St. Mary's Law Journal

Volume 47 | Number 3 Article 5

1-1-2016

Ford v. State: Texas Forces a Resolution in the Cell Site Location Information Debate.

Brandon J. Grable

RECENT DEVELOPMENT

FORD V. STATE: TEXAS FORCES A RESOLUTION IN THE CELL SITE LOCATION INFORMATION DEBATE

BRANDON J. GRABLE*

* The author thanks Professor John Schmolesky and Professor Michael Ariens for their selfless guidance over the last three years as the author rigorously researched the constant transformation of this area of law. The author also appreciates the thoughtful and insightful comments from Stephanie Green and Frank Scaglione. He also thanks Dorian Ojemen, Managing Executive Editor, for taking the time and effort to make this Recent Development the best product possible.

INTRODUCTION

All levels of the judiciary[1] are debating whether the government's warrantless collection of cell site location information (CSLI) amounts to a Fourth Amendment violation.[2] On December 16, 2015, the Texas Court of Criminal Appeals boldly weighed in with its unanimous decision in *Ford v. State*.[3] With the *Ford* decision, Texas created a split among states by becoming the first state supreme court to hold the collection of CSLI

1. The United States Supreme Court, however, recently sidestepped two opportunities to settle this issue. *See* Davis v. United States (*Davis III*), 136 S.Ct. 479 (2015) (denying certiorari to address the constitutionality of the collection of cell site data); Riley v. California, 134 S.Ct. 2473, 2489 n.1 (2014) (refusing to address "whether the collection or inspection of aggregated digital information amounts to a search").

2. Thus far, the Third, Fourth, Fifth, Sixth, Seventh, and Eleventh Circuit Courts of Appeal have taken this issue. The Third, Fifth, Sixth, and Eleventh Circuits held the warrantless collection of CSLI did not violate the Fourth Amendment. United States v. Carpenter, Nos. 14-1572, 14-1805, 2016 WL 1445183 (6th Cir. Apr. 13, 2016); United States v. Davis (*Davis II*), 785 F.3d 498, 513 (11th Cir.) (en banc), *cert denied*, 136 S.Ct. 479 (2015); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013); *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't (*In re* Application (Third Circuit)), 620 F.3d 304, 313 (3d Cir. 2010). The Seventh Circuit refused to "take sides" after finding the issue was waived. United States v. Daniels, 803 F.3d 335, 351 (7th Cir. 2015). The Fourth Circuit remains undecided but under different circumstances. The court initially held an opposite view of its sister courts, but an en banc rehearing was quickly granted. United States v. Graham, 796 F.3d 332, 360–61 (4th Cir.), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015). This situation echoes the Eleventh Circuit. United States v. Davis (*Davis I*), 754 F.3d 1205, 1217 (11th Cir.) (holding initially that CSLI collection required a warrant but was later vacated and overruled by the en banc panel), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014) (en banc), *cert. denied*, 136 S.Ct. 479 (2015). A few state supreme courts have decided this issue. Florida, Massachusetts, and New Jersey all held CSLI collection requires a warrant. Tracey v. State, 152 So.3d 504, 526 (Fla. 2014); Commonwealth v. Augustine, 4 N.E.3d 846, 865–66 (Mass. 2014); State v. Earls, 70 A.3d 630, 644 (N.J. 2013).

3. Ford v. State (*Ford II*), 477 S.W.3d 321 (Tex. Crim. App. 2015). Judge Yeary did not participate in the decision. *Id.* at 335.

without a warrant does not necessarily violate the Fourth Amendment.[4]

This Recent Development seeks to analyze the *Ford* decision in light of the current national landscape addressing this issue. Part I briefly explains CSLI. Part II provides facts of the *Ford* case and analyzes how the court arrived at its conclusion. Part III suggests the *Ford* decision may be incorrectly decided and probably demands a narrow application, but the decision is nonetheless necessary to push the Supreme Court to finally close the widened chasm between society, courts, and law enforcement.

PART I: UNDERSTANDING THE IMPORTANCE OF CSLI

A. *What Is CSLI?*

A subscriber's mobile device generates CSLI each time it registers with a service provider's (AT&T or Sprint, e.g.) cell site.[5] "[T]he service provider automatically captures and retains certain information about the communication, including identification of the specific cell site and sector through which the connection is made."[6] Cell sites have a limited reach, so service providers wrapped the country in a "quilt of cell [sites] . . . stitched together to provide seamless coverage."[7] This coverage grants a subscriber's device not only the privilege of constant connectivity but also continuous CSLI.

The current telecommunications network is comprised of around 300,000 cell sites.[8] Cell sites are strategically "placed at various locations . . . [and] arranged in sectors facing multiple directions to better facilitate radio transmissions."[9] The average coverage radius is "one to

4. *Id.* at 330.

5. Cell sites are the antennae responsible for receiving and transmitting data to and from cell phones. *See Explaining Reception*, CELLRECEPTION, http://www.cellreception.com/guides/page1.html (last visited Mar. 14, 2016) ("Cell phones are essentially 'radios.' They communicate to the world by transmitting and receiving voice through cell towers setup throughout the area."). Cell sites are sometimes referred to as antennae, base stations, or towers. FCC, HUMAN EXPOSURE TO RADIO FREQUENCY FIELDS: GUIDELINES FOR CELLULAR AND PCS SITES 1 (2015), http://www.fcc.gov/cgb/consumerfacts/rfexposure.pdf.

6. *Graham*, 796 F.3d at 343.

7. Sprint Spectrum LP v. Jefferson Cty., 968 F.Supp. 1457, 1460 (N.D. Ala. 1997).

8. *Annual Wireless Industry Survey*, CTIA-WIRELESS ASS'N, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last visited Mar. 14, 2016). To put this in perspective, the United States has a total area of 3.79 million square miles. *State Area Measurements and Internal Point Coordinates*, U.S. CENSUS BUREAU, https://www.census.gov/geo/reference/state-area.html (last updated Dec. 5, 2012). Assuming cell sites were evenly placed throughout the country, each cell site would account for twelve to thirteen square miles.

