"TIME WORKS CHANGES": MODERNIZING FOURTH AMENDMENT LAW TO PROTECT CELL SITE LOCATION INFORMATION

Abstract: In 2012, federal juries convicted two men of armed robbery based in part on historical cell site location information ("CSLI") evidence. Historical CSLI can reproduce a person's location with great specificity. Cell phone users generate CSLI automatically by operating their cellular phones. These facts raise serious privacy concerns. This Note argues that Congress must take action to ensure that law enforcement agents can access a suspect's historical CSLI only after a neutral magistrate finds probable cause that a crime has been committed. Further, this Note argues that because cell phone users do not voluntarily convey CSLI to their phone companies, the government may not, absent a probable cause warrant, access that information by invoking the third party doctrine announced by the U.S. Supreme Court in its1979 decision in *Smith v. Maryland*.

INTRODUCTION

On February 10, 2012, in *United States v. Davis*, a jury in federal district court in Florida found Quartavious Davis guilty on seventeen counts stemming from his commission of seven armed robberies in 2010.[1] Less than three months later, in *United States v. Graham*, a jury in federal district court in Maryland found Aaron Graham guilty on seventeen counts arising from his perpetration of six armed robberies in 2011.[2] The prosecution in both cases obtained and used the suspects' historical cell site location information ("CSLI") by meeting a statutory standard of justification that requires less judicial scrutiny than the traditional probable cause standard mandated by the Fourth Amendment.[3] Historical CSLI is data that the cellular service provider creates and keeps about the communication between an individual cell phone

[1] United States v. Davis, 785 F.3d 498, 500–01 (11th Cir.) (en banc), *cert. denied*, 136 S. Ct. 479 (2015); Jury Verdict at 1–5, United States v. Davis, No. 10-20896 (S.D. Fla. Feb. 10, 2012), ECF No. 293.

[2] United States v. Graham (*Graham I*), 796 F.3d 332, 338–39, 342 (4th Cir. 2015), *aff'd on reh'g*, 824 F.3d 421, 421 (4th Cir. 2016) (en banc) (*Graham II*); Jury Verdict at 1–5, United States v. Graham et al., No. 11-00094 (D. Md. May 2, 2012), ECF No. 139.

[3] *Graham I*, 796 F.3d at 344; *Davis*, 785 F.3d at 502; Memorandum Opinion on Defendants' Motion to Suppress Historical Cell Site Location Data at 3–4, United States v. Graham, No. 11-00094 (D. Md. Mar. 1, 2012), ECF No. 84; Scott A. Fraser, Note, *Making Sense of New Technologies and Old Law: A New Proposal for Historical Cell-Site Location Jurisprudence*, 52 SANTA CLARA L. REV. 571, 574–75 (2012).

and the cellular network.[4] In 2015, on rehearing, an en banc panel of the Fourth Circuit Court of Appeals held that the prosecution's use of historical CSLI in the *Graham* case violated the defendant's Fourth Amendment right to be free from unreasonable search and seizure.[5]

A lively debate exists as to whether citizens are aware that, through a court order under the Stored Communications Act ("SCA"), the government may obtain their historical CSLI without a showing of probable cause.[6] In a growing number of jurisdictions, individuals lose an objective expectation of privacy in their physical location simply by switching on their cellular telephones.[7] Judges rationalize this view by reasoning that because subscribers receive notice in their contracts that service providers collect CSLI, just turning on a cell phone equates to a voluntary CSLI transmission.[8] Some judges believe otherwise and have held that cellular service contracts do not provide sufficient notice to subscribers, meaning that most subscriber CSLI transmissions are involuntary.[9]

Regardless of how our society eventually settles the debate over whether law enforcement agencies must have probable cause to obtain historical CSLI, the fact remains that five federal Courts of Appeals covering more than 155 million Americans have approved acquisition of historical CSLI by law en-

---

[4] *See* Fraser, *supra* note 3, at 574–75 (defining historical cell site location information ("CSLI")). Unlike prospective CSLI that encompasses the user's real-time data, historical CSLI refers to the user-generated data that the cellular service provider preserves. *Id.*

[5] *Graham I*, 796 F.3d at 343; *Davis*, 785 F.3d at 500.

[6] *See* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) (declining to find a reasonable expectation of privacy in the defendant's historical CSLI); *Graham I*, 796 F.3d at 347 (determining that tracking a criminal suspect to his home through the use of his CSLI violates the suspect's reasonable expectation of privacy); *Davis*, 785 F.3d at 511 (holding that cell subscribers have no objective expectation of privacy in their CSLI). The Stored Communications Act ("SCA") directs magistrate judges to issue court orders for CSLI on a showing of specific and articulable facts demonstrating that it is reasonable to believe that the records requested are relevant to an ongoing criminal investigation. 18 U.S.C. § 2703(d) (2012).

[7] *See Davis*, 785 F.3d at 511 (deciding that individuals have no objective expectation of privacy in their historical CSLI); *In re* Historical Cell Site Data, 724 F.3d 600, 614–15 (5th Cir. 2013) (declining to find an objective expectation of privacy in cell phone users' historical CSLI); *In re* Order Directing a Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't (*Elec. Commc'n Serv.*), 620 F.3d 304, 313 (3d Cir. 2010). In *In re Electronic Communication Service*, the Third Circuit determined that the magistrate judge below erred when she found the SCA required a probable cause standard due to the privacy interest implicated in CSLI. 620 F.3d at 313.

[8] *Davis*, 785 F.3d at 511; *In re Historical Cell Site Data*, 724 F.3d at 613, 614. In *In re Historical Cell Site Data*, the Fifth Circuit determined that users voluntarily turn over their CSLI to their service providers. 724 F.3d at 613. The court reached this conclusion after observing that user agreements inform subscribers that their providers collect this information, and also that cell subscribers understand that their devices must send a signal to a nearby tower in order to connect their calls. *Id.* at 614.

[9] *See Graham I*, 796 F.3d at 355–56 (holding that users do not voluntarily convey their CSLI to their carriers, and that consent to warrantless acquisition of CSLI is a myth); *Davis*, 785 F.3d at 534–35 (Martin, J., dissenting) (opining that cell phone subscribers do not voluntarily convey CSLI when they receive a call).

forcement on a low, "specific and articulable facts" standard.[10] The Department of Justice has argued in favor of this approach before at least two federal Courts of Appeals.[11] In response, civil liberties watchdogs and technology proponents assert that the Fourth Amendment requires law enforcement to obtain a warrant based on a showing of probable cause for the collection of historical CSLI.[12]

When the government obtains a criminal suspect's historical CSLI from his or her cellular carrier without first demonstrating probable cause to a neutral magistrate, that suspect experiences an invasion of his or her Fourth Amendment rights.[13] This imposition on personal liberty affects every American citizen who carries a cell phone, from the most conscientious and law-abiding among us to the most hardened criminals on our streets.[14] Accordingly,

---

[10] *See Carpenter*, 819 F.3d at 888 (holding that the government did not conduct an unreasonable search by acquiring the defendant's historical CSLI); *Graham II*, 824 F.3d at 424 (upholding warrantless government acquisition of historical CSLI); *Davis*, 785 F.3d at 518 (holding constitutional government use of the third party doctrine to obtain historical CSLI); *In re Historical Cell Site Data*, 724 F.3d at 614–15 (approving government collection of historical CSLI without a warrant); *Elec. Commc'n. Serv.*, 620 F.3d at 313 (assenting to government acquisition of historical CSLI under the low SCA standard); U.S. CENSUS BUREAU, POPULATION DIVISION, ANNUAL ESTIMATES OF THE RESIDENT POPULATION: APRIL 1, 2010 TO JULY 1, 2014—2014 POPULATION ESTIMATES, AM. FACT-FINDER (Dec. 2014) (showing populations of states where federal courts have approved warrantless collection of CSLI); FED. JUDICIAL CTR., GEOGRAPHICAL BOUNDARIES OF THE U.S. COURTS OF APPEALS AND U.S. DISTRICT COURTS AS SET FORTH BY 28 U.S.C. §§ 41, 81–131 (1999), http://www2.fjc.gov/sites/default/files/2012/IJR00007.pdf [https://perma.cc/WY28-DV53] (displaying the states that compose each federal circuit).

[11] *In re Historical Cell Site Data*, 724 F.3d at 603; *Elec. Commc'n Serv.*, 620 F.3d at 305.

[12] *See, e.g.*, Brief for ACLU Foundation et al. as Amici Curiae Supporting Defendants-Appellants at 15–16, United States v. Graham, 796 F.3d 332 (4th Cir. 2015) (No. 12-4659), 2013 WL 3328019 (emphasizing that the acquisition of CSLI for a 221-day period is a violation of the Fourth Amendment unless the government conducts the acquisition pursuant to a probable cause warrant); En Banc Brief for Electronic Frontier Foundation as Amicus Curiae Supporting Appellant at 4, United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (No. 12-12928), 2014 WL 7006395 (arguing that a probable cause search warrant should be required for law enforcement to access CSLI).

[13] *See* Commonwealth v. Augustine, 4 N.E.3d 846, 865–66 (Mass. 2014) (holding that criminal suspects have an objective expectation of privacy in their CSLI that law enforcement's warrantless acquisition of CSLI violates in contravention of the Fourth Amendment); Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 38 (2013) (noting that probable cause should be required for the acquisition of CSLI because obtaining precise location information is a significant government intrusion).

[14] Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, THE ATLANTIC, (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/ [https://perma.cc/3FEJ-2BDV] (noting that cellular service providers develop a detailed database of many Americans' whereabouts based on their CSLI); Abigail Tracy, *While the Supreme Court Hesitates on Warrantless Cell Location Data Collection, Your Privacy Remains at Risk*, FORBES (Oct. 16, 2015, 9:00AM), http://www.forbes.com/sites/abigailtracy/2015/10/16/while-the-supreme-court-hesitates-on-warrantless-cell-location-data-collection-your-privacy-remains-at-risk/ [https://web.archive.org/web/20160322181311/http://www.forbes.com/sites/abigailtracy/2015/10/16/while-the-

this Note argues that law and public policy require legislative and judicial reexamination of the federal circuit court decisions allowing acquisition of historical CSLI on a "specific and articulable facts" standard.[15] To effect a reexamination consonant with the Fourth Amendment, the federal judiciary must take two actions.[16] First, courts should declare § 2703 of the SCA unconstitutional as applied to the acquisition of historical CSLI.[17] Second, courts should hold the third party doctrine inapplicable to the disclosure of historical CSLI.[18] Additionally, Congress must establish a statutory probable cause requirement for historical CSLI acquisition and must pass legislation that places control over CSLI transmission and recording in the hands of cell phone users.[19]

Part I of this Note provides an overview of Fourth Amendment jurisprudence and includes an introduction both to § 2703 of the SCA and to the third party doctrine.[20] Part II discusses how four Courts of Appeals have applied the SCA and the third party doctrine to law enforcement requests for historical CSLI.[21] Part III suggests that Congress should replace § 2703 with legislation that requires probable cause to access historical CSLI and consent by cellular subscribers for collection of their CSLI.[22] Part III also argues that § 2703 of the SCA should be struck down because it violates the Fourth Amendment as applied to historical CSLI requests.[23] Finally, this Note concludes that the U.S. Supreme Court should both reform the third party doctrine for the modern era and hold that cell phone users have an objectively reasonable expectation of privacy in their historical CSLI.[24]

---

supreme-court-hesitates-on-warrantless-cell-location-data-collection-your-privacy-remains-at-risk/#3523cd11738e] (emphasizing that cellular providers collect CSLI on every subscriber).

[15] *See infra* notes 162–201 and accompanying text.

[16] *See infra* notes 162–201 and accompanying text.

[17] *See infra* notes 174–201 and accompanying text.

