**Constitutional Law**—Maryland District Court Finds Government's Acquisition of Historical Cell Site Data Immune from Fourth Amendment—*United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012)

A criminal defendant's motion to suppress often implicates the Fourth Amendment's protections against "unreasonable searches and seizures."[1] Nevertheless, the extent to which government surveillance activities associated with wireless communication and location tracking technology fall within the ambit of the Fourth Amendment is unclear.[2] In *United States v. Graham*,[3] the United States District Court for the District of Maryland considered whether defendants' Fourth Amendment rights were violated when the government acquired historical cell site location information (CSLI) without a search warrant.[4] The court found that the defendants' Fourth Amendment rights were

1. U.S. CONST. amend IV. The Fourth Amendment to the United States Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ." *Id.* At the time the Fourth Amendment was adopted, the verb to "search" meant, "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection . . . ." 2 NOAH WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (1828); *see* Katz v. United States, 389 U.S. 347, 372 (1967) (Black, J., dissenting) (indicating Fourth Amendment adopted in 1791). According to the Supreme Court, "[a] search compromises the individual interest in privacy . . . ." Horton v. California, 496 U.S. 128, 133 (1990). Law enforcement agents are generally required to obtain a warrant based on a showing of probable cause before undertaking a search as a procedural deterrent against unreasonable searches. *See* Texas v. Brown, 460 U.S. 730, 735 (1983) (plurality opinion) (observing Supreme Court precedent favors "procedure by way of a warrant"); *see also* Renée McDonald Hutchins, *Tied up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 421 (2007) (summarizing warrantless searches as "presumptively unreasonable" under Supreme Court's Fourth Amendment analysis). Probable cause requires facts sufficient to warrant a belief by a person of reasonable caution that the specific items being sought may constitute evidence of a crime. *See* Texas v. Brown*,* 460 U.S. 730, 742 (1983) (plurality opinion); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 620 (2003) (likening probable cause requirement to demonstrating crime likely committed and search locale contains evidence); *see also* BLACK'S LAW DICTIONARY 1321 (9th ed. 2009) (defining probable cause as, "reasonable ground to suspect that a person has committed . . . a crime").

2. *See* Justin P. Webb, Note, *Car-Ving Out Notions of Privacy: The Impact of GPS Tracking and Why* Maynard *Is a Move in the Right Direction*, 95 MARQ. L. REV. 751, 756 (2012) (characterizing court decisions concerning GPS surveillance as "failing to provide clarity" on Fourth Amendment implications); *cf.* Russell D. Covey, *Pervasive Surveillance and the Future of the Fourth Amendment*, 80 MISS. L.J. 1289, 1300 (2011) (observing Fourth Amendment law's failure to promulgate useful rules in face of technological change).

3. 846 F. Supp. 2d 384 (D. Md. 2012).

4. *Id.* at 388. CSLI may be used to identify the address of the nearest cellular tower that a cellular telephone accesses during a specified time period and, hence, also the location of the user with reasonable accuracy. *See generally* Christian Levis, Note, *Smartphone, Dumb Regulations: Mixed Signals in Mobile Privacy*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 191, 194–204 (2011) (explaining cellular location technology). Accordingly, CSLI may be a useful tool for law enforcement in a criminal investigation to determine a suspect's whereabouts at a given time. *See* Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 422 (2007) (asserting

not violated because they did not have a legitimate expectation of privacy—a requisite condition precedent to an unconstitutional search determination—in the CSLI at issue.[5]

On February 5, 2011, robberies occurred at a Baltimore, Maryland-area Burger King restaurant and McDonald's restaurant.[6] Shortly after the McDonald's robbery, police apprehended Aaron Graham and Eric Jordan.[7] Police officers recovered a handgun and United States currency from the suspects and their vehicle before arresting them.[8] After the arrest, police obtained search warrants for two cellular telephones recovered from the vehicle, and then matched the phones with the telephone numbers Graham and Jordan had provided to investigators.[9]

Following further investigation into the robberies, the government applied for a court order pursuant to the Stored Communications Act (SCA) to compel Graham's and Jordan's wireless providers to disclose the CSLI related to the use of their cellular telephones.[10] Magistrate Judge Gauvey granted the application after finding that the government had met the requisite "specific and articulable facts" standard under the SCA.[11] While the restaurant robbery

law enforcement has utilized cellular location tracking).