9. *Graham*, 796 F.3d at 343.

one-and-a-half miles . . . . [, but] the density of cell towers in an urban area . . . would make the coverage of any given tower smaller."[10]

B. *Why Is CSLI Useful to Law Enforcement?*

CSLI allows law enforcement to "interpolate the path the cell phone, and the person carrying the phone, travelled during a given time period."[11] There are more mobile device subscriptions in this country than there are people.[12] So, in essence, CSLI allows law enforcement to track every step that every person has ever taken with a cell phone.[13] One appellate judge, with much concern, acknowledged "any one of us can be tracked from afar regardless of whether or not we are actively using our phones. Even just sitting at home alone, your phone may be relaying data, including your location data."[14]

Congress appeared to anticipate these concerns long before CSLI even became the issue it is today. For instance, the investigative significance of location information was always known. A 1985 report to Congress found CSLI to be of "great interest to investigative authorities . . . [because] determining the location of parties . . . [is] valuable at any stage of an investigation."[15] But at that time, "no traditional technique[] for obtaining" CSLI existed.[16]

Fears were probably delayed or unrealized because CSLI was not reliable in 1985. Precise locations could not be ascertained from the few cell sites in existence.[17] But the government was well aware that as cell

10. *Davis II*, 785 F.3d 498, 503 (11th Cir.) (en banc), *cert denied*, 136 S.Ct. 479 (2015).

11. *Graham*, 796 F.3d at 343.

12. An annual wireless survey, last conducted in December 2014, reported 355.4 million wireless subscriptions in the United States. *Annual Wireless Industry Survey*, *supra* note 8. The Census Bureau estimates the current United States population to be over 323 million people. *U.S. and World Population Clock*, U.S. CENSUS BUREAU, http://www.census.gov/popclock (last visited Mar. 14, 2016).

13. "We cannot reject the hypothesis that CSLI may, under certain circumstances, be used to approximate the past location of a person. If it can be used to allow the inference of present, or even future, location, in this respect CSLI may resemble a tracking device which provides information as to the actual whereabouts of the subject." *In re* Application (Third Circuit), 620 F.3d 304, 312 (3d Cir. 2010).

14. *Graham*, 796 F.3d at 378 (Thacker, J., concurring).

15. OFFICE OF TECH. ASSESSMENT, ELECTRONIC SURVEILLANCE & CIVIL LIBERTIES 42 (1985), http://www.justice.gov/sites/default/files/jmd/legacy/2013/10/15/fgit-1985.pdf. The purpose of the report was to "present new or changed opportunities for and vulnerabilities to electronic surveillance" since "[n]ew technologies . . . have outstripped the existing statutory framework" used to balance "civil liberty versus law enforcement or investigative interests." *Id.* at Forward.

16. *Id.* at 42.

17. *Id.* at 39.

phones became "more popular, cell sizes [would] be reduced allowing more precise tracking."[18] This assessment was correct. In today's society, CSLI can be more accurate than global position systems (GPS) data—depending on the number of cell sites in a given data set and the sophistication of the cell site technology.[19]

C. *How Does Law Enforcement Obtain CSLI?*

In 1986, the Stored Communications Act (SCA) was enacted.[20] In its current form, the SCA states, "A provider of electronic communication service . . . shall disclose to a governmental entity the . . . local and long distance telephone connection records . . . [of] a subscriber to or customer of such service . . . [with a] court order . . . [issued upon] specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . or the records or other information sought, are relevant and material to an ongoing criminal investigation."[21] A court order under this process is referred to as a 2703(d) order.[22] A 2703(d) order possesses a lighter burden than probable cause[23] and, for that reason, is the method of choice by investigators.[24]

---

18. *Id.*

19. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 712 (2011) (acknowledging when multiple sources are available for triangulation, the location area could be significantly reduced achieving GPS-like accuracy); *see also ECPA Reform and The Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 29–30 (2010) (statement of Matt Blaze, Professor, University of Pennsylvania) (attributing advancement in cell site technology as one reason for GPS being comparable to cell site data); *id.* at 40–41 (statement of Michael Amarosa, Vice President, TruePosition, Inc.) (noting GPS could be less reliable than cell site data because satellite signals are affected when the cell phone is indoors). Precision also "depends on how close together the cell towers are" at any given point in time. Freiwald, *supra*, at 710.

20. The SCA is contained in Title II of the Electronic Communications Privacy Act of 1986. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1860 (codified as amended at 18 U.S.C. §§ 2701–2712 (2012)).

21. 18 U.S.C. § 2703(c)–(d) (2012).

22. This is because a 2703(d) order is promulgated under 18 U.S.C. § 2703(d) (2012).

23. *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 606 (5th Cir. 2013) ("The 'specific and articulable facts' standard is a lesser showing than the probable cause standard that is required by the Fourth Amendment to obtain a warrant."); *In re* Application (Third Circuit), 620 F.3d 304, 313 (3d Cir. 2010) (noting the standard required for a 2703(d) order "is a lesser one than probable cause").

24. The Department of Justice advises "2703(d) orders are an appropriate tool to compel a provider to collect cell phone location information." ELEC. SURVEILLANCE UNIT, U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 44–45 (2005), http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf [hereinafter ELECTRONIC SURVEILLANCE MANUAL]. *See also* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC

D. *The Rise of the 2703(d) Order in the Collection of CSLI*

The SCA provides for numerous methods of collection. Section 2703(c)(1) allows law enforcement to obtain records through a warrant, 2703(d) order, or customer consent.[25] These varying methods sparked the first notable issue addressed on the federal appellate level: Whether law enforcement can seek CSLI under a 2703(d) order rather than a warrant.

In 2010, the government appealed a magistrate's decision rejecting the use of a 2703(d) order to obtain CSLI.[26] The magistrate rejected the request for two reasons.[27] First, CSLI fell outside the scope of the SCA and, therefore, Section 2703(d) was inapplicable.[28] Second, a warrant should be required to ease privacy concerns since CSLI "encroach[es] upon . . . citizens' reasonable expectations of privacy regarding their physical movements and locations."[29]

The reviewing court disagreed, finding "legislative history does not show that Congress intended to exclude CSLI."[30] Under this position, CSLI can be collected using a 2703(d) order.[31] And since the SCA allows for multiple methods of collection, magistrates do "not have 'arbitrary' discretion to require a warrant."[32]

While this 2010 case emboldened the government's use of 2703(d) orders to obtain CSLI, the technique faces growing scrutiny. The complexity is furthered by a lack of information available to the public. For instance, society is unaware how long this method has been used[33]—

EVIDENCE IN CRIMINAL INVESTIGATIONS 160 (2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf ("In most districts, investigators may obtain prospective cell-site information through [2703(d) orders].").

25. 18 U.S.C. § 2703(c)(1) (2012).

26. *In re Application (Third Circuit)*, 620 F.3d at 304.

27. *Id.* at 305.

28. *Id.* at 308.

29. *Id.* at 312.

30. *Id.* at 315.

31. *Id.* at 319.

32. *Id.* at 316.