[18] *See infra* notes 193–201 and accompanying text.

[19] *See* S. 356, 114th Cong. (2015) (as referred to S. Comm. on the Judiciary, Feb. 4, 2015) (Senate bill establishing a probable cause warrant requirement for historical CSLI); H.R. 283, 114th Cong. (2015) (as referred to H. Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations, Feb. 2, 2015) (suggesting a probable cause requirement for historical CSLI collection); *infra* notes 165–173 and accompanying text (outlining action that Congress should take to safeguard the privacy of cell phone users); *see also* S. 2270, 114th Cong. (2015) (as referred to S. Comm. on the Judiciary, Nov. 10, 2015) (establishing a weak consent requirement for phone company's collection of CSLI).

[20] *See infra* notes 25–116 and accompanying text.

[21] *See infra* notes 117–159 and accompanying text.

[22] *See infra* notes 165–173 and accompanying text.

[23] *See infra* notes 174–177 and accompanying text.

[24] *See infra* notes 178–201 and accompanying text.

I. EXPECTATIONS OF PRIVACY AND THEIR APPLICATION TO CSLI ACQUISITION AND USE

Over the past century, the U.S. Supreme Court has changed its views of Fourth Amendment protections to comport with advances in surveillance technology.[25] This Part provides an introduction to Fourth Amendment jurisprudence, to § 2703 of the SCA, and to the third party doctrine.[26] Section A of this Part examines the Fourth Amendment's warrant requirement and the evolution of Fourth Amendment jurisprudence.[27] Section B introduces the third party doctrine, which is a special exception to the Fourth Amendment warrant requirement.[28] Section C discusses the legislative response to government surveillance.[29] Section D examines enacted and pending legislation applicable to the discussion of historical CSLI.[30] Section E describes how the government obtains historical CSLI and uses that information at trial.[31]

A. "And No Warrants Shall Issue, but upon Probable Cause": The Fourth Amendment Warrant Requirement

The Fourth Amendment provides the American people with a fundamental right to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures.[32] To protect this right, the Amendment requires law enforcement to acquire a warrant from a neutral magistrate prior to conducting a search or seizure in most cases.[33] Warrants issue in accordance with the Fourth Amendment only when law enforcement swears or affirms that probable cause exists for the requested search or seizure.[34] In addition to meeting the probable cause requirement, a valid warrant must describe with particu-

---

[25] *Compare* United States v. Jones, 132 S. Ct. 945, 952 (2012) (combining trespass theory with ideas of reasonableness annunciated by the Supreme Court in the late 1960s), *with* Olmstead v. United States, 277 U.S. 438, 457, 466 (1928) (rejecting Fourth Amendment protection for wiretap subject on trespass theory).

[26] *See infra* notes 22–112 and accompanying text.

[27] *See infra* notes 32–55 and accompanying text.

[28] *See infra* notes 56–72 and accompanying text.

[29] *See infra* notes 73–88 and accompanying text.

[30] *See infra* notes 89–98 and accompanying text.

[31] *See infra* notes 99–116 and accompanying text.

[32] *See* U.S. CONST. amend. IV ("[N]o 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.").

[33] *Id.*; *see* Florida v. Jimeno, 500 U.S. 248, 251 (1991) (recognizing a consent exception to the warrant requirement in the context of vehicle searches); Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971) (holding that searches conducted without prior judicial approval are unreasonable under the Fourth Amendment).

[34] U.S. CONST. amend. IV; *see* Griffin v. Wisconsin, 483 U.S. 868, 877 (1987) (holding that when a warrant is required, probable cause is required as well).

larity the place to be searched and the people or items that the police seek to seize.[35]

Courts have recognized several exceptions to the Fourth Amendment warrant requirement.[36] Generally, the Fourth Amendment does not require a warrant for searches that society views as reasonable.[37] More specifically, the warrant requirement does not apply when the subject of a search consents, when exigent circumstances are present, when illegal items are in plain view of law enforcement, and when law enforcement conducts a search incident to arrest.[38] Warrantless searches that do not fall under one of these excepted categories are unconstitutional under the Fourth Amendment.[39]

Under the exclusionary rule, the government generally cannot introduce evidence at trial that it obtained through an unlawful search.[40] By disallowing unlawfully obtained evidence, the exclusionary rule aims to deter future unlawful police conduct, and thereby bolsters the Fourth Amendment's guarantee against unreasonable searches and seizures.[41] In keeping with the deterrent

---

[35] U.S. CONST. amend. IV; *see Coolidge*, 403 U.S. at 455, 467 (noting that the Fourth Amendment addresses the revolutionary-era concern about government agents rummaging through personal belongings by requiring that a warrant particularly describe the items to be seized and recognizing that technological developments "have made the values served by the Fourth Amendment more, not less, important").

[36] *See* Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) (describing the plain-view doctrine, by which officers can legally seize an object if they have lawful access to the object and if they view it from a position where they are lawfully situated); *Jimeno*, 500 U.S. at 251 (approving consent searches); Maryland v. Buie, 494 U.S. 325, 334 (1990) (holding that a subject may be searched without a warrant if the search occurs incident to arrest and the officer seeks to protect his or her own safety or safeguard evidence from destruction).

[37] *See* Harris v. United States, 331 U.S. 145, 150–51 (1947) (observing that law enforcement may conduct some searches and seizures, including searches incident to arrest, without a warrant); Carroll v. United States, 267 U.S. 132, 147 (1925) (holding that the Fourth Amendment only bars unreasonable searches and seizures).

[38] *See* Brigham City, Utah v. Stuart, 547 U.S. 398, 400 (2006) (concluding that police can enter a home without a warrant in the exigent circumstance raised by their reasonable belief that an occupant is seriously injured or threatened with serious injury); *Dickerson*, 508 U.S. at 375 (establishing plain-view exception); *Jimeno*, 500 U.S at 251 (providing for consent exception); *Buie*, 494 U.S. at 334 (recognizing exigent circumstances exception).

[39] *See* Welsh v. Wisconsin, 466 U.S. 740, 749–50 (1984) (implying that, absent the presence of an excepted circumstance, warrantless searches are *per se* unreasonable); Steagald v. United States, 451 U.S. 204, 211 (1981) (noting that without consent or exigent circumstances, searches are presumptively unreasonable and require a warrant).

[40] *See, e.g.*, Illinois v. Krull, 480 U.S. 340, 347 (1987) (holding that the exclusionary rule precludes use of evidence obtained through an illegal search); United States v. Calandra, 414 U.S. 338, 347 (1974) (explaining that under the exclusionary rule, the government cannot use illegally obtained evidence at trial); Mapp v. Ohio, 367 U.S. 643, 648, 650 (1961) (incorporating the exclusionary rule to the states). *But see* United States v. Leon, 468 U.S. 897, 919 (1984) (establishing an exception to the exclusionary rule when law enforcement believes in good faith that it is conducting a legal search).

[41] *Calandra*, 414 U.S. at 347 (explaining that the purpose of the exclusionary rule is to secure Fourth Amendment rights by deterring unlawful police conduct); *Mapp*, 367 U.S. at 648 (noting deterrent effect of exclusionary rule).

purpose of the exclusionary rule, the Supreme Court has recognized that the rule does not operate when law enforcement violates the Fourth Amendment through good-faith reliance on a faulty warrant.[42] Both the Fourth Amendment and the exclusionary rule remedy are enforceable at the state level.[43]

Over the past century, the Court's Fourth Amendment jurisprudence has reflected varying degrees of judicial concern for individual privacy.[44] The Court's conception of Fourth Amendment protections first expanded, but then narrowed during the latter half of the twentieth century.[45] Prior to the late 1960s, the Supreme Court had emphasized that searches involving physical trespass against a person or his or her property violated the Fourth Amendment.[46]

In 1967, in *United States v. Katz*, the Supreme Court supplemented the physical trespass doctrine by holding that the Fourth Amendment protects individual privacy.[47] The majority opinion written by Justice Stewart left unanswered the critical question of precisely when a search that invaded individual privacy required law enforcement to obtain a warrant based on probable cause.[48] Instead, to determine when the Fourth Amendment mandates that law enforcement procure a search warrant, courts apply the reasonableness test established in Justice Harlan's concurrence in *Katz*: a person must have "ex-

---

[42] *See Leon*, 468 U.S. at 919 (recognizing good faith exception to exclusionary rule). In 1984, in *United States v. Leon*, the Supreme Court determined that the exclusionary rule has no deterrent effect against officers who acted in good-faith reliance on a warrant, and therefore ruled that the rule should not be applied in cases when such good-faith reliance occurred. *Id.* at 919–20.

[43] *Mapp*, 367 U.S. at 655. In 1961, in *Mapp v. Ohio*, the Supreme Court held that the exclusionary rule is enforceable against the states through the Fourteenth Amendment because the rule is essential to a scheme of ordered liberty. *Id.*

[44] *Compare* Kyllo v. United States, 533 U.S. 27, 40 (2001) (augmenting the trespass theory with the reasonable expectation of privacy doctrine), *and* Katz v. United States, 389 U.S. 347, 351 (1967) (determining that the Fourth Amendment "protects people, not places"), *with Olmstead*, 277 U.S. at 457, 466 (holding that because a wiretap did not constitute physical trespass, no Fourth Amendment violation occurred), *and* Boyd v. United States, 116 U.S. 616, 630 (1886) (linking Fourth Amendment protections to the sanctity of a person's home and private property).

[45] *Compare Katz*, 389 U.S. at 351 (announcing the rule of reasonableness by holding that "the Fourth Amendment protects people, not places"), *with Olmstead*, 277 U.S. at 457, 466 (affirming the trespass theory of Fourth Amendment jurisprudence by ruling that a warrantless wiretap does not constitute a Fourth Amendment violation).

[46] *See Olmstead*, 277 U.S. at 457, 466 (refusing to recognize a warrantless wiretap as a Fourth Amendment violation); Gouled v. United States, 255 U.S. 298, 305 (1921) (focusing on the unreasonable nature of searching a home or office without a warrant); *Boyd*, 116 U.S. at 630 (emphasizing the Fourth Amendment's protection of home and private property).

[47] *See Katz*, 389 U.S. at 353 (holding that the government violated the expectation of privacy on which the defendant reasonably relied when it listened to his conversation in a closed telephone booth).

[48] *Id.* at 352; *see* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 821 (2004) (noting that Justice Stewart's opinion does not set out a test to determine when the Constitution requires law enforcement to obtain a warrant).

hibited an actual (subjective) expectation of privacy," and that expectation must be one that "society is prepared to recognize as reasonable."[49]

The Supreme Court today recognizes that law enforcement may violate the Fourth Amendment through physical trespass or through activity that infringes on a person's objective expectation of privacy.[50] *Katz*'s progeny recognize the threat that technological advances pose to individuals.[51] Some of these decisions invoke Fourth Amendment protections by combining the rule of reasonableness with trespass theory.[52] In two such Supreme Court cases, *Kyllo v. United States* and *United States v. Karo*, law enforcement used invasive technology to gain information about the interior of the defendants' homes.[53] The Court determined in each case that the government violated the defendant's reasonable expectation of privacy by affecting a functional trespass against him through the intrusive use of technology.[54] The Court ruled in both cases that the government could not track an individual within his or her home without a warrant.[55]

B. Voluntary Exposure: The Third Party Doctrine

Prior to *Katz*, the Supreme Court established that individuals do not retain a legitimate expectation of privacy in information that they voluntarily convey

---

[49] Bond v. United States, 529 U.S. 334, 340–41 (2000) (Breyer, J., dissenting) (following Justice Harlan's reasonableness test from *Katz*); California v. Ciraolo, 476 U.S. 207, 211 (1986) (reaffirming the *Katz* reasonableness test as articulated by Justice Harlan); *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (internal quotation marks omitted).