5. *See* 846 F. Supp. 2d at 389.

6. *Id.* at 385. Witnesses at both robberies provided police with descriptions of the robber and get-away vehicle. *Id.* at 386.

7. *Id.* The vehicle Graham and Jordan were apprehended in, and the jacket Graham was wearing, matched the witnesses' descriptions. *Id.*

8. *Id.* During the arrest Graham and Jordan provided their cellular telephone numbers to the arresting officers. *Id.*

9. 846 F. Supp. 2d at 386. Initially, federal authorities only charged Graham and Jordan with firearms violations. *Id.*

10. *Id.* The application sought CSLI for a total of fourteen days. *Id.* The government intended to use the CSLI to conclusively link Graham and Jordan to the two robberies. *Id.* The SCA permits the government to obtain such an order "if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (2006). In *Graham*, the government alleged that the CSLI sought was relevant to the ongoing Burger King and McDonald's robbery investigations, as well as several others in which Graham and Jordan were suspects. 846 F. Supp. 2d at 386.

11. 846 F. Supp. 2d at 386. Whether the SCA's specific and articulable facts threshold has been met is a question of fact for a judge. *See id.* (referring to Magistrate Judge Gauvey's factual finding that government met its burden under SCA); 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, 1219 (2004) (explaining judicial process behind obtaining SCA order). *But cf.* United States v. Cortez, 449 U.S. 411, 417 (1981) (admonishing use of term "articulable reasons" as failing to provide clear guidance). Moreover, the government's burden in seeking an order pursuant to the SCA—that is, meeting the specific and articulable facts standard—is less than in cases where it seeks a search warrant and must demonstrate probable cause. *See* Kerr, *supra* note 1, at 620 (ranking legal thresholds for government surveillance). Under the SCA, the government need only proffer specific and articulable facts illustrative of the likelihood that the information sought will be relevant to a criminal *investigation*, as opposed to proffering facts illustrative of evidence of a crime. *See* 18 U.S.C. § 2703(d); *supra* note 1 (explaining probable cause and its stringent requirements). In *Graham*, the government amended its initial indictment—charging Graham and Jordan with firearms violations—to include conspiracy to commit robbery and robbery of the Burger King and McDonald's restaurants after its application was granted. 846 F.

investigations were still ongoing, the government uncovered new evidence of additional robberies in the Baltimore area and submitted a second application for CSLI.[12] Magistrate Judge Grimm, presiding over the government's second application, approved it after also finding that the government had met the SCA's specific and articulable facts standard.[13] Graham then filed a motion to suppress the CSLI, which Jordan joined, arguing that the extensive cellular monitoring associated with the CSLI infringed upon his expectation of privacy in violation of his Fourth Amendment rights.[14] In denying Graham and Jordan's motion to suppress, Judge Bennett held that the government's acquisition of the data did not constitute an unreasonable search under the Fourth Amendment because the movants did not have a legitimate expectation of privacy in the CSLI.[15]

To date, no clearly articulated standard exists as to what constitutes an "unreasonable search" under the Fourth Amendment.[16] The early formulation of the "search" test for deciding when government surveillance violates the Constitution was predicated on a requirement that law enforcement commit common-law trespass.[17] Conversely, current Fourth Amendment jurisprudence

Supp. 2d at 386. The amended indictment eventually included additional robberies in the Baltimore area as well. *Id.*