33. The first reported case was in 2005, but the practices appear to have been in place before. *See In re* Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 384 F.Supp.2d 562, 566 (E.D.N.Y. 2005) (denying a 2703(d) application seeking CSLI because there was no "case law directly on point" but only confusion in other jurisdictions as to whether law enforcement could obtain such data under "the relaxed standard set forth in 18 U.S.C. § 2703, or instead requires adherence to the more exacting standard of probable cause"). Interestingly, media reports from the 1990s indicate law enforcement obtaining CSLI, but it is unclear whether it was through the use of a warrant or some other practice. *See generally* Anemona Hartocollis, *When the Trill of a Cellphone Brings the Clang of Prison Doors*, N.Y. TIMES (July 16, 2007), http://www.nytimes.com/2007/07/16/nyregion/16cell.html?_r=0 (examining various instances when cell site information was used in court

or how many requests for CSLI have been made.[34] The recent *Ford* decision highlights the issues surrounding the use of these orders and vaguely attempts to find a balance between individual privacy and law enforcement needs. As addressed below, *Ford* seems to create more confusion, but does it create enough to require the high Court to put this issue to rest?

PART II: EVALUATING THE IMPACT OF *FORD V. STATE*

A. *Facts*

On New Year's Eve in 2008, appellant attended a New Year's Eve party with two friends and his ex-girlfriend, the decedent.[35] Decedent and appellant ended their relationship a few months prior, but they shared the same social circles.[36] At one point during the party, appellant "became slightly irritated" when his relationship with decedent was brought up during a game the four were playing.[37] One friend later testified, "I made a fuss . . . I think it rubbed [appellant] the wrong way."[38] Appellant left before midnight, texting to the other friend the party was "[n]o longer fun."[39] Appellant did not respond to any other text messages or phone calls that night.[40]

Decedent and two friends "left the party around 12:45 a.m."[41] Appellant left his cooler of beer at the party, so his two friends attempted to drop it off with him.[42] When they drove by his home, they did not see his white Chevy Tahoe, so they left.[43] One of them texted appellant around 1:00 a.m., letting him know they had his cooler and would talk to

---

both in defense of and against the accused). *But see* Pullin v. State, 534 S.E.2d 69, 71 (Ga. 2000) (acknowledging "search warrants obtained in this state us[ed] cellular telephone historical data as the basis for probable cause" on numerous occasions).

34. *See* Press Release, Sen. Edward Markey, For Second Year in a Row, Markey Investigation Reveals More Than One Million Requests by Law Enforcement for Americans Mobile Phone Data (Dec. 9, 2013), http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data (showing service providers handle at least a million requests each year for CSLI and it could be more since not all service providers responded to the survey).

35. *Ford II*, 477 S.W.3d 321, 322–23 (Tex. Crim. App. 2015).

36. *Id.*

37. *Id.* at 323.

38. *Id.* (alteration in original).

39. *Id.*

40. *Id.* at 323–24.

41. *Id.* at 323.

42. *Id.*

43. *Id.*

him in the morning.[44]

Morning came and decedent was supposed to meet with her parents.[45] When she failed to show and did not respond to phone calls, her parents drove to her condominium.[46] Within minutes, they found their daughter deceased, with a "white towel with blood . . . draped over her face."[47] There were no signs of forced entry, and only the decedent's two dogs were missing.[48]

Police contacted appellant, who "volunteered to give a statement."[49] He told police he arrived at home from the party around 11:30 p.m. and went to sleep shortly after.[50] He mentioned his phone "had been in his possession the entire night . . . . [and] nobody had used his phone or driven his white Chevy Tahoe except him."[51]

Detectives grew suspicious of this alibi after obtaining video footage from a bank near decedent's condominium.[52] The video showed a white SUV driving by decedent's complex a number of times.[53] Around 11:42 p.m., a person wearing "clothing consistent with what appellant had worn out that evening" was recorded walking into decedent's complex.[54] The video showed Decedent arriving home at 1:00 a.m.[55] Around 2:00 a.m., the person who entered at 11:42 p.m. was recorded walking out of the condominium.[56] A few minutes later, a white SUV drove by.[57] The SUV made one more visit to the decedent's complex from 3:12 a.m. to 3:16 a.m., but this time "with its lights off."[58]

On January 14, 2009, law enforcement filed a 2703(d) order seeking four days of CSLI.[59] Law enforcement focused on fourteen "events"[60]

---

44. *Id.* at 323–24.

45. *Ford II*, 477 S.W.3d 321, 324 (Tex. Crim. App. 2015).

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.* at 324–25.

55. *Ford II*, 477 S.W.3d 321, 324–25 (Tex. Crim. App. 2015).

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.* The court acknowledged the application was also filed pursuant to Article 18.21, Section 5(a), of the Texas Code of Criminal Procedure. *Id.* Section 5(a) is outside the scope of this discussion since the court also invoked the SCA. *Id.*

60. The state's expert referred to tower pings as "events," but it appears an event in this case could contain more than one data point. *See id.* at 327 ("Event five showed [a phone call to

spanning from 8:10 p.m., December 31, 2008, to 9:43 a.m., January 1, 2009.[61] "Twelve of these were texts or phone calls to or from" one of appellant's friends from the party; another was "a passive-use data upload or download from the internet[;] and one was an active call to voicemail."[62]

The state's expert testified that when appellant received a call at 11:45 p.m., after leaving the party, and the 1:00 a.m. text regarding his beer cooler, the appellant's phone was located in the sector covering decedent's residence.[63] The expert noted the impossibility for appellant to be at home, since the cell sites "did not have a line of sight" to his residence.[64] The data point generated by the passive upload or download pinged off of a cell site near a dam at 1:32 a.m.[65] This was "significant because that is where police recovered the body" of one of decedent's dogs.[66]

B. *Procedural History*

In February 2012, appellant was found guilty of murder and sentenced to forty years confinement.[67] In his appeal, appellant challenged the admission of CSLI, arguing it was an unreasonable search.[68] The court of appeals affirmed the conviction in August 2014, "rel[ying] upon the third-party record doctrine, explaining that appellant had voluntarily disclosed the location of his cell phone through cell-site data to a third party when he obtained a cell phone, chose AT&T as a service provider, and availed himself of the benefits of AT&T's network."[69] The dissent argued appellant retained a reasonable expectation of privacy and "did not voluntarily surrender his reasonable expectation of privacy in his physical location and movements simply by using his cell phone"; therefore, the

---

appellant] at 11:45 p.m. and a text to [appellant] at 1:19 a.m.). Courts tend to focus on each data point separately. *See* United States v. Graham, 796 F.3d 332, 350 (4th Cir.) (referring to CSLI records as "data points"), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015); *Davis II*, 785 F.3d 498, 533 (11th Cir.) (en banc) (Martin, J., dissenting) (identifying CSLI records as containing "data points"), *cert denied*, 136 S.Ct. 479 (2015).

61. *Ford II*, 477 S.W.3d at 326–27.

62. *Id.* at 326.

63. *Id.* at 327.