[50] *See Jones*, 132 S. Ct. at 952 (suggesting that the Supreme Court recognizes Fourth Amendment arguments grounded on either trespass theory or the rule of reasonableness); *Kyllo*, 533 U.S. at 31 (determining that a person enjoys greater Fourth Amendment protection within the home); *Katz*, 389 U.S. at 361 (implying that trespass theory remains operative because the rule of reasonableness arises from prior decisions).

[51] *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (observing that new technologies can send reasonable expectations of privacy into flux); *Kyllo*, 533 U.S. at 34 (expressing fear that use of new thermal imaging technology without sensible limitations would diminish the Fourth Amendment's privacy protections); United States v. Karo, 468 U.S. 705, 712 (1984) (determining that the use of emerging technologies involves the Fourth Amendment).

[52] *See Jones*, 132 S. Ct. at 951 (discussing the intimate relationship between the trespass and reasonableness theories); Soldal v. Cook County, Ill., 506 U.S. 56, 66 (1992) (holding that the plain-view exception is applicable only if law enforcement did not engage in a trespass while viewing the contraband).

[53] *See Kyllo*, 533 U.S. at 29 (noting that Department of the Interior agents used a thermal imager to determine whether the defendant was using grow lamps for marijuana within his home); *Karo*, 468 U.S. at 709–10 (explaining that Drug and Enforcement Agency agents used a radio beeper to determine that the defendant placed and maintained a can of drug precursor within his home).

[54] *See Kyllo*, 533 U.S. at 40 (concluding that the use of a thermal imager to obtain otherwise private information about a home invades private space, and accordingly works an unreasonable search); *Karo*, 468 U.S. at 714–16 (holding that the use of a beeper violates a reasonable expectation of privacy because it reveals information that law enforcement could not gain through unaided observation from outside the curtilage of a home).

[55] *Kyllo*, 533 U.S. at 40; *Karo*, 468 U.S. at 714–15.

to third parties.[56] The Court later applied the *Katz* standard to third party disclosures.[57] Specifically, the Court found that individuals have a diminished expectation of privacy when they voluntarily convey information to third parties.[58] By making a voluntary disclosure to a third party, a person assumes the risk that the third party will, in turn, disclose that information to the government.[59]

With its landmark 1979 decision in *Smith v. Maryland*, the Supreme Court named and further refined the third party doctrine.[60] *Smith* focused on whether law enforcement could acquire records of the telephone numbers that Smith, the defendant, had dialed from his telephone company without a warrant based on probable cause.[61] Smith's telephone company had allowed the police to place a pen register at the company's offices for the purpose of recording the numbers dialed on Smith's home telephone.[62] At trial in Maryland state court, Smith moved to suppress the numbers that law enforcement collected from the pen register because the police did so without a warrant.[63] The trial court denied Smith's motion on the ground that law enforcement's collection of business records from a third party does not require a warrant based on probable cause to comply with the Fourth Amendment.[64]

Smith appealed to the U.S. Supreme Court, which granted certiorari and affirmed the conviction.[65] The Court held that a person has no legitimate expectation of privacy in information that the person voluntarily surrenders to a

---

[56] *See* Lopez v. United States, 373 U.S. 427, 437–38 (1963) (deciding that no Fourth Amendment violation occurred when the government listened to a conversation between petitioner and a wired informant); On Lee v. United States, 343 U.S. 747, 751–52 (1952) (holding that the government did not violate petitioner's Fourth Amendment rights by listening to a conversation that he had with a wired informant).

[57] *See* Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (observing no objective expectation of privacy in information voluntarily transferred to a third party); United States v. Miller, 425 U.S. 435, 442 (1976) (concluding, based on *Katz*, that the Fourth Amendment does not protect information, such as business records, that someone knowingly exposes to a third party).

[58] *See Smith*, 442 U.S. at 744 (deciding that because Smith's telephone company created a record of the numbers that he dialed in the course of ordinary business, the assumption of risk doctrine applied); *Miller*, 425 U.S. at 442–43 (holding that because bank records are business documents that a person voluntarily transferred to a third party, the person assumed the risk that the bank would share those records with the government).

[59] *Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 442–43.

[60] 442 U.S. at 743–44; Tim Sheehan, Note, *Taking the Third-Party Doctrine Too Far: Why Cell Phone Tracking Data Deserves Fourth Amendment Protection*, 13 GEO. J. L. & PUB. POL'Y 181, 188–89 (2015) (noting that *Smith* recognized a "broad third-party rule").

[61] *Smith*, 442 U.S. at 745–46.

[62] *Id.* at 737. A pen register records dialing information transmitted by telephone but does not capture the contents of any telephone conversation. 18 U.S.C § 3127(3) (2012).

[63] *Smith*, 442 U.S. at 737–38.

[64] *Id.*

[65] *Id.* at 738, 745–46.

third party.[66] The Court observed that telephone users know they must convey the numbers they dial to their phone companies and also know that their phone companies record that information for business purposes.[67] Given the knowledge of these practices that society imputed to Smith, society would view Smith's expectation of privacy in his dialing information as unreasonable.[68] The Supreme Court reasoned that Smith failed Justice Harlan's reasonableness test because he lacked an objective expectation of privacy in his dialing information.[69]

Since the Supreme Court decided *Smith*, third party doctrine jurisprudence has not changed substantially on the federal level.[70] State courts and some federal judges, however, have questioned, and in some cases completely disavowed, the third party doctrine.[71] These judicial pronouncements have led some academic commentators to conclude that the Supreme Court will have to reconsider the third party doctrine in the near future.[72]

---

[66] *Id.* at 738, 743–45.

[67] *Id.* at 743; *see* Ryan Merkel, Note, *Playing Hide and Seek with Big Brother: Law Enforcement's Use of Historical and Real Time Mobile Device Data*, 35 N. ILL. U. L. REV. 429, 437–38 (2015) (noting that the defendant in *Smith* assumed the risk that his phone company would turn over his dialing information to the government because he voluntarily exposed that information to the phone company).

[68] *Smith*, 442 U.S. at 743. Some commentators think that the Supreme Court should have formulated the third party doctrine as an issue of consent. *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588–89 (2009) (arguing that disclosures to third parties do not waive reasonable expectations of privacy, but rather take the form of consent to searches that are unreasonable).

[69] *Smith*, 442 U.S. at 743; *see* Sheehan, *supra* note 60, at 188–89 (observing that because Smith knew that his telephone company recorded the number that he dialed, he had no subjective expectation of privacy in his dialing information).

[70] *See* Kerr, *supra* note 68, at 569 (noting that the Supreme Court decided its final case on the third party doctrine in 1980).

[71] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (suggesting that new technologies may necessitate judicial reconsideration of the third party doctrine); Tracey v. State, 152 So. 3d 504, 522–23 (Fla. 2014) (declining to apply the third party doctrine to case involving transmission of a defendant's CSLI from his phone company to the government because the defendant could not reasonably be construed to have voluntarily transmitted his CSLI to the phone company); Commonwealth v. Augustine, 4 N.E.3d 846, 859 (Mass. 2014) (concluding on state constitutional grounds that technological developments have rendered the third party doctrine obsolete).

[72] *See, e.g.*, Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 51 (2011) (predicting that lower court cases and technological advances will cause the Supreme Court to overturn the third party doctrine if a case involving the doctrine reaches the Court); Shaun B. Spencer, *The Aggregation Principle and the Future of Fourth Amendment Jurisprudence*, 41 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 289, 291 (2015) (reasoning that because judicial decisions on the third party doctrine in the lower courts have been more at odds with each other since the Supreme Court's *Jones* decision, a national movement to update the third party doctrine may gain traction).

C. Congress Responds to Increased Government Surveillance: The Omnibus Crime Control and Safe Streets Act of 1968 and Its Progeny

Emerging surveillance technology inspired Congress to enact privacy protections in addition to those that the Supreme Court provided through its ruling in *Katz*.[73] Congress reacted to expansive government use of listening devices in the *Katz* era by passing the Omnibus Crime Control and Safe Streets Act of 1968 ("Wiretap Act").[74] The Wiretap Act, as amended in 1986, prevents the government from intercepting voice communications transmitted over a common carrier without first obtaining a court order.[75]

A law enforcement agent seeking such an order, which is the functional equivalent of a warrant, must apply in writing and under oath to a judge responsible for the territorial jurisdiction in question.[76] The application must contain particularized facts about the communication that the agent seeks to intercept.[77] Upon review of the agent's application, the judge may issue an order under the Wiretap Act if the agent's application meets one of four conditions.[78] Two of these conditions call for a finding of probable cause.[79] By requiring both particularized facts and a finding of probable cause to obtain a

---

[73] *See* 18 U.S.C. § 2511 (2012) (responding to *Katz* by instituting a probable cause requirement for wiretaps); H.R. REP. NO. 99-647, at 17–18 (1986) (expressing Congress's concern about emerging surveillance technologies). The *Chicago Tribune* reported in 1965 that the Senate Judiciary Subcommittee on Administrative Practice and Procedure found that the government could place a listening device in a martini olive. William Moore, *Snoopers Can 'Bug' Olive in Martini, Probers Learn*, CHI. TRIB., Feb. 19, 1965, § 1, at 4.

[74] *See* 18 U.S.C. § 2511; H.R. REP. NO. 99-647, at 17–18 (explaining Congress's decision to enact the Wiretap Act in response to modern surveillance technologies and practices).

[75] 18 U.S.C. § 2518 (2012); H.R. REP. NO. 99-647, at 17. *But see* Hutton v. Woodall, 70 F. Supp. 3d 1235, 1240 (D. Colo. 2014) (finding § 2511(1)(a) of the Omnibus Crime and Safe Streets Act unconstitutional as applied to a purely local communication that never implicated interstate commerce).

[76] 18 U.S.C. § 2518(1).

[77] *Id.* § 2518(1)(b).

[78] *Id.* § 2518(3). These conditions include:

> (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

Id. § 2518(3)(a)–(d).

[79] *Id.* § 2518(3)(a)–(b), (d).

Wiretap Act court order, Congress reemphasized the constitutional warrant requirement for federal law enforcement agencies' wiretaps.[80]

The advent of electronic communications independent of common carriers enabled law enforcement to circumvent the Wiretap Act's Fourth Amendment protections by the mid-1980s.[81] To safeguard the public against unauthorized interception of private electronic communications, Congress amended title III of the Wiretap Act in 1986.[82] The amendment, the SCA, established procedures that provide judicial oversight for government surveillance of electronic communications.[83] Congress explicitly intended for the SCA to govern cellular telephone communications.[84]

The SCA provides less protection to cell phone users than the Wiretap Act provides to landline users.[85] Significantly, § 2703 of the SCA does not require law enforcement to show probable cause when an agency seeks to obtain a cellular customer's communications or records.[86] Instead, the SCA requires law enforcement to secure a court order based on a showing of specific and articulable facts demonstrating reasonable grounds to think that the requested records are germane to an ongoing criminal inquiry.[87] Congress explained that the SCA represents a balance between law enforcement interests and the individual's expectation of privacy, indicating that Congress intended to lower the justification required for a § 2703 order from one of probable cause to one of specific and articulable facts.[88]

---

[80] *See* U.S. CONST. amend. IV (requiring probable cause for a warrant to issue); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 24–25 (2004) (explaining that the Wiretap Act drafters sought to accommodate Supreme Court precedent by requiring a Fourth Amendment probable cause standard for law enforcement to conduct wiretaps).

[81] *See* S. REP. NO. 99-541, at 2–3 (1986) (observing that developments in surveillance technology required new legislation ensuring that citizens could continue to enjoy Wiretap Act privacy protections).

[82] *See* 18 U.S.C. §§ 2701, 2703 (2012); S. REP. NO. 99-541, at 1 (declaring that Congress drafted the Stored Communications Act to safeguard personal privacy).

