mail warrant applications to judges and receive e-mail responses within 15 minutes (citing Missouri v. McNeely, 133 S. Ct. 1552, 1561–63 (2013))).

544 Ricardo J. Bascuas, *Property and Probable Cause: The Fourth Amendment's Principled Protection of Privacy*, 60 RUTGERS L. REV. 575, 592–93 (2008).

545 *See Riley*, 134 S. Ct. at 2486.

546 *See id.* at 2487 ("[I]f [law enforcement officers] are concerned about encryption or other potential problems, they can . . . place [a phone] in an enclosure that isolates the phone from radio waves. Such devices are commonly called 'Faraday bags' . . . . They are essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use.").

547 *See Davis*, 785 F.3d at 543 ("Nor is cell site data the type of information which would spoil or perish during the short time it takes to get a warrant.").

548 *Id.*

VI. CONCLUSION

Section 2703(d) of the SCA violates the Fourth Amendment because individuals have a legitimate expectation of privacy in CSLI, and thus the government must first obtain a warrant supported by probable cause to access CSLI. First, § 2703(d) stands in opposition to the Founders' intent in drafting and ratifying the Fourth Amendment to protect against the unbridled authority of the government to examine one's private affairs. Second, compelling the production of CSLI is clearly a "search" under the Fourth Amendment, and the plain language of the Fourth Amendment requires law enforcement to first obtain a warrant that is supported by probable cause. Third, individuals typically maintain a subjective expectation of privacy in CSLI that society is willing to recognize as objectively reasonable. Fourth, CSLI does not succumb to the Fourth Amendment's third-party exception doctrine. Fifth, and finally, the needs of law enforcement do not justify warrantless access to CSLI.

The Fourth Amendment fundamentally stands for the proposition that citizens have the "right to be left alone."[549] If the use of a device indispensable to participation in modern society subjects one's every move to warrantless examination by law enforcement, the Fourth Amendment has been utterly annulled. The time is now for the Supreme Court and, more importantly, Congress to recognize that § 2703(d) of the SCA is unconstitutional and in dire need of revision. The very essence of what it means to be a free American demands it.

*Raymond Boyce**

---

[549] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

* J.D., West Virginia University College of Law, 2015; B.A. in Political Science, Virginia Polytechnic Institute and State University, 2009. The Author would like to thank the members of the *West Virginia Law Review*, past and present, for their tireless effort during the drafting and editing process. The Author would additionally like to thank his Note Advisor, Stacy Etheredge, for her research expertise and perpetual positivity and encouragement. The Author would similarly like to thank F. Italia Patti for her research contributions. Finally, the Author wishes to thank his friends and family for their unyielding devotion and understanding, and in particular, Katherine M. Moore, without whose tremendous guidance, emotional support, and loyal friendship, this Note would not exist. All errors or omissions contained herein are the Author's alone.