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.* at 328 (citing Ford v. State (*Ford I*), 444 S.W.3d 171, 190 (Tex. App.—San Antonio 2014, pet granted)).

state should have obtained a warrant.[70]

The issue taken by the Texas Court of Criminal Appeals was whether "the State's warrantless acquisition of four days[']' worth of [CSLI] recorded by" appellant's service provider violated appellant's Fourth Amendment rights.[71] On December 16, 2015, the court determined there was no violation and affirmed the conviction.[72]

C. *Analysis*

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[73] Fourth Amendment claims must be based on either a "trespass theory of search" or a "privacy theory of search."[74]

Under the privacy theory, the appellant must show "(1) he has a subjective expectation of privacy in the place or object searched, and (2) society is prepared to recognize that expectation as 'reasonable' or 'legitimate.'"[75] To define a "legitimate" expectation of privacy, the court cited to *Rakas v. Illinois*.[76] "Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment.... [O]ne who owns or lawfully possess or controls property will in all likelihood have a legitimate expectation of privacy...."[77] Thus, since appellant possessed and controlled his phone and the contents therein, his expectation of privacy for the phone and its contents is legitimate.[78]

Logically, the court then questioned whether this same legitimacy exists in CSLI, which are not contents possessed or owned by the appellant. "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party...."[79] This theory is rooted under the Third-Party Doctrine.[80] The Third-Party Doctrine was recognized by the

70. *Id.* (citing *Ford I*, 444 S.W.3d at 202–03 (Chapa, J., dissenting)).

71. *Ford II*, 477 S.W.3d 321, 322 (Tex. Crim. App. 2015). The court determined a second issue involving a Texas constitutional claim was improvidently granted after determining the issue was not raised before the trial court. *Id.*

72. *Id.* at 335.

73. U.S. CONST. amend. IV.

74. *Ford II*, 477 S.W.3d at 328 (citing United States v. Jones, 132 S.Ct. 945, 949–50 (2012)).

75. *Id.* (citing State v. Granville, 423 S.W.3d 399, 405 (Tex. Crim. App. 2014)).

76. Rakas v. Illinois, 439 U.S. 128 (1978).

77. *Id.* at 143 n.12.

78. *Ford II*, 477 S.W.3d at 328–29.

79. *Id.* at 329.

80. The Third-Party Doctrine commonly refers to Supreme Court decisions in *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979).

Supreme Court, first in *United States v. Miller*[81] and then in *Smith v. Maryland*.[82]

1. United States v. Miller

The 1976 *Miller* decision originated from an investigation into a warehouse fire where police discovered "175-gallons of nontax-paid whiskey."[83] The investigation revealed Miller may have committed other crimes, including tax fraud.[84] Through the course of the investigation, law enforcement obtained Miller's bank transaction records with defective subpoenas.[85] When deciding the legitimacy of the subpoenas, the Court held Miller did not have a reasonable expectation of privacy in the bank records because the documents "contain[ed] only information [he] voluntarily conveyed" to the banks.[86] The Court applied this same standard to telephone numbers three years later.

2. Smith v. Maryland

In 1979, the Court in *Smith* considered for the first time whether the use of a pen register[87] without a warrant amounted to a Fourth Amendment search.[88] Applying the two-pronged test from *Katz v. United States*,[89] the Court found that Smith did not have any "actual expectation of privacy in the phone numbers he dialed, and even if he did, his expectation was not 'legitimate.'"[90] Society could not recognize Smith's expectation of privacy as reasonable because in 1979, "[a]ll telephone users realize[d] that they must 'convey' phone numbers to the telephone company."[91] As in *Miller*,

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

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

83. *Miller*, 425 U.S. at 437.

84. *Id.* at 436.

85. *Id.* at 437–39.

86. *Id.* at 442.

87. The Court defined pen register as a "mechanical device that records the numbers dialed . . . It does not overhear oral communications and does not indicate whether calls are actually completed.'" *Smith*, 442 U.S. at 736 (quoting United States v. New York Tel. Co., 434 U.S. 159, 161 n.1 (1977)).

88. *Id.*

89. Katz v. United States, 389 U.S. 347 (1967). The standard recognized by the *Miller* Court was from Justice Harlan's concurrence, where he defined the reasonable expectation test as (1) whether the individual "exhibited an actual (subjective) expectation of privacy," and (2) whether society is prepared to recognize that expectation as reasonable. *Id.* at 361 (Harlan, J., concurring).

90. *Smith*, 442 U.S. at 745. The focus was on the numbers dialed, and because the pen register could not hear sound, Smith could only argue he had a reasonable expectation of privacy in the numbers he dialed. *Id.* at 742.

91. *Id.*

the Court considered the information (dialing of a number) to be voluntarily conveyed to a third party (the phone company), thus waiving any reasonable expectation of privacy.[92]

The Texas court relied on Professor Wayne LaFave to briefly explain *Miller* and *Smith*:

> [T]he critical fact in both *Miller* and *Smith* was that the information was given to a third party for that party's use; in both cases, this information had to be disclosed for the telephone company or bank to provide the requested service.[93]

3. Federal Circuit Split

The Texas Court of Criminal Appeals briefly noted the appearance of a circuit split between "[t]he Third, Fourth, Fifth, and Eleventh Circuits."[94] All but the Fourth Circuit refused to require law enforcement to obtain a warrant based upon probable cause before seeking the collection of CSLI.[95] Specifically, those courts held CSLI is "a record that the 'provider has already created'—[and therefore] is not subject to a reasonable expectation of privacy that implicates the Fourth Amendment."[96] Contrariwise, the Fourth Circuit held government inspection of CSLI without a warrant violates the Fourth Amendment.[97] But because the

92. *Id.* at 744 ("[P]etitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business.").

93. *Ford II*, 477 S.W.3d 321, 329 (Tex. Crim. App. 2015) (quoting 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f), at 927 (5th ed. 2012)). While the *Ford* court cited to LaFave as authority, the court omitted his reservations and overall lack of confidence in the *Miller* and *Smith* decisions. LaFave contended the *Miller* result was "dead wrong" by labeling the Supreme Court's reasoning as "woefully inadequate," which did "great violence to the theory of Fourth Amendment protection." 1 LAFAVE, *supra*, § 2.7(c), at 970. LaFave is more critical of *Smith*. He thought the *Smith* opinion was a "mockery of the Fourth Amendment" since the result allows police, "without any cause whatsoever and for whatever purpose they choose[,] [to] uncover private relationships with impunity merely because the telephone company . . . . has the capacity to make a record of such relationships." *Id.* § 2.7(b), at 954. LaFave rejected these cases largely because he understood business records contain an "enormous quantity of information about people," and permitting "unrestrained police access to such data would constitute a devastating imposition upon privacy." *Id.* § 2.7(c), at 976.