[83] 18 U.S.C. § 2703; *see* 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, 1208 n.1 (2004) (noting that commentators refer to Title II of the Electronic Communications Privacy Act as the Stored Communications Act).

[84] S. REP. NO. 99-541, at 2–3; H.R. REP. NO. 99-647, at 20–21.

[85] *Compare* 18 U.S.C. § 2703 (allowing a court order to issue on a showing of specific and articulable facts), *with id.* § 2518 (requiring a warrant based upon a showing of probable cause).

[86] *See id.* § 2703(d) (lacking a probable cause requirement).

[87] *Id.*

[88] *See* S. REP. NO. 99-541, at 5 (discussing the balance that Congress intended to institute through its enactment of § 2703).

D. Probable Cause and Voluntariness: Congressional Efforts to Protect Cell Phone Users' CSLI

As the Third Circuit Court of Appeals articulated in *In re U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government* in 2010, it is Congress's role to adjust § 2703 after weighing citizens' privacy concerns and law enforcement authorities' legitimate requirements.[89]

Senators and members of Congress partially responded to the rulings of the Third, Fifth, and Eleventh Circuit Courts of Appeals by introducing the Electronic Communications Privacy Act Amendments Act of 2015 ("ECPAAA") in both houses of Congress.[90] The ECPAAA institutes a probable cause requirement for governmental entities seeking to compel an electronic communication service provider, such as a telephone company, to disclose the content of a message.[91] Notably, the ECPAAA does not provide guidance to the courts regarding CSLI because the Act does not state whether Congress considers CSLI to be content or simply routing material.[92] At the time of this writing, the ECPAAA was under consideration by both the Senate Judiciary Committee and the House Committee on Crime, Terrorism, Homeland Security, and Investigations.[93]

---

[89] 620 F.3d at 319. The Fifth and Eleventh Circuits largely agreed with the Third Circuit, stressing that only Congress can change historical CSLI court order requirements. *See Davis*, 785 F.3d at 512 (reminding litigants that only Congress can change the SCA); *In re Historical Cell Site Data*, 724 F.3d at 614 (holding that the SCA comprises an appropriate response to emerging technology); *Reforming the Electronic Communications Privacy Act: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 30 (2015) [hereinafter *Reforming the ECPA Hearing*] (opening statement of Sen. Grassley, Chairman, S. Comm. on the Judiciary) (noting that Congress must strike a balance between the needs of law enforcement and privacy interests).

[90] *See* S. 356, 114th Cong. (2015) (as referred to S. Comm. on the Judiciary, Feb. 4, 2015) (adding a probable cause requirement for acquisition of message content); H.R. 283, 114th Cong. (2015) (as referred to H. Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations) (requiring law enforcement to have a probable cause warrant before obtaining message content from a service provider). Members of Congress introduced, but failed to pass, legislation similar to the ECPAAA in both 2012 and 2013. Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013); Electronic Communications Privacy Act Modernization Act of 2012, H.R. 6339, 112th Cong. (2012).

[91] S. 356 § 3(a); H.R. 283 § 3(a).

[92] *See* S. 356 (lacking specific language regarding application to historical CSLI); H.R. 283 (failing to address whether bill considers historical CSLI to be message content); S. REP. NO. 113-34, at 14 (2013) (noting that in an identical version of the ECPAAA introduced in the 113th Congress, Congress did not take a position as to whether the Act would require law enforcement to show probable cause before obtaining a § 2703 court order).

[93] *All Bill Information (Except Text) for S.356—Electronic Communications Privacy Act Amendments Act of 2015*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/senate-bill/356/all-info [https://perma.cc/P4BH-X9RP]; Congress, *All Bill Information (Except Text) for H.R.283—Electronic Communications Privacy Act Amendments Act of 2015*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/house-bill/283/all-info [https://perma.cc/J7YX-AVAC].

In addition to the ECPAAA, the Senate also is considering the Location Privacy Protection Act of 2015 ("LPPA").[94] The LPPA would require that cell phone users provide affirmative consent before service providers could collect their geolocation information.[95] To protect public safety, the LPPA's drafter, Senator Franken of Minnesota, included several exceptions to this requirement.[96] Like the ECPAAA, Congress has failed to pass the LPPA in multiple sessions.[97] The LPPA also remains under the Senate Judiciary Committee's consideration.[98]

E. Putting It on the Map: Acquiring Historical CSLI and Using CSLI at Trial

Law enforcement obtains historical CSLI through a SCA § 2703 court order that it may later use at trial.[99] In *Davis*, the government applied to a federal magistrate for a § 2703 court order to compel the defendant's cellular service provider, MetroPCS, to disclose historical CSLI associated with the defendant's cellular telephone number.[100] The government limited its request to CSLI from the period beginning August 1, 2010 and ending October 6, 2010.[101] According to the Eleventh Circuit sitting en banc, no party disputed that the government met the § 2703 court order standard by submitting specific and articulable facts establishing reasonable grounds to believe that Davis's historical

---

[94] S. 2270, 114th Cong. (2015) (as referred to S. Comm. on the Judiciary, Nov. 10, 2015).

[95] *See id.* § 3(a)–(b) (requiring cell phone service providers to obtain affirmative consent from subscribers before collecting their geolocation information). The LPPA defines geolocation information as information sufficient to ascertain the physical address of a device. *Id.* § 3(a).

[96] *See id.* § 3(b)(2)(C) (including public safety exceptions to the LPPA's general consent requirement); Bradley W. Guyton, *Updated Location Privacy Protection Act Introduced*, PRIVACY & SEC. L. BLOG (Apr. 3, 2014), http://www.privsecblog.com/2014/04/articles/marketing-and-consumer-privacy/updated-location-privacy-protection-act-introduced/ [https://perma.cc/X5WB-8VPV] (reporting that Senator Franken sought to protect public safety by including exceptions to the LPPA's consent requirement when he wrote the Act).

[97] S. 2171, 113th Cong. (2014) (as reported to S. Comm. on the Judiciary, Mar. 27, 2014); S. 1223, 112th Cong. (2012) (as reported by S. Comm. on the Judiciary, Dec. 17, 2012).

[98] *All Bill Information (Except Text) for S. 2270 - Location Privacy Protection Act of 2015*, CONGRESS.GOV, https://www.congress.gov/bill/114th-congress/senate-bill/2270/all-info [https://perma.cc/DND7-LXVH].

[99] *See Graham I*, 796 F.3d at 343–44 (noting that the government acquired the defendant's historical CSLI pursuant to a § 2703 court order); *Davis*, 785 F.3d at 502 (stating that the government obtained a § 2703 court order before acquiring the defendant's historical CSLI).

[100] *See* Order for Stored Cell Site Information at 1, United States v. Reid, et. al, No. 1:10-cr-20896 (S.D. Fla. Jan. 27, 2012), ECF No. 266-1 (noting that the government requested an order for the defendant's historical CSLI).

[101] *Id.* at 2. This time interval corresponded to the period during which Davis committed the crimes for which he was charged. *See Davis*, 785 F.3d at 500 (stating that the government charged the defendant with a series of crimes that were committed between August and October 2010).

CSLI would be material to an ongoing criminal investigation.[102] The federal magistrate issued the § 2703 order and MetroPCS complied.[103]

At trial in *Davis* and in *Graham*, the government used the historical CSLI that the defendants' cellular providers disclosed to place the defendants at the scenes of several of the armed robberies for which the juries later convicted them.[104] In *Davis*, a custodian of records for MetroPCS first testified that the company created and retained toll records encompassing CSLI during the normal course of business.[105] The custodian also explained some cellular network basics; he stated that each cellular tower had a range of one-and-a-half miles and had a coverage area that is broken into either three or six sectors.[106] After the MetroPCS custodian provided his introduction to cellular network operations, the government called a detective from the Miami-Dade Police Department to interpret evidence maps that he had created using Davis's CSLI.[107] The detective noted that during the time of the robberies, cell towers in the areas where the robberies occurred routed calls placed and received by Davis and his co-conspirators.[108] The government relied on this information to argue that Davis was at least near the robbery locations when the robberies happened.[109]

Davis, Graham, and their attorneys recognized the damaging nature of the government's historical CSLI evidence prior to Davis and Graham's respective trials.[110] Before their trials, Graham and Davis moved to suppress the historical CSLI that the government obtained by § 2703 orders on the ground that the government conducted a search under the Fourth Amendment when it obtained

---

[102] *Davis*, 785 F.3d at 502.

[103] *Id.* at 500, 502; Order for Stored Cell Site Information, *supra* note 100, at 1–2. MetroPCS provided the government with information including the date, time, and length of Davis's calls; the cell tower that connected each call that Davis placed and received; and the sector of the cell tower's coverage area in which Davis was located during each call. *Davis*, 785 F.3d at 500, 502.

[104] *Graham I*, 796 F.3d at 351; *Davis*, 785 F.3d at 504.

[105] *Davis*, 785 F.3d at 503. The government likely elicited testimony on MetroPCS's collection of CSLI as a business record both to avoid the hearsay bar and to present or preserve a third party doctrine argument under *Smith*. *See* 442 U.S. at 743–44 (applying third party doctrine to business records); *Davis*, 785 F.3d at 511–12 (noting that a MetroPCS custodian of records testified as to the fact that MetroPCS collects historical CSLI as a business record).

[106] *Davis*, 785 F.3d at 503. Additionally, the custodian acknowledged that the coverage range of any tower in an urban location such as Miami could be smaller than that of a typical tower, but did not provide a specific coverage range of an ordinary urban tower. *Id.*

[107] *Id.* at 504.

[108] *Id.*

[109] *Id.* at 502.

[110] *See* Defendant Davis's Motion to Suppress Electronic Location Evidence at 1, United States v. Davis, No. 1:10-cr-20896 (S.D. Fla. Jan. 29, 2012), ECF No. 272 (seeking to exclude defendant's historical CSLI from admission at trial); Motion to Suppress Tangible and Derivative Evidence - Cellphone Data and Historical Cell Site Location Data at 1, United States v. Graham, No. 1:11-cr-00094 (D. Md. July 28, 2011), ECF No. 38 (arguing for exclusion of defendant's historical CSLI at trial).

their CSLI.[111] The court in each case denied the defendant's motion, allowing the prosecution to introduce the CSLI.[112] At least in part on the basis of Davis's historical CSLI, the jury convicted Davis of seven armed robberies.[113]

Appeals in cases that turn on suppression or allowance of historical CSLI evidence such as *Davis* frequently focus on the constitutionality of § 2703.[114] Davis adhered to this pattern by arguing on appeal that the SCA's lack of a probable cause requirement rendered the Act unconstitutional as applied to his case.[115] Additionally, Davis contended on appeal that applying the third party doctrine to his case violated his Fourth Amendment rights against unreasonable search and seizure.[116]

II. Searches and Voluntary Conveyance: The Views of the Federal Courts of Appeals

Five federal Courts of Appeals have ruled on the issue of whether the government violates a criminal defendant's Fourth Amendment rights when law enforcement obtains historical CSLI with a § 2703 court order instead of with a warrant based on probable cause.[117] All five Courts of Appeals held that the Fourth Amendment allows acquisition of historical CSLI through the § 2703 process.[118] One Court of Appeals panel, which was later overruled en

---

[111] Defendant Davis's Motion to Suppress Electronic Location Evidence, *supra* note 110, at 8; Motion to Suppress Tangible and Derivative Evidence, *supra* note 110, at 4.

[112] Order Denying Defendants' Motion to Suppress Evidence at 2, United States v. Graham, No. 1:11-cr-00094 (D. Md. Mar. 1, 2012), ECF. No. 84; Order Denying Defendant's Motion to Suppress Electronic Location Evidence, United States v. Davis, No. 10-20896 (S.D. Fla. Jan. 31, 2012), ECF No. 276.

[113] *Davis*, 785 F.3d at 505; Jury Verdict, *supra* note 1, at 1–5.

[114] *See Graham I*, 796 U.S. at 342–43, 351 (probing the defendant's argument that § 2703 is unconstitutional and that he has a reasonable expectation of privacy in his CSLI); *Davis*, 785 F.3d at 505.

[115] *Davis*, 785 F.3d at 505.

[116] *Id.*

[117] *See* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) (deciding that the government did not conduct an unreasonable search by acquiring the defendant's historical CSLI); United States v. Graham (*Graham I*), 796 F.3d 332, 344 (4th Cir. 2015), *aff'd on reh'g*, 824 F.3d 421, 421 (4th Cir. 2016) (en banc) (*Graham II*) (determining that the government violated the Fourth Amendment when it obtained the defendant's historical CSLI using a § 2703 court order); United States v. Davis, 785 F.3d 498, 500–01 (11th Cir.) (en banc), *cert. denied*, 136 S. Ct. 479 (2015) (holding that the defendant's Fourth Amendment right against unlawful search and seizure was not violated when the government acquired his historical CSLI with a § 2703 court order); *In re* Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (observing that the government constitutionally obtained the defendant's historical CSLI when it applied for and received a § 2703 court order); *In re* Order Directing a Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010) [hereinafter *Elec. Commc'n Serv.*] (approving the use of a § 2703 court order to acquire the defendant's historical CSLI).

[118] *Graham II*, 824 F.3d at 424; *Davis*, 785 F.3d at 500; *In re Historical Cell Site Data*, 724 F.3d at 613; *Elec. Commc'n Serv.*, 620 F.3d at 313. The Eleventh Circuit in *United States v. Davis* and the Fifth Circuit in *In re Historical Cell Site Data* expressly held that cell phone users do not have a rea-

banc, determined that law enforcement acquisition of historical CSLI under § 2703 is an unreasonable search and that the third party doctrine does not apply to historical CSLI.[119] This Part discusses the views of the federal Courts of Appeals on the topic of whether the Fourth Amendment requires probable cause for historical CSLI acquisition.[120] Section A discusses the reasoning of the courts that held specific and articulable facts searches consistent with the Fourth Amendment.[121] Section B presents the Fourth Circuit panel's determination that such searches should be unconstitutional.[122]

A. When Is a Search Unreasonable? The Courts of Appeals on Expectations of Privacy and Trespass Doctrine

The Courts of Appeals diverge in their views of whether law enforcement conducts an unreasonable search when it acquires historical CSLI through the § 2703 process that requires a lower constitutional justification than probable cause.[123] Four federal Courts of Appeals and some academic commentators posit that law enforcement conducts a reasonable search under the Fourth Amendment when it obtains historical CSLI through a § 2703 order.[124] To begin their analysis, these courts either explicitly noted or alluded to the fact

---

sonable expectation of privacy in their historical CSLI and that even if they did have such an expectation, they forfeit it by voluntarily conveying CSLI to their phone companies. *Davis*, 785 F.3d at 511; *In re Historical Cell Site Data*, 724 F.3d at 613–14. In *In re Order Directing a Provider of Electronic Communication Services to Disclose Records to the Government*, the Third Circuit did not reach the third party question, but dispensed with a probable cause requirement for CSLI collection in favor of the specific and articulable facts standard in § 2703. 620 F.3d at 313.

[119] *Graham I*, 796 F.3d at 344–45.

[120] *See infra* notes 123–159 and accompanying text.

[121] *See infra* notes 123–132 and accompanying text.

[122] *See infra* notes 133–159 and accompanying text.

[123] *Compare Graham I*, 796 F.3d at 344–45 (holding that the government conducts an unreasonable search when it allows law enforcement to procure historical CSLI without a warrant), *with Davis*, 785 F.3d at 518 (determining that a search did not occur when law enforcement accessed the defendant's historical CSLI by § 2703 order), *and Elec. Commc'n Serv.*, 620 F.3d at 319 (enabling magistrates to require a warrant should the privacy interests of the defendant outweigh the government's need for the historical CSLI).

[124] *See Graham II*, 824 F.3d at 424; *Davis*, 785 F.3d at 500; *In re Historical Cell Site Data*, 724 F.3d at 615; *Elec. Commc'n Serv.*, 620 F.3d at 313; M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1457 (2007) (arguing that no search occurs when law enforcement obtains CSLI that tracks a subject outside of a residence or private place); Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1787–88 (2009) (noting the argument that law enforcement conducts a reasonable search by obtaining historical CSLI by court order because historical CSLI provides no greater level of surveillance than officers could conduct with their own senses). Analogizing to the Supreme Court's 1976 decision in *United States v. Miller*, at least one practitioner has argued that using a cell phone is just as voluntary an action as the one that Miller took when he used the banking system. 425 U.S. 435, 437 (1976); Clark, *supra*, at 1470–71. Just as the government collected Miller's bank records from his financial institution, so too can the government collect a criminal suspect's historical CSLI from his cellular provider. *Miller*, 425 U.S. at 442–44; Clark, *supra*, at 1470–71.

that the Fourth Amendment only proscribes warrantless searches that are unreasonable.[125] The Fourth, Fifth, and Eleventh Circuits then went on to reason that cell phone subscribers do not have an objectively reasonable expectation of privacy in their historical CSLI.[126] To support this reasoning, the courts determined that the governmental interest in apprehending and punishing the defendants clearly outweighed the personal privacy interest that the defendants had in their historical CSLI.[127]

In addition to applying the reasonableness balancing test, the Fourth, Fifth, and Eleventh Circuits also held that, under a third party doctrine analysis, the defendants had no reasonable expectation of privacy in their historical CSLI.[128] The *Graham II*, *Davis*, and *In re Historical Cell Site Data* courts all determined that historical CSLI is a business record.[129] Then, the courts proceeded to apply the third party doctrine according to their interpretation of *Miller* and *Smith*.[130] In 2013, in *In re Historical Cell Site Data*, the Fifth Circuit decided that cell phone subscribers voluntarily convey their CSLI to their cellular providers, but the Eleventh Circuit did not expressly address the voluntariness pillar of the *Smith* analysis in its *Davis* opinion.[131] The *Graham II*, *Davis*,

---

[125] *See Davis*, 785 F.3d at 516 (noting that the Fourth Amendment protects against unreasonable warrantless searches); *In re Historical Cell Site Data*, 724 F.3d at 615 (stating that Fourth Amendment protections extend only to reasonable expectations of privacy); *see also Elec. Commc'n Serv.*, 620 F.3d at 312–13 (declining to decide whether CSLI unreasonably impinges on privacy interests, citing a dearth of facts).

[126] *See Graham II*, 824 F.3d at 428 (holding that suspects have no objectively reasonable expectation of privacy in their CSLI); *Davis*, 785 F.3d at 517–18 (deciding that Davis's expectation of privacy was unreasonable because the government's interest in apprehending him outweighed his interest in personal privacy); *In re Historical Cell Site Data*, 724 F.3d at 614–15 (affirming the balancing of personal privacy and governmental interest that Congress conducted in drafting the SCA as reasonable under the Fourth Amendment).

[127] *Graham II*, 824 F.3d at 428; *Davis*, 785 F.3d at 518; *In re Historical Cell Site Data*, 724 F.3d at 614–15.

[128] *See Graham II*, 824 F.3d at 427 (declining to decide that the defendant had a reasonable expectation of privacy in his historical CSLI); *Davis*, 785 F.3d at 511 (stating that Davis had no objective expectation of privacy in his cell provider's business records); *In re Historical Cell Site Data*, 724 F.3d at 614–15 (holding that by passing § 2703, Congress created a solution, as Justice Alito counseled in *Jones*, that balanced an individual's expectation of privacy in business records with the governmental interest in apprehending criminals).

[129] *Graham II*, 824 F.3d at 427; *Davis*, 785 F.3d at 511; *In re Historical Cell Site Data*, 724 F.3d at 611.

[130] *Graham II*, 824 F.3d at 427; *Davis*, 785 F.3d at 511 (determining that Supreme Court precedent, including *Miller* and *Smith*, compelled the conclusion that the government did not violate the Fourth Amendment when it obtained Davis's historical CSLI with a § 2703 court order); *In re Historical Cell Site Data*, 724 F.3d at 615 (reasoning that, per *Miller*, the phone company owned the defendant's historical CSLI, and, per *Smith*, such routing information is not protected under the Fourth Amendment).

[131] *See Davis*, 785 F.3d at 511–12 (implying that because the telephone user in *Smith* necessarily revealed his location by using a landline, he voluntarily conveyed location information to his telephone company); *In re Historical Cell Site Data*, 724 F.3d at 612 (concluding that cell phone users convey CSLI to their phone companies voluntarily).

and *In re Historical Cell Site Data* courts held that cell phone subscribers have no reasonable expectation of privacy from the government in the CSLI that they transfer to their phone companies.[132]

B. Historical CSLI Collection Without Probable Cause as an Unreasonable Search

The *Graham* panel majority, *Davis* dissent, and many academic commentators disagree with the Fourth, Fifth, and Eleventh Circuits, and instead take the view that law enforcement's historical CSLI collection in the absence of probable cause is an unreasonable search.[133] The *Graham* panel and the *Davis* dissent found that people have an objectively reasonable expectation of privacy in their historical CSLI.[134] The dissent in *Davis* and the *Graham* panel majority also held the third party doctrine inapplicable to government acquisition and inspection of historical CSLI.[135]

Judges who think that historical CSLI collection in the absence of probable cause constitutes an unreasonable search focus on two factors to substantiate their view: the locations at which historical CSLI can place a suspect and the length of time for which the government requests and inspects historical CSLI.[136] Judge Martin, dissenting in *Davis*, expressed her explicit concern that the *Davis* majority had provided the government with a powerful, intrusive tool that could determine a suspect's location with remarkable specificity.[137] For Judge Martin and her colleagues, the ability for historical CSLI to reveal a suspect's patterns of movement is of critical importance because such patterns

---

[132] *Graham II*, 824 F.3d at 428; *Davis*, 785 F.3d at 512, 513; *In re Historical Cell Site Data*, 724 F.3d at 610.

[133] *See Graham I*, 796 F.3d at 344–45 (requiring law enforcement to procure a probable cause warrant to obtain and inspect historical CSLI that covers an extended period of time); *Davis*, 785 F.3d at 541 (Martin, J., dissenting) (determining that because the defendant had an objectively reasonable expectation of privacy in his historical CSLI, a Fourth Amendment violation occurred when law enforcement obtained and inspected it without a warrant); Patrick E. Corbett, *The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait for the Supremes?*, 8 FED. CTS. L. REV. 215, 226 (2015) (arguing that the Supreme Court likely will find the warrantless acquisition of historical CSLI to be a Fourth Amendment violation, but will allow the government to avoid suppression through the use of exclusionary rule exceptions).

[134] *Graham I*, 796 F.3d at 345; *Davis*, 785 F.3d at 541 (Martin, J., dissenting).

[135] *Graham I*, 796 F.3d at 353; *Davis*, 785 F.3d at 538 (Martin, J., dissenting).

[136] *See Graham I*, 796 F.3d at 346–47, 350 (holding that the government violates a person's privacy by viewing CSLI that tracks them to their home and that the government conducts an unreasonable search when it inspects historical CSLI for a period longer than two weeks); *Elec. Commc'n Serv.*, 620 F.3d at 312 (acknowledging the possibility that historical CSLI can resemble a tracking device that reveals a suspect's prior location).