94. *Ford II*, 477 S.W.3d at 329–30 (noting the Fourth Circuit's outlier opinion was recently vacated). The Sixth Circuit's opinion came after *Ford*, but it joined the consensus. *See generally* United States v. Carpenter, Nos. 14-1572, 14-1805, 2016 WL 1445183 (6th Cir. Apr. 13, 2016) (joining the Fifth and Eleventh Circuits in permitting the government's warrantless collection of CSLI); *see also infra* note 175 for a discussion on how Texas would treat the Sixth Circuit's decision.

95. *Id.* at 330.

96. *Id.*

97. *Id.* (citing United States v. Graham, 796 F.3d 332, 356 (4th Cir.), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015)).

opinion was vacated after an en banc rehearing was granted, the *Ford* court concluded this case was of "indefinite precedential value."[98]

The *Ford* court went on to apply the Third-Party Doctrine to the facts of this case, finding "appellant neither owned nor possessed the records he sought to suppress."[99] Because the Third-Party Doctrine predates cell phones, the court relied on the Eleventh Circuit's recent application.[100] The Eleventh Circuit in *Davis v. United States*[101] presumed cell phone users "knew of uncontroverted and publically available facts about technologies and practices . . . . about the functions of cell towers [and] about telephone providers' recording cell tower usage."[102] The *Davis* court suggested this was the logic taken by the Supreme Court in *Smith*, despite *Smith* dealing strictly with landline telephones.[103] In applying the *Davis* analysis, the *Ford* court determined the service provider "collects and stores this historical [CSLI] for its own business purposes, in part to optimize service on its network."[104]

The court also adopted an interesting claim[105] from the Fifth Circuit that service providers are "not required by the government to record this information or store it."[106] This declaration appears overly simple and ignores the convoluted relationship between the Department of Justice and the telecommunications network.[107] Attempting to understand the extent of government involvement in the collection of CSLI would be unprecedented in this type of case; but it is necessary to properly evaluate

98. *Id.*

99. *Id.*

100. *Id.* (citing *Davis II*, 785 F.3d 498, 511 (11th Cir.) (en banc), *cert denied*, 136 S.Ct. 479 (2015)).

101. *Davis II*, 785 F.3d 498 (11th Cir.) (en banc), *cert denied*, 136 S.Ct. 479 (2015).

102. *Id.* at 511.

103. *Id.* at 511–12.

104. *Ford II*, 477 S.W.3d at 330.

105. What makes this claim interesting is the Fifth Circuit's speculative interpretation that the SCA "conforms to existing Supreme Court Fourth Amendment precedent. This precedent, as it now stands, does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure." *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 614–15 (5th Cir. 2013). However, this analysis misapplies or ignores the original intent behind the SCA, which was meant to correct Supreme Court precedent and not conform to it. *See infra* Part III.B.3.

106. *Ford II*, 477 S.W.3d at 330 (citing *In re U.S. for Historical Cell Site Data*, 724 F.3d at 611–12). The court further proclaimed service providers "control what they record" and the "Government merely comes in after" to obtain the records. *Id.* at 330–31. To come to this conclusion, the court acknowledged FCC regulations that require service providers to determine the location of a caller and recognized service providers are not required to record the information. *Id.* at 330 & n.10. However, the court did not explain this conclusion beyond citing to a student-written note detailing the records-keeping practice of AT&T. *Id.* at 331 n.11.

107. *See infra* Part III.B.2. for further discussion.

the legitimacy of subscriber privacy.[108] Unfortunately, the *Ford* court appeared content with the Fifth Circuit's position by adopting it without much discussion. Accordingly, the court held appellant's expectation of privacy lacked legitimacy.[109]

"Appellant fairly manifested a subjective expectation of privacy" since the records were created from passive activity, but this expectation was not legitimate considering he did not own or control the records and voluntarily purchased a phone on AT&T's network.[110] The court also concluded society would not find this expectation reasonable because "cell users know that they must transmit signals to cell towers . . . exposing to their service provider their general location."[111]

Next, the court distinguished this case from the Supreme Court case, *United States v. Jones*.[112] In *Jones*, law enforcement placed a tracker on a vehicle for twenty-eight days.[113] The Court held the practice unconstitutional under a trespass theory as opposed to one under a reasonable expectation of privacy.[114] But in *Ford*, unlike *Jones*, "there [was] no GPS device, no physical trespass . . . . [and] only short-term CSLI was acquired."[115] The Texas court also distinguished the instant case from that of the Fourth Circuit.[116] The Fourth Circuit's case, *United States v. Graham*,[117] involved CSLI collection for 221 days.[118] The *Ford* panel stated, "The Fourth Circuit took pains to repeatedly note that it was only

108. The Supreme Court is known for recognizing Fourth Amendment protection when private entities gather information "in conjunction with or at the behest of law enforcement." Ferguson v. City of Charleston, 532 U.S. 67, 79 n.15 (2001) (quoting New Jersey v. T.L.O., 469 U.S. 325, 341 n.7 (1985)).

109. *Ford II*, 477 S.W.3d at 330.

110. *Id.* at 331.

111. *Id.* (first citing *Davis II*, 785 F.3d 498, 511 (11th Cir.) (en banc), *cert denied*, 136 S.Ct. 479 (2015); then citing *In re U.S. for Historical Cell Site Data*, 724 F.3d at 613–14. It appears *Davis* and *In re U.S. for Historical Cell Site Data* adopted this reasoning to analogize it with the idea in *Smith*—that when users dial phone numbers, they generally understand it must go through the phone company. *See supra* note 93 and accompanying text. Obviously, cell phone technology is much more complicated than simply giving a phone number to an operator to connect a call. *See, e.g.*, *In re U.S. for Historical Cell Site Data*, 724 F.3d at 602 n.1 (noting the government's own lack of understanding of how or when phones transmit data to the network).

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

113. *Id.* at 948.

114. *Id.* at 949.

115. *Ford II*, 477 S.W.3d at 333.