[137] *See Davis*, 785 F.3d at 541–42 (Martin, J., dissenting) (arguing that due to the specificity of the CSLI that the government obtained, Davis had a reasonable expectation of privacy in his CSLI).

can track people to and within their homes.[138] They cite the Supreme Court's decisions in *United States v. Karo*, *Kyllo v. United States*, and *United States v. Jones* to substantiate their view that the Fourth Amendment prohibits law enforcement from placing an individual in his or her home at a certain time.[139]

Additionally, those who think that the government must obtain a warrant based on probable cause in order to access and inspect historical CSLI also take issue with the lengthy time periods for which the government may gain access to historical CSLI under a § 2703 order.[140] One commentator notes that courts must answer two questions: how long a period of surveillance must last to provide intimate details of a suspect's life and the amount of time after which law enforcement would be incapable of conducting the surveillance by conventional means.[141]

Judges generally hesitate to provide a specific answer for the two questions posed above regarding the acceptable length of time for which law enforcement may obtain historical CSLI absent a finding of probable cause.[142] The *Graham* panel, however, responded to both questions by finding that the government violates the Fourth Amendment when it obtains location information not available to the general public that covers a period such as fourteen or 221 days.[143] Like the Fifth and Eleventh Circuits, the *Graham* panel did not provide a floor indicating the time period covered by historical CSLI records that would be acceptable for law enforcement to procure without showing probable cause.[144] One may infer from each of the U.S. Court of Appeals opin-

---

[138] *See Graham I*, 796 F.3d at 346–47 (discussing sanctity of the home); *Davis*, 785 F.3d at 540–41 (Martin, J., dissenting) (noting that historical CSLI could reveal the place where Davis lived and slept).

[139] *Graham I*, 796 F.3d at 346–47 (noting that all information about a suspect within the home is private because the suspect can reasonably expect that information to be free from government surveillance); *Davis*, 785 F.3d at 540–41 (Martin, J., dissenting).

[140] *See Davis*, 785 F.3d at 540–41 (Martin, J., dissenting) (expressing concern that the 11,606 CSLI data points that the government received from a period of sixty-seven days revealed intimate, private details about his habits); *Elec. Commc'n Serv.*, 620 F.3d at 311 (acknowledging that historical CSLI can reveal a person's home to the government); Spencer, *supra* note 72, at 301 (concluding that the aggregation of CSLI presents a new Fourth Amendment challenge that courts must address).

[141] Spencer, *supra* note 140, at 293.

[142] *See Davis*, 785 F.3d at 540 (Martin, J., dissenting) (opining that the sixty-seven days of Davis's historical CSLI that the government obtained was enough to reveal private information about him); *Elec. Commc'n Serv.*, 620 F.3d at 311 (noting, without further detail, that historical CSLI can place a person at his or her home).

[143] *See Graham I*, 796 F.3d at 349–50 (citing *Karo*, *Kyllo*, and *Riley* to substantiate the holding that historical CSLI is not in public use, and as such, law enforcement violates a suspect's reasonable expectation of privacy if CSLI is obtained for an extended period of time); Spencer, *supra* note 140, at 293.

[144] *Graham I*, 796 F.3d at 349–50; *see also Davis*, 785 F.3d at 533 (Martin, J., dissenting) (concluding that the government violated the defendant's Fourth Amendment rights by acquiring sixty-seven days of his CSLI without a warrant); *Elec. Commc'n Serv.*, 620 F.3d at 311 (recognizing only that historical CSLI can reveal private details of a suspect's existence).

ions that hold or would hold acquisition of historical CSLI on a specific and articulable facts standard unconstitutional that any time period that would reveal intimate personal details about a suspect is a period that requires a finding of probable cause.[145]

In addition to concluding that suspects have a reasonable expectation of privacy in their historical CSLI, the *Graham* panel and the *Davis* dissent both vigorously asserted that a suspect could not lose that expectation by operation of the third party doctrine.[146] The *Davis* dissent and the *Graham* panel argued that the third party doctrine is inapplicable to historical CSLI cases for three reasons: people do not voluntarily convey their CSLI to their cellular providers, the Supreme Court has suggested that individuals do not lose their entire expectation of privacy in information that they expose to third parties, and people expose so much information about themselves to their phone companies that they must retain some privacy interest in that information.[147]

The judges who support a probable cause requirement focus on the view that cell phone users involuntarily transmit CSLI, because if such transmissions are involuntary, then the government cannot reasonably acquire them under the Supreme Court's 1979 *Smith v. Maryland* decision.[148] The *Graham* panel and *Davis* dissent observed that cell phone users do not ordinarily enter their location into their phones.[149] The *Graham* panel went further, stating that cell phone users do not even convey location information to their service providers at all because service providers automatically generate CSLI.[150] Without voluntary transmission of CSLI, Judge Davis opined in his *Graham* panel opinion, a suspect never assumes the risk that his or her cellular provider will turn his or her CSLI over to the government, and accordingly maintains a reasonable expectation of privacy in that information.[151]

---

[145] *See Graham I*, 796 F.3d at 348 (holding that long-term CSLI searches implicate privacy interests); *Davis*, 785 F.3d at 533 (Martin, J., dissenting) (expressing concern that the government could access private information about suspects by acquiring their historical CSLI); *Elec. Commc'n Serv.*, 620 F.3d at 311 (noting that the government can access critical information about a suspect's habits by obtaining his or her historical CSLI).

[146] *See Graham I*, 796 F.3d at 353 (concluding that the third party doctrine is inapplicable to the defendant's case); *Davis*, 785 F.3d at 538 (Martin, J., dissenting) (arguing that applying the third party doctrine to the defendant's case is inappropriate due to the advance of technology since the Supreme Court decided *Miller* and *Smith*).

[147] *Graham I*, 796 F.3d at 354–60; *Davis*, 785 F.3d at 534–37 (Martin, J., dissenting).

[148] *Graham I*, 796 F.3d at 353; *Davis*, 785 F.3d at 534 (Martin, J., dissenting); *see* Smith v. Maryland, 442 U.S. 735, 744 (1979) (requiring that the suspect voluntarily transfer information to a service provider for the third party doctrine to apply).

[149] *Graham I*, 796 F.3d at 355; *Davis*, 785 F.3d at 534 (Martin, J., dissenting).

[150] *Graham I*, 796 F.3d at 354.

[151] *Id.*; *see also* Kerr, *supra* note 68, at 588–89 (arguing that courts should center their third party doctrine inquiries on the question of whether defendants consented to release of their private information). Professor Kerr provides a consent-based view of the third party doctrine that is consonant

In addition to their focus on voluntary CSLI transmission, Judges Davis and Martin highlighted intimations from the U.S. Supreme Court that suspects do not surrender their entire privacy interests in the information that they convey to third parties.[152] The judges thought that the Supreme Court sent such signals in cases that protected the contents of letters and packages entrusted to carriers and in a case that protected the contents of a hotel room from a search authorized by the hotel clerk without the permission of the room renter.[153] Noting that people have a reasonable expectation of privacy in their online personae, the *Davis* dissent and the *Graham* panel refused to apply the third party doctrine in the historical CSLI context.[154] Judges Davis and Martin worried that bluntly applying the third party doctrine to law enforcement's requests for historical CSLI would expose an extraordinary amount of private, constitutionally protected information to the government.[155] Remarkably, both judges relied on Justice Sotomayor's concurrence in 2012 in *United States v. Jones*, in which she considered the third party doctrine to be poorly matched to present realities, under which ordinary people convey an extraordinary amount of private information to third parties.[156]

Taken together, Judges Davis and Martin expressed views regarding the acquisition of historical CSLI by law enforcement that contrast diametrically with those of their colleagues in the *Davis*, *In re Historical Cell Site Data*, and en banc-*Graham* majorities.[157] These starkly opposed views are but the most

---

with the *Graham I* court's holding that the government conducts an unreasonable search when it obtains historical CSLI. Kerr, *supra* note 68, at 588–89.

[152] *See Graham I*, 796 F.3d at 357–58 (referencing *Katz* to support reasoning that a person has a Fourth Amendment interest in information that he or she seeks to preserve as private); *Davis*, 785 F.3d at 535 (Martin, J., dissenting) (citing a line of U.S. Supreme Court cases that generate doubt as to the third party doctrine's extent).

[153] *See Graham I*, 796 F.3d at 357–58 (noting that the Supreme Court suggested in *Ex Parte Jackson* that not all information exposed to a third party is open to warrantless inspection by the government); *Davis*, 785 F.3d at 535 (Martin, J., dissenting) (questioning the third party doctrine's breadth due to Supreme Court opinions in *United States v. Jacobsen* and *Stoner v. California*); *see also* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (holding that although packages and letters touch the hands of the postman, who is a third party, the public maintains a reasonable expectation of privacy in the contents of the letters and packages); Stoner v. California, 376 U.S. 483, 487–88 (1964) (determining that a hotel clerk cannot provide valid consent for the search of a patron's hotel room).

[154] *Graham I*, 796 F.3d at 359–60; *Davis*, 785 F.3d at 535–38 (Martin, J., dissenting).

[155] *Graham I*, 796 F.3d at 359–60; *Davis*, 785 F.3d at 535–38 (Martin, J., dissenting).

[156] 132 S. Ct. 945, 957 (2012) (Sotomayor, J. concurring); *Graham I*, 796 F.3d at 360; *Davis*, 785 F.3d at 538 (Martin, J., dissenting); *see* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 3 (2013) (acknowledging that the concurring justices in *Smith* expressed doubts about the third party doctrine's relevance to modern conditions).

[157] *Compare Graham I*, 796 F.3d at 344–45 (holding that an unreasonable search occurs when the government obtains historical CSLI without a warrant), *and Davis*, 785 F.3d at 541 (Martin, J., dissenting) (arguing that the government violated Davis's Fourth Amendment rights when it obtained and inspected his historical CSLI without a warrant because Davis had a reasonable expectation of privacy in that information), *with Graham II*, 824 F.3d at 424 (determining that the government does

recent arguments in a judicial discussion of privacy dating from the events that precipitated the American Revolution.[158] The widely divergent Courts of Appeals opinions on the Fourth Amendment's application to historical CSLI cases leave open for debate at least one existential question regarding the nature and extent of American liberty: how much of the self does society view as so intrinsically private that our fundamental law prevents the government from accessing it at will?[159]

III. THE GOVERNMENT AS THE EVERYMAN: TOWARD A DEFENSIBLE CSLI ACQUISITION REGIME

The *Graham II*, *Davis*, and *In re Historical Cell Site Data* circuit courts applied a version of the third party doctrine that violates the Supreme Court's intention in *Katz v. United States* and *Smith v. Maryland*.[160] By refusing to protect suspects' historical CSLI in spite of a societal expectation of privacy in location information, the Fourth, Fifth, and Eleventh Circuit Courts of Appeals adopted a narrow construction of the Fourth Amendment that the Supreme Court must overturn.[161]

---

not violate the Fourth Amendment by acquiring a defendant's historical CSLI), *and Davis*, 785 F.3d at 511 (concluding that no search occurred because Davis had no reasonable expectation of privacy in his historical CSLI), *and In re Historical Cell Site Data*, 724 F.3d at 613–14 (refusing to hold that the defendant had a reasonable expectation of privacy in his historical CSLI).

[158] *Compare* Thomas K. Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 980 (2011) (identifying assertive British search and seizure operations leading up to the American Revolution as a genesis of the Fourth Amendment), *with* United States v. Rabinowitz, 339 U.S. 56, 60 (1950) (asserting that the Framers would not require a warrant for every search).