116. *Id.*

117. United States v. Graham, 796 F.3d 332 (4th Cir.), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

118. *Id.* at 342.

addressing long-term [CSLI]."[119]

Before closing the opinion, the Texas Court of Criminal Appeals "acknowledge[d] that Fourth Amendment concerns might be raised if long-term location information were acquired."[120] Until then, the court reasoned that because a third-party service provider "gathered and maintained the information as business records . . . [appellant] did not have a reasonable expectation of privacy in the data."[121] And while "it is widely predicted that the Supreme Court is primed to take up the issue," the court was "confident that the discrete four days" was not enough to "reveal a comprehensive view of the specific details of appellant's daily life."[122]

PART III: *FORD V. STATE* ADDS TO THE WIDESPREAD CONSTITUTIONAL CONCERNS SURROUNDING THE WARRANTLESS COLLECTIONS OF CSLI

A. Ford v. State *Bases Fourth Amendment Protection on Time Rather than Content and Precision*

While the *Ford* court thinks *Graham* is factually distinguishable, its holdings are highly relevant to the issues of law in *Ford.* The overall goal of examining CSLI is to "track a person's movements between public and private spaces."[123] And while the Fourth Circuit emphasized a focus on long-term CSLI,[124] long-term in *Graham* means something entirely different than *Ford* leads us to believe. "[T]he government cannot know in advance of obtaining [CSLI] how revealing it will be or whether it will detail the cell phone user's movements in private spaces."[125] It did not matter whether the government sought CSLI for "14 days or 221 days."[126] Instead, the court was troubled with the "well over 100 data

119. *Ford II*, 477 S.W.3d at 333.

120. *Id.* at 334. This suggestion is in line with the Supreme Court's concern with prolonged surveillance, which allows law enforcement to reconstruct "nearly every aspect" of someone's life, "from the mundane to the intimate." Riley v. California, 134 S.Ct. 2473, 2490 (2014). *Riley* quoted Justice Sotomayor's concern that long-term monitoring generates a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* (quoting United States v. Jones, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

121. *Ford II*, 477 S.W.3d at 322.

122. *Id.* at 334.

123. *Graham*, 796 F.3d at 348.

124. *See supra* note 120 and accompanying text.

125. *Graham*, 796 F.3d at 350.

126. *Id.*

points for each Appellant per day."[127]

In applying this logic to *Ford*, officers reasonably knew the four days of CSLI would reveal at least some data points within Ford's home—based on the timeframe and appellant's own voluntary statement. Nothing in the facts provides that law enforcement knew what the records would show or to what precision. While detectives may have inferred what the records would show, these inferences "do[] not ameliorate or lessen in any manner the invasion of privacy."[128] It should be quite concerning that judges signing 2703(d) orders for CSLI do so "without knowing how precise [or invasive] the location information will be."[129]

B. *Why the Third-Party Doctrine Should Not Apply*

The Third-Party Doctrine predates cell phones and CSLI. "[T]he extent of information that we expose to third parties has increased by orders of magnitude since the Supreme Court decided *Miller* and *Smith*."[130] Justice Sotomayor called the approach "ill-suited to the digital age," and it should not be used to disentitle society from Fourth Amendment protection.[131] Even if it does apply, there are two questions still to be addressed: whether a person voluntarily conveys CSLI to a service provider and what actually constitutes a business record.

1. A Legitimate Expectation of Privacy Turns on Whether Someone Voluntarily Conveys CSLI

"[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[132] In *Miller*, the defendant actively turned over information to banks by writing information on deposit slips.[133] In *Smith*, the defendant actively volunteered his numerical information to the phone company when placing calls.[134] Even in light of precedent, the Court never held third-party records are excluded from Fourth Amendment protection. Instead the focus was always on voluntary conveyance because "that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of

127. *Id.*
128. *Id.* at 351.
129. *Davis II*, 785 F.3d 498, 543 (11th Cir. 2015) (en banc) (Martin, J., dissenting).
130. *Id.* at 538.
131. United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring).
132. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
133. United States v. Miller, 425 U.S. 435, 442 (1976).
134. *Smith*, 442 U.S. at 744.

privacy."[135]

CSLI is automatically generated each time a phone and cell site connect.[136] There is no active participation on part of the user. Therefore, it is improper 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."[137]

Graham is in contention with *Ford*'s (and the Fifth and Eleventh Circuits') position that "users volunteer to convey their location information simply by choosing to activate and use their cell phones."[138] The Supreme Court recently classified cell phones as a "pervasive and insistent part of daily life."[139] So without the assumption of risk that comes with a voluntary conveyance, applying the Third-Party Doctrine "would simply permit the government to convert an individual's cell phone into a tracking device . . . and to do so without probable cause."[140]

Ford, in accord with *Davis*, acknowledged the existence of a subjective reasonable expectation of privacy—however diminished from the so-called "voluntary conveyance"—but determined it is not enough to warrant Fourth Amendment protection.[141] The Supreme Court would reject these contentions because "diminished privacy interests do[] not mean that the Fourth Amendment falls out of the picture."[142] Unfortunately, the Supreme Court missed an opportunity to do by denying a writ of certiorari in the *Davis* case.[143]

Ford's contention about what society actually knows also appears inconsistent with the Supreme Court's understanding of what the public knows of cell phone technology. The Court reasoned, "Cell phone users often may not know whether particular information is stored on the device

135. United States v. Graham, 796 F.3d 332, 354 (4th Cir.), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

136. *Id.*

137. *Id.* at 355.

138. *Id.*

139. Riley v. California, 134 S.Ct. 2473, 2484 (2014); *see also* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) ("Cell phone[s] . . . are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

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

141. *Ford II*, 477 S.W.3d 321, 331 (Tex. Crim. App. 2015); *accord Davis II*, 785 F.3d 498, 518 (11th Cir.) (en banc) (noting diminished expectations of privacy do find a presumption of constitutional protection), *cert denied*, 136 S.Ct. 479 (2015).

142. *Riley*, 134 S.Ct. at 2488.

143. *Davis III*, 136 S.Ct. 479 (2015).

or in the cloud, [but] it generally *makes little difference.*"[144]

2. Why CSLI Is Not a Business Record

Collecting CSLI is not required to complete the provided service but serves more of a law enforcement function. "Cell phone users do not actively or knowingly communicate or 'trade' their location information to their service providers as part of the consideration for the services provided . . . ."[145] Instead, the relationship between cell phone users and the phone company should be compared to that of a hotel proprietor and his guests. The Supreme Court "explicitly refused to permit an otherwise unlawful police search of a hotel room to rest upon consent of the hotel proprietor."[146] While seemingly possible for officers to seek basic information from a hotel proprietor, such as the guest's name, address, and any other basic information necessary to complete the transaction, it would appear wholly impermissible to allow further inquiry with neither a warrant nor the guest's consent.[147] It is hard to reason service providers in the telecommunications industry are somehow an exception.

Imagine if the availability of a 2703(d) order was deemed limited to non-location information. Law enforcement would then be restricted to the other two Section 2703(c)(1) options to acquire CSLI: (1) obtain a warrant or (2) "consent of the subscriber or customer."[148] The statute does not provide for the service provider to give consent on behalf of the cell phone user. Assuming CSLI can be obtained under the SCA, the Act appears to recognize cell phone users possess some sort of ownership interest in their location information recorded and stored by the phone companies.

Ford highlights other ownership concerns but from the service provider's perspective. The court determined service providers are not

144. *Riley*, 134 S.Ct. at 2491 (emphasis added).

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

146. Stoner v. California, 376 U.S. 483, 489 (1964).

147. The Supreme Court recently struck down a city ordinance requiring hotel proprietors to collect specific non-business related information on guests, including "the guest's date and time of arrival and scheduled departure date; the room number assigned to the guest; . . . . and any guests who rent a room for less than 12 hours." City of Los Angeles v. Patel, 135 S.Ct. 2443, 2447–48 (2015). Although the *Patel* Court struck the ordinance because it also required hotel proprietors to release this detailed guest information to law enforcement upon request, the Court had no trouble holding that law enforcement access to the information amounted to a warrantless search without a recognized exception and a violation of the Fourth Amendment. *Id.* at 2451–54. Unfortunately, *Patel* resulted from a facial challenge from hotel owners, so the Court never examined the privacy interests of the guests.

148. 18 U.S.C. § 2703(c)(1)(A), (B) (2012).

required to collect or store CSLI. This ignores the relationship between service providers and law enforcement, which existed since the inception of CSLI.[149] This relationship is documented through various legislative and regulatory schemes; the most significant is attached to the FCC's Enhanced 911 systems mandate requiring the collection and storage of CSLI.[150]

Many feared "once the wireless carriers and third-party service providers collect the information" under the 911 mandate, "the government [would] then be able to access the stored information."[151] Immediately after one of the earlier releases of the 911 mandate, the FTC held a workshop consisting of various government agencies and service providers to determine the overall impact and viability of collecting CSLI under the new system.[152] One issue raised was cost,[153] which providers settled by passing to its subscribers.[154] Published panel discussions

149. Congress first tipped the scales in 1994, when it ordered service providers to update their systems to permit for immediate government access upon proper request. H.R. REP. NO. 103-827, pt. 1, at 16 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3497. Aware of the expense needed to quickly facilitate access, Congress agreed to pay $500 million in taxpayer dollars to assist service providers. *Id.* at 16. The result of the 1994 amendment, as understood by Congress, was that service providers were to collect specific information and compile it in one place, "reveal[ing] a great deal about [Americans'] private lives." *Id.* at 17.

150. *See generally In re* Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, 14 FCC Rcd. 17388 (1999) (requiring service providers to be able to locate a subscriber's cell phone so dispatchers know where a 911 caller is located). Prior to 1999, service providers had discretion whether to improve their location gathering capabilities by October 1, 2001—but even then, the requirements were stringent. *See* 911 Service, 47 C.F.R. § 20.18(e) (1996) (indicating service providers who submitted location data must provide "longitude and latitude within a radius of 125 meters"). Service providers could have been forced to upgrade their systems but only if a mechanism was in place to allow service providers to recoup costs associated with upgrading and transmitting location data. *Id.* § 20.18(f). In 1998, the relaxed requirements remained, but the FCC clarified the accuracy requirement applied to all 911 calls. 911 Service, 47 C.F.R. § 20.18(e) (1998). In 2000, the requirements completely changed. As a result of these revisions, all service providers were now required to obtain location data on all callers in their coverage area by October 1, 2002. 911 Service, 47 C.F.R. § 20.18(f) (2000). Location data had to be within "100 meters for 67 percent of calls, [and] 300 meters for 95 percent of calls." *Id.* § 20.18(h)(1). To improve accuracy, the FCC also mandated that cell phones be manufactured and sold with location capabilities starting March 1, 2001. *Id.* § 20.18(g)(1).

151. Geoffrey D. Smith, Note, *Private Eyes Are Watching You: With the Implementation of the E-911 Mandate, Who Will Watch Every Move You Make?*, 58 FED. COMM. L.J. 705, 709 (2006).

152. FTC, PUBLIC WORKSHOP: THE MOBILE WIRELESS WEB, DATA SERVICES AND BEYOND: EMERGING TECHNOLOGIES AND CONSUMER ISSUES (2002), https://www.ftc.gov/sites/default/files/documents/reports/mobile-wireless-web-data-services-and-beyond-emerging-technologies-and-consumer-issues/wirelesssummary_0.pdf [hereinafter FTC PUBLIC WORKSHOP].

153. *Id.* at 27.

154. *See, e.g.*, *Understanding the Surcharges, Taxes, Fees and Other Charges on Your Bill*, SPRINT, http://support.sprint.com/support/article/Know_aboutSprint_surcharges_taxes_fees_and_other_charges/case-ib376964-20090810-135914 (last updated Mar. 7, 2016) (listing and describing the

provide the following soundbites that show the significance of collecting and storing CSLI under the 911 mandate: "[L]ocation information is extremely sensitive";[155] "[C]ompanies will be able to track location in a way that was never available before";[156] "[O]nce the service provider has the information, others could obtain the data through a court order";[157] and "[C]arriers are not currently archiving this location information."[158] Because the government is so clearly intertwined in this process, it is obvious CSLI was initially generated mostly, if not purely, "*for law enforcement purposes*," which is not a business-related event.[159]

3. Even If CSLI Is a Business Record, Congress Intended to Recognize Privacy in Subscriber Information Under the SCA

Following the *Miller* decision,[160] Congress responded with the Right to Financial Privacy Act of 1978.[161] The purpose was to recognize "privacy in financial records" where the Court decided there was none "since the records are the 'property' of the financial institution."[162] Likewise, the SCA was "modeled after the Right of Financial Privacy Act" and designed

various additional charges that customers may see on their monthly bill).

155. FTC PUBLIC WORKSHOP, *supra* note 152, at 8.

156. *Id.*

157. *Id.*

158. *Id.* at 9.

159. Ferguson v. City of Charleston, 532 U.S. 67, 83 (2001). CSLI may no longer be solely for law enforcement purposes. Many understood service providers would eventually "find commercial application for the information once collected" to take advantage of having such sensitive consumer information on hand. FTC PUBLIC WORKSHOP, *supra* note 152, at 10; *see also* Smith, *supra* note 151, at 713 ("Location-based services are being developed that provide customers with information to traffic, weather, and retail stores based upon their geographical position at any given time. . . . Also, businesses have begun using location tracking in cellular phones to keep tabs on their employees and increase productivity.").

160. The Right to Financial Privacy Act of 1978 was meant to be a

> congressional response to the Supreme Court decision in the *United States v. Miller* which held that a customer of a financial institution has no standing under the constitution to contest government access to financial records. The Court did not acknowledge the sensitive nature of these records, and instead decided that since the records are the 'property' of the financial institution, the customer has no constitutionally recognizable privacy interest in them. Nevertheless, while the Supreme Court found no constitutional right of privacy in financial records, it is clear that Congress may provide protection of individual rights beyond that afforded in the Constitution.