[159] *See* Olmstead v. United States, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting) (arguing for a liberal construction of the Fourth Amendment that protects the inner self against government surveillance). In the Supreme Court's 1928 decision in *Olmstead v. United States*, Justice Brandeis quoted *Weems v. United States* when he wrote that "'time works changes, brings into existence new conditions and purposes.'" *Id.* at 473 (quoting Weems v. United States, 217 U.S. 349, 373 (1910)). Specifically, Justice Brandeis warned that "subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." *Id.*

[160] *Compare* Smith v. Maryland, 442 U.S. 735, 743 (1979) (predicating the third party doctrine on an objective expectation of privacy as set out in *Katz*), *and* Katz v. United States, 389 U.S. 347, 361 (1967) (requiring that a suspect have a subjective expectation of privacy for a court to accord his communication Fourth Amendment protection), *with* United States v. Graham (*Graham I*), 796 F.3d 332, 338–39, 342 (4th Cir. 2015), *aff'd on reh'g*, 824 F.3d 421, 421 (4th Cir. 2016) (en banc) (*Graham II*) (declining to hold that a suspect enjoys an objectively reasonable expectation of privacy in his historical CSLI), *and* United States v. Davis, 785 F.3d 498, 500–01 (11th Cir.) (en banc), *cert. denied*, 136 S. Ct. 479 (2015) (holding that a suspect has no objective expectation of privacy in his historical CSLI), *and In re* Historical Cell Site Data, 724 F.3d 600, 610 (5th Cir. 2013) (determining that suspects do not have a reasonable expectation of privacy in their historical CSLI).

[161] *See Graham II*, 824 F.3d at 421 (observing that the defendant did not enjoy a reasonable expectation of privacy in his historical CSLI); *Davis*, 785 F.3d at 512, 513 (recognizing no objective

This Part proposes a two-pronged response to the problem of government acquisition and inspection of historical CSLI without probable cause.[162] Section A advocates for Congress to amend § 2703 by instituting a probable cause requirement for historical CSLI orders and by requiring affirmative consent from cell users before cellular providers generate and record their CSLI.[163] Section B argues that the U.S. Supreme Court should grant certiorari on a historical CSLI case and use the opportunity presented by that case to constitutionalize the requirement that law enforcement obtain a warrant on a showing of probable cause prior to executing a historical CSLI search.[164]

A. By the People and for the People: Congress's Role in Safeguarding Individual Privacy

The Supreme Court and the U.S. Courts of Appeals that have ruled on the issue of law enforcement's acquisition of historical CSLI have suggested that Congress has a responsibility to protect individual privacy.[165] Congress should accept these courts' suggestion and enact amendments to the SCA that protect individuals from government intrusion.[166] Specifically, to ensure that law enforcement must show probable cause as a prerequisite to obtaining a § 2703 order, Congress should modify the ECPAAA and incorporate it into a larger amendment to the SCA.[167] During a hearing on the ECPAAA before the Senate

---

expectation of privacy in historical CSLI); *In re Historical Cell Site Data*, 724 F.3d at 610 (holding that the defendant could not objectively believe that his historical CSLI was private); Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 520 (2012) (explaining that compelling empirical research proves that a majority of the public views an expectation of privacy in CSLI as reasonable, and that the third party doctrine accordingly should be inoperative in historical CSLI cases).

[162] *See infra* notes 165–201 and accompanying text.

[163] *See infra* notes 165–173 and accompanying text.

[164] *See infra* notes 174–201 and accompanying text.

[165] *See* United States v. Jones, 132 S. Ct. 945, 962–64 (2012) (Alito, J. concurring) (suggesting that Congress should protect individual privacy interests in historical CSLI by enacting legislation, as Congress did in the Wiretap Act); *Davis*, 785 F.3d at 512 (concluding that citizens concerned about privacy issues should demand that Congress change the law rather than seek such a change from the judiciary); *In re Historical Cell Site Data*, 724 F.3d at 614 (arguing that the legislature is best suited to gauge societal expectations of privacy and to balance individual privacy interests with public safety concerns).

[166] *See Davis*, 785 F.3d at 512; *In re Historical Cell Site Data*, 724 F.3d at 614; *In re* Order Directing a Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't (*Elec. Commc'n Serv.*), 620 F.3d 304, 319 (3d Cir. 2010) (holding that Congress must balance the privacy and safety concerns surrounding law enforcement access to historical CSLI); Owsley, *supra* note 13, at 47 (concluding that Congress should pass a law that institutes a probable cause requirement for government acquisition of historical CSLI).

[167] *See* S. 356, 114th Cong. (2015) (as referred to S. Comm. on the Judiciary, Feb. 4, 2015); H.R. 283, 114th Cong. (2015) (as referred to H. Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations) (prescribing a probable cause standard for government acquisition of geolocation data); *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance*

Committee on the Judiciary, senators heard both from law enforcement officials concerned that the Act would pose a problem in some crime-fighting situations, and from privacy advocates who strongly supported the Act's probable cause requirement.[168] Congress should include language in the Act that explicitly requires law enforcement to show probable cause before a neutral magistrate may issue an order compelling the production of CSLI.[169]

In addition to prescribing a probable cause standard for historical CSLI acquisition, Congress should act to restrain the Supreme Court's exercise of the third party doctrine with regard to CSLI by requiring that cell service providers obtain affirmative consent from subscribers before collecting their geolocation information.[170] Congress should supplement its amendment to the SCA by including the LPPA alongside the modified ECPAAA.[171] Doing so would protect individual privacy by clearly establishing consent as an affirmative act that requires more than simply turning on one's phone.[172] The legislative language regarding consent contained within the LPPA would provide the judiciary with precisely the guidance for reform of the third party doctrine that Justice Sotomayor implied in 2012 in *United States v. Jones*.[173]

Before the H. Comm. on the Judiciary, 113th Cong. 113–34, at 4 (2013) [hereinafter *ECPA Hearings*] (statement of Representative John Conyers, Jr.) (arguing that Congress must establish a probable cause standard for geolocation data collection).

[168] *Compare Reforming the ECPA Hearing*, *supra* note 89, at 5 (testimony of Elana Tyrangiel, Principal Deputy Assistant Attorney General, U.S. Department of Justice) (urging that Congress consider the situations, such as the civil context, where a warrant requirement may be problematic), *with ECPA Hearings*, *supra* note 167, at 1 (responses of Chris Calabrese, Vice President, Policy, Center for Democracy & Technology, to Written Questions of Senator Patrick Leahy) (expounding the privacy benefits of warrants in the stored electronic communication context).

[169] *See ECPA Hearings*, *supra* note 167, at 4 (opining that the correct standard for government acquisition of geolocation data is probable cause). Representative Conyers argued that citizens have a reasonable expectation of privacy in not allowing the government to track their every movement. *Id.* Additionally, Representative Conyers specifically noted Justice Alito's request in 2012 in *United States v. Jones* for legislation on the proper standard of justification for CSLI acquisition by the government. *Id.*

[170] *See Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy Before the S. Comm. on the Judiciary*, 112th Cong. 112–857, at 4–5 (2011) [hereinafter *Protecting Mobile Privacy Hearing*] (statement of Senator Patrick J. Leahy) (stating that Congress should consider taking action to require communications providers to obtain consent from users before collecting their geolocation data); *see also id.* at 86 (prepared statement of Justin Brookman, Director, Consumer Privacy, Center for Democracy & Technology) (arguing that Congress should institute a warrant requirement for the collection of CSLI by law enforcement because the SCA currently does not protect information collected without a user's consent).

[171] S. 2270, 114th Cong. (2015) (as referred to S. Comm. on the Judiciary, Nov. 10, 2015).

[172] *See id.* (requiring affirmative consent from cell phone users for the collection of their CSLI); *Protecting Mobile Privacy Hearing*, *supra* note 170, at 225 (letter from Senator Al Franken) (evincing Sen. Franken's intent that communications companies obtain affirmative consent prior to collecting location information from their users).

[173] *See* S. 2270 (providing explicit guidance from Congress as to the nature of consent required for government acquisition of historical CSLI); *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (implying that the third party doctrine is outdated and must be updated for the modern age).

B. The Right of the People to Be Secure: The Supreme Court's Duty to Update the Third Party Doctrine for the Digital Age

When Congress acts in violation of the people's rights, or when, by inaction, Congress allows old statutes to work harms that intrude upon constitutional protections, the Supreme Court should exercise its power of judicial review and strike down the offending statute.[174] First, this Note will assert that the Court should update the third party doctrine for the digital age by adopting a new balancing test for voluntariness.[175] Second, this Note will argue that the Court should require a warrant issued on probable cause and subject to existing warrant exceptions if analysis under the new third party doctrine formulation reveals that the subject has an objectively reasonable expectation of privacy in his or her historical CSLI.[176] By striking down § 2703, the Supreme Court will update the third party doctrine for the digital age and will protect the objectively reasonable expectation of privacy that most American cell phone users share.[177]

1. The Government as Everyman, Not Every Man: Updating the Third Party Doctrine for the Digital Age

Reasonable expectations of privacy in information that one shares with a third party change as technology develops.[178] In the pre-digital world, citizens shared information with third parties in a deliberate way.[179] In contrast with the

---

[174] *See* THE FEDERALIST NO. 78, at 463, 466 (Alexander Hamilton) (Clinton Rossiter ed., 2003) (explaining that the Constitution, as the will of the people, should trump statutes because statutes are the work of the people's agents); D. Brooks Smith, *Judicial Review in the United States*, 45 DUQ. L. REV. 379, 390 (2007) (concluding that the Constitution should trump federal statutes contrary to it).

[175] *See infra* notes 186–192 and accompanying text.

[176] *See infra* notes 193–201 and accompanying text.

[177] *See* McAllister, *supra* note 161, at 520 (using statistical analysis to show that the current third party doctrine does not comport with contemporary views of personal privacy); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 641, 649 (2011) (recognizing that the Supreme Court is likely to move away from a blunt application of the third party doctrine and toward a more nuanced approach dependent on social setting).

[178] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (noting that technology has changed societal expectations of privacy such that a blunt application of the third party doctrine no longer conforms to those expectations); *Katz*, 389 U.S. at 352–53 (shifting from a reliance on trespass doctrine to a reliance on reasonable expectations of privacy in response to the advent of electronic eavesdropping technology).

[179] *See Smith*, 442 U.S. at 745 (focusing on Smith's voluntary conveyance of phone numbers to his telephone company); United States v. Miller, 425 U.S. 435, 442 (1976) (noting that the bank documents that the government obtained were composed of information that Miller voluntarily conveyed to his bank).

Smith era, citizens today frequently share a tremendous amount of sensitive information with third parties in transactions that are entirely involuntary.[180]

Historical CSLI is a prime example of such involuntarily transferred private information.[181] Citizens in the modern American republic must own a cell phone to fully participate in society, but to operate a cell phone, a user has no choice but to produce location information and communicate it with their cellular provider.[182] The third party doctrine does not apply to CSLI cases because cell phone users do not voluntarily convey CSLI to their phone companies.[183]

When courts prohibit the government from invoking the third party doctrine to provide Fourth Amendment justification for its warrantless collection of historical CSLI, they should also reject government reliance on trespass or *Katz* reasonableness analyses to accomplish the same end.[184] Given the statistical evidence, judicial rulings, and implication of the home that suggest a strong, objective expectation of privacy in location information, it is likely that the Supreme Court would find such an expectation and would require a warrant if the government seeks to obtain historical CSLI.[185]

---

[180] *See* Riley v. California, 134 S. Ct. 2473, 2492–93 (2014) (expressing concern that searches of cell phones are equivalent to rummaging due to the amount of sensitive information contained within those phones); United States v. Graham (*Graham I*), 796 F.3d 332, 350, 356–57 (4th Cir. 2015), *aff'd on reh'g*, 824 F.3d 421, 421 (4th Cir. 2016) (en banc) (*Graham II*) (observing that the government captured 29,659 data points on the defendant, and concluding that the transmission of CSLI is involuntary).