H.R. REP. NO. 95-1383, at 28 (1978), *reprinted in* 1978 U.S.C.C.A.N. 9273, 9306.

161. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (codified as amended at 12 U.S.C. §§ 3401–3422 (2012)).

162. H.R. REP. NO. 95-1383, at 28.

"to protect privacy interests in personal and proprietary information."[163] These two Acts suggest Congress did not agree with the then emerging Third-Party Doctrine.

However, the question arises whether the SCA dispenses of the warrant requirement by offering alternative collection methods. The statute's text does not explain when a 2703(d) order may be chosen over the warrant requirement. But an examination of legislative history provides two logical explanations.

First, the Justice Department was very involved in the debate process and probably objected to needing a warrant over a subpoena.[164] But Senator Leahy, the original bill's sponsor, tends to be more protective of civil liberties. Therefore, one possibility is Section 2703(d) was added to garner needed support from the Justice Department to finally get the SCA enacted. After all, the bill took years to get enacted[165] and involved lengthy "negotiations with the Justice Department."[166] Second, the information initially accessible under the SCA did not implicate privacy concerns anywhere near what it does today. The SCA allowed for the collection of a "record or other information pertaining to a subscriber,"[167] which was later defined in an amendment to mean "name, address, telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber."[168]

From the 1980s through the 1990s, requiring a judge to approve an otherwise normal subpoena for basic subscriber information was a significant privacy-protecting method. However, these protections evaporated with the 2001 terrorist attacks. Within six weeks of September 11, 2001, absent any formal debate, voting procedure, or other legislative processes, Congress passed the sweeping Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).[169] Without any

163. S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

164. Senator Leahy presented the SCA on the Senate floor in 1986, announcing it was a result of "[two] years of hard work" with the Justice Department and a number of civil liberty groups to "update the law to better protect communications privacy." 132 CONG. REC. 14,600 (1986) (statement of Sen. Patrick Leahy).

165. *See id.* ("Our 2-year effort . . . began in 1984 when [we] asked the Attorney General whether he believed interceptions . . . were covered by the [1968] Federal wiretap laws.").

166. *Id.* at 14,609 (statement of Sen. Charles Mathias Jr.).

167. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1862 (amended 1994) (codified as amended at 18 U.S.C. § 2703(c) (2012)).

168. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279, 4292 (1994) (codified at 18 U.S.C. § 2703(c) (2012)).

169. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept

trace of legislative intent, the SCA was amended under the USA PATRIOT Act to allow for the collection of "connection records."[170] Nothing exists in the text or history of the SCA to define connection records. Seemingly, this obscures the original purpose behind the SCA and possibly ignited this nationwide debate.[171] Furthermore, with the timing of the passage of the enhanced 911 mandate and the 2001 amendment to the SCA, it would appear "the government has enabled itself to collect personal information indirectly, which it most likely would have been prevented from doing under the Constitution."[172]

CONCLUSION

The Supreme Court hinted to law enforcement: When cell phones are involved, "get a warrant."[173] The message was succinct. Texas, with the *Ford* case, shows this matter is not so simply resolved. In denying certiorari in *Davis*, the Supreme Court passed on the opportunity to make its message absolute. By allowing the *Davis* decision to stand, the temporary split may have subsided, but the root of this issue remains. Not surprisingly, the Fourth Circuit, with its *Graham* decision, quickly reignited the federal split. Now Texas, with *Ford*, provided a much needed split among states.[174]

Ford did not merely reject Fourth Amendment protection as most federal cases have. It suggested the Fourth Amendment could apply, but not for four days' worth of CSLI. It should follow then, regardless of an

---

and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 18 U.S.C., 22 U.S.C., 31 U.S.C., 47 U.S.C. & 50 U.S.C.). This act only took six weeks to pass and did so with "an overwhelming majority in both the House and Senate." Regina Germain, *Rushing to Judgment: The Unintended Consequences of the USA PATRIOT Act for Bona Fide Refugees*, 16 GEO. IMMIGR. L.J. 505, 505 (2002).

170. USA PATRIOT Act, Pub. L. No. 107-56, § 210, 115 Stat. 272, 283 (2001). *See generally id.* (omitting any discussion related to changes in the SCA); *see also* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 24, at 49 ("The legislative history does not comment on the intent of this change nor did this topic arise in any of the negotiations surrounding the passage of the Act.").

171. See *supra* note 33 for a brief discussion of the first report case of law enforcement obtaining CSLI, which occurred in 2005, four years after the 2001 amendment.

172. Smith, *supra* note 151, at 709.

173. Riley v. California, 134 S.Ct. 2473, 2495 (2014).

174. *See supra* note 2. The *Ford* court acknowledged the Florida and New Jersey decisions but attempted to distinguish them from the instant case by explaining the CSLI in *Ford* was different because it did not amount to real-time information. *Ford II*, 477 S.W.3d 321, 334 n.18 (Tex. Crim. App. 2015) (first citing Tracey v. State, 152 So.3d 504, 526 (Fla. 2014); then citing State v. Earls, 70 A.3d 630, 644 (N.J. 2013)). However, *Graham* holds the distinction "constitutionally insignificant," noting "[t]he Fourth amendment challenge is directed toward the government's investigative conduct, i.e., its decision to seek and inspect CSLI records without a warrant." United States v. Graham, 796 F.3d 332, 350 (4th Cir.), *reh'g en banc granted*, 624 F. App'x 75 (4th Cir. 2015).

assumption of risk or voluntary conveyance, the collection at some point could amount to a Fourth Amendment search requiring a warrant.[175] But the court implied so long as law enforcement limited their 2703(d) requests to a few days, the collection would not amount to a search, regardless of content or precision of the records. Because Texas emerged a new split with new issues, it is clear the Supreme Court can no longer avoid addressing the constitutionality of the warrantless collection of CSLI. Texas may have finally forced a resolution in this decade-old debate.

175. The Texas court, for example, would probably disagree with the recent Sixth Circuit decision. The Sixth Circuit held the warrantless collection of CSLI obtained "from various wireless carriers for 16 different phone numbers" from December 2010 through June 2011 did not implicate the Fourth Amendment. United States v. Carpenter, Nos. 14-1572, 14-1805, 2016 WL 1445183, at *1 (6th Cir. Apr. 13, 2016). The Sixth Circuit's opinion is the broadest thus far. It did not examine any assumption of risk or voluntary conveyance to find cell phone users lack Fourth Amendment protection, because CSLI is just a business record. *See generally id.* at *3–8 (examining this case largely under a premise that CSLI is collected merely for business purposes). See *supra* Part III.B.2 for a discussion why CSLI is not a business record. *But see supra* notes 105 and 106 and accompanying text, showing the assumption that CSLI is a business record.