[181] *See* Brief of Amici Curiae Electronic Frontier Foundation et al. in Support of Affirmance of the District Court at 19–22, *In re* Order Directing a Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227), 2009 WL 3866619 (distinguishing *Smith* and *Miller* from CSLI cases based on the lack of voluntary CSLI transmission); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 732 (2011) (concluding that cell phone users do not create CSLI voluntarily).

[182] City of Ontario, Cal. v. Quon, 560 U.S. 746, 760 (2010) (observing that cell phones are so widespread in American society that they have become an essential tool of modern life); *Graham I*, 796 F.3d at 356 (holding that courts cannot find that a suspect has surrendered his expectation of privacy simply by participating in modern life through the ownership and use of a cell phone).

[183] *See Graham I*, 796 F.3d at 353 (recognizing that the creation and transmission of CSLI is an involuntary activity); *Davis*, 785 F.3d at 534 (Martin, J., dissenting) (declining to apply the third party doctrine because cell phone users involuntarily transfer their CSLI); Freiwald, *supra* note 181, at 733 (observing that cell phone users do not voluntarily create and transfer CSLI).

[184] *See Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (observing that new technologies can send reasonable expectations of privacy into flux); Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that intrusions into the home by technological means are presumptively unreasonable); United States v. Karo, 468 U.S. 705, 717–18 (1984) (deciding that the government conducts an unreasonable search when it tracks a suspect inside his home without a warrant).

[185] *See Jones*, 132 S. Ct. at 950–51 (emphasizing the sanctity of the home); *Graham I*, 796 F.3d at 345 (holding that cell phone subscribers have an objectively reasonable expectation of privacy in their historical CSLI); Corbett, *supra* note 133, at 226 (arguing that the Supreme Court likely will find government collection of historical CSLI pursuant to § 2703 order to be unconstitutional); McAllister, *supra* note 161, at 520 (presenting empirical research suggesting an objective expectation of privacy in historical CSLI).

The Supreme Court should modernize the third party doctrine by dispensing with the notion that an individual loses an objective expectation of privacy in *any* information that he or she voluntarily exposes to a third party.[186] The Supreme Court should instead institute a balancing test predicated on a fulcrum of necessary disclosure.[187] If the subject was forced to reveal the information, or functionally was forced to do so, then courts should find that he or she does not lose his or her objectively reasonable expectation of privacy in the information; if the subject revealed the information for the sake of convenience alone, then courts should find that he or she lost Fourth Amendment protection of the information.[188] By more closely defining the third party doctrine's voluntariness requirement, this balancing analysis would assure that courts allow the government to act not as an omniscient surveillance apparatus, but rather as a typical person to whom a third party betrays a client's confidence.[189]

This test would require a case-by-case analysis to determine whether the subject transferred his or her information to a third party in a truly voluntary manner.[190] The analysis under this theory for historical CSLI cases is relatively simple; transmitting CSLI is required to operate a cell phone, and operating a cell phone is required to fully participate in modern society.[191] Thus, transferring CSLI to a phone company—a functionally involuntary activity—falls on

---

[186] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (suggesting that the third party doctrine should be updated for the digital age); Commonwealth v. Augustine, 4 N.E.3d 846, 863 (Mass. 2014) (holding that CSLI is qualitatively different than the business records in *Smith* and *Miller*, warranting a deviation from the third party doctrine application in those cases); Erin Murphy, *The Case Against the Case for the Third Party Doctrine*, 24 BERKELEY TECH. L.J. 1239, 1252 (2009) (proposing a balancing test based on voluntariness to determine whether a subject loses his or her expectation of privacy by conveying information to a third party).

[187] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (calling for modernization of the third party doctrine); *Graham I*, 796 F.3d at 355–56 (disregarding the notion of voluntary CSLI conveyance upon which the third party doctrine is predicated); Murphy, *supra* note 186, at 1252 (proposing a balancing test to replace the current third party doctrine).

[188] *See* Murphy, *supra* note 186, at 1252 (suggesting an updated third party doctrine).

[189] *See id.* at 1250 (arguing that the Founders feared a surveillance state, and sought to prevent the advent of one by restricting the government's search powers to those that ordinary citizens may employ for private purposes).

[190] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (opining that citizens have a reasonable expectation of privacy in some of the information that they disclose to third parties); *Davis*, 785 F.3d at 535 (Martin, J., dissenting) (noting that the Supreme Court has cast doubt on the notion that citizens always lose a reasonable expectation of privacy in the information that they disclose to third parties); Murphy, *supra* note 186, at 1252 (putting forward an updated third party doctrine predicated on a continuum of disclosure).

[191] *See Graham I*, 796 F.3d at 355–56 (holding that cell phone use is necessary for participation in American culture); *Davis*, 785 F.3d at 535–36 (Martin, J., dissenting) (declining to find a knowing disclosure of CSLI solely through use of a cell phone).

the protected side of the third party doctrine balancing test that this Note proposes.[192]

2. No Warrants Shall Issue, but upon Probable Cause: A Return to Reasonableness

If the Supreme Court reforms the third party doctrine as this Note suggests, then the justices would next proceed to consider whether to require a probable cause warrant for the government's acquisition of historical CSLI as the *Graham I* panel did.[193] In the absence of legislation from Congress, such as that proposed above, popular opinion and judicial decisions would support a Supreme Court decision finding that citizens have an objectively reasonable expectation of privacy in their historical CSLI.[194] Statistical data clearly show that cellular subscribers have an expectation of privacy in their historical CSLI that society would regard as reasonable.[195] State courts, federal trial courts, and federal appellate courts all have determined that cell phone users have an objectively reasonable expectation of privacy in their historical CSLI.[196] Further, the Supreme Court appears ready to borrow from the traditional trespass analysis by incorporating a statement on the sanctity of the home into a potential opinion on CSLI acquisition and use by law enforcement.[197] Cell phone users

---

[192] *See Graham I*, 796 F.3d at 355–56 (implying that cell phone users are functionally required to transmit their CSLI); *Davis*, 785 F.3d at 535–36 (Martin, J., dissenting) (determining that cell phone users involuntarily create and transmit their CSLI).

[193] *See Graham I*, 796 F.3d at 344–45 (holding that the defendant had an objectively reasonable expectation of privacy in his historical CSLI); Corbett, *supra* note 133, at 226 (concluding that the Supreme Court likely will find the warrantless acquisition of historical CSLI to be a Fourth Amendment violation but will stop short of requiring a warrant due to exclusionary rule exceptions).

[194] *See Jones*, 132 S. Ct. at 950–51 (prohibiting searches that invade suspects' homes); *Graham I*, 796 F.3d at 345 (holding that citizens have an objectively reasonable expectation of privacy in their historical CSLI); Corbett, *supra* note 133, at 226 (noting that the Supreme Court will likely determine that law enforcement violates the Fourth Amendment when relying upon § 2703 orders to collect historical CSLI); McAllister, *supra* note 161, at 520 (establishing that empirical data reveal an objectively reasonable expectation of privacy in historical CSLI).

[195] *See* McAllister, *supra* note 161, at 520 (explaining that the results of a statistical analysis show a strong public expectation of privacy in location data).

[196] *Graham I*, 796 F.3d at 345; *Davis*, 785 F.3d at 541 (Martin, J., dissenting); *In re* Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d 113, 119–20 (E.D.N.Y 2011) (holding that people retain a reasonable expectation of privacy in long-term CSLI); *In re* Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone, 849 F. Supp. 2d 526, 539 (D. Md. 2011) (finding a reasonable expectation of privacy in location data when a subject is tracked for a period of thirty days); *Augustine*, 4 N.E.3d at 865–66 (concluding that criminal defendants have an objectively reasonable expectation of privacy in their CSLI); State v. Earls, 70 A.3d 630, 632 (N.J. 2013) (holding that under the New Jersey state constitution, the defendant had an objectively reasonable expectation of privacy in his CSLI).

[197] *See Jones*, 132 S. Ct. at 950–51 (refusing to sanction government surveillance that penetrated the home); Soldal v. Cook County, Ill., 506 U.S. 56, 64 (1992) (commenting on sanctity of the home). In *Jones* and *Soldal*, the Supreme Court emphasized that *Katz* augmented, rather than extinguished, property-based Fourth Amendment protections that center on the sanctity of the home. *Jones*, 132 S.

have an objectively reasonable expectation of privacy in their historical CSLI.[198]

Following *Katz*, the Supreme Court should require that the government obtain a warrant issued on a finding of probable cause before acquiring historical CSLI and using it at trial.[199] If the Supreme Court institutes a probable cause warrant requirement for the collection and use at trial of historical CSLI, then the Court also should hold that all pre-existing warrant exceptions apply to warrants for historical CSLI.[200] Authorizing reasonable law enforcement actions would create a safety valve to protect the public in exigent circumstances when law enforcement needs are at their maximum.[201]

CONCLUSION

Congress and the Supreme Court should act in concert to protect the Fourth Amendment rights of citizens when the government seeks their historical CSLI from cellular providers. The reason for doing so is as old as the American Revolution itself. The Founders sought to create a nation ruled in an absolute sense—not by men, but by law. They thought that the best republics were those that, by the arrangement of their powers, best and most impartially executed just laws. As time—and technology—work changes, this vital under-

---

Ct. at 950–51; *Soldal*, 506 U.S. at 64. The *Graham I* court recognized this signal from the Supreme Court and expressed its concern that historical CSLI could track a subject to and within a home, where Fourth Amendment protections are at a maximum. 796 F.3d at 346–47.

[198] *See Graham I*, 796 F.3d at 344–45 (determining that cell phone users have an objectively reasonable expectation of privacy in their historical CSLI); *Davis*, 785 F.3d at 541 (Martin, J., dissenting) (deciding that cell phone users have an objectively reasonable expectation of privacy in their historical CSLI); *Elec. Commc'n Serv.*, 620 F.3d at 312–13 (observing that Fourth Amendment concerns arise when historical CSLI tracks citizens within their homes).

[199] *See Graham I*, 796 F.3d at 344–45 (deciding that the government must obtain a warrant before acquiring historical CSLI); *Davis*, 785 F.3d at 541 (Martin, J., dissenting) (stating that without a probable cause warrant, the government violates the Fourth Amendment when it collects historical CSLI); Corbett, *supra* note 133, at 226 (arguing that a showing of probable cause is necessary if the government seeks to obtain historical CSLI).

[200] *See Graham I*, 796 F.3d at 345 (holding that the Fourth Amendment requires a warrant for historical CSLI unless a warrant exception applies); Corbett, *supra* note 133, at 226 (noting that the Supreme Court likely will find that the Fourth Amendment requires a warrant for the collection of historical CSLI, but that the Court also will find the exigency exception applicable to many CSLI cases). To protect citizens from an imminent risk of harm by a criminal suspect, the Court may reaffirm the exigency exception and allow the warrantless acquisition of historical CSLI. *See* Brigham City v. Stuart, 547 U.S. 398, 400 (2006) (establishing a warrant exception for exigent circumstances when police reasonably believe that the occupant of a residence is or may imminently be seriously injured); Corbett, *supra* note 133, at 226 (noting that the Supreme Court may invoke a warrant exception to allow government collection of historical CSLI without a warrant).

[201] *See Brigham City*, 547 U.S. at 403 (implying that warrant exceptions arise when the needs of law enforcement become so compelling that they outweigh an individual's reasonable expectation of privacy); *Graham I*, 796 F.3d at 345 (requiring that the government obtain a warrant for the collection of historical CSLI unless a warrant exception applies).

standing of our national character has remained the same. To secure our nation's commitment to the rule of law, the government and its officials must heed the fundamental commands enshrined in our Constitution and Bill of Rights. A government that violates its Constitution engenders contempt for the law and invites anarchy by encouraging every man to follow rules of his own creation. Our leaders must remain true to the protections that our Founders so wisely adopted at our nation's birth.

ALEXANDER PORTER