12. 846 F. Supp. 2d at 386–87. The second CSLI application sought all of the records acquired as part of the government's first application as well as the records for time periods covering the additional robberies. *Id.* at 387. The total amount of time for which the government sought CSLI was approximately seven months. *Id.* Graham and Jordan were indicted on these additional robberies in connection with this investigation. *Id.*

13. *Id.*

14. *Id.* at 385, 387. Graham's motion to suppress was based on an as-applied challenge to the SCA. *Id.* at 387. An as-applied challenge is "a claim that a statute is unconstitutional on the facts of a particular case or in its application to a particular party." BLACK'S LAW DICTIONARY 261 (9th ed. 2009).

15. 846 F. Supp. 2d at 389.

16. *See* Kyllo v. United States, 533 U.S. 27, 31–32 (2001) (lamenting complexity of Fourth Amendment "search" determination under Supreme Court's precedent); Chapman v. United States, 365 U.S. 610, 618 (1961) (Frankfurter, J., concurring) ("The course of true law pertaining to searches . . . has not—to put it mildly—run smooth."); Hutchins, *supra* note 1, at 422 (stating no single definition for term "search" under current law); Eli R. Shindelman, Note, *Time for the Court to Become "Intimate" with Surveillance Technology*, 52 B.C. L. REV. 1909, 1910 (2011) (describing what constitutes "search" as "subject of much jurisprudential debate"); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 349 (1974) (criticizing Supreme Court's treatment of Fourth Amendment law). Part of the difficulty in setting the parameters of a Fourth Amendment search lies in the variety of ways that the government may undertake criminal surveillance. *See, e.g.*, Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (deciding government's aerial photographs of open industrial complex not constitutionally protected search); Hoffa v. United States, 385 U.S. 293, 302 (1966) (refusing to extend Fourth Amendment protection to voluntary conversations between defendant and government informant); On Lee v. United States, 343 U.S. 747, 751 (1952) (seeing no Fourth Amendment issue with federal agents' use of concealed microphone to incriminate defendant).

17. *See* On Lee v. United States, 343 U.S. 747, 751, 753–54 (1952) (decreeing eavesdropping without more fails to meet trespass requirement of unreasonable search); Goldman v. United States, 316 U.S. 129, 134–35 (1942) (maintaining search requires tangible, physical government trespass), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); Olmstead v. United States, 277 U.S. 438, 464 (1928) (concluding no search under Fourth Amendment because no entry of defendants' houses or offices), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); *see also* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L.

has turned away from the trespass distinction, instead focusing on the two-part test Justice Harlan posited in his concurring opinion in the landmark case of *Katz v. United States*.[18] First, the *Katz* inquiry asks whether the individual has a (subjective) expectation of privacy and second, whether that expectation is objectively reasonable.[19]

REV. 1511, 1517 (2010) (noting initial Fourth Amendment test focused on physical intrusions); Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 1–2 (2009) (explaining Supreme Court's early, narrow reading of Fourth Amendment where search necessarily involved trespass). At common law, trespass is defined as the "intentional interference with property"; the interference may be with respect to either real or personal property. *See* WILLIAM L. PROSSER, HANDBOOK OF THE LAW OF TORTS 76 (1941) (dividing interference with property transgression into trespass to land and trespass to chattels, respectively); *see also* RESTATEMENT (SECOND) OF TORTS §§ 158, 217 (1965) (defining trespass to land and trespass to chattels).

18. 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Katz was convicted in federal court for transmitting wagering information by telephone between three states. *Id.* at 348. FBI agents fastened an electronic listening and recording device to a phone booth that Katz regularly used to place phone calls for wagering purposes. *Id.* At trial and over Katz's objection, the court allowed the government to introduce evidence of the calls obtained through the FBI's use of the electronic device. *Id.* The Supreme Court ultimately overturned Katz's conviction, holding that the government's electronic surveillance activities constituted an unconstitutional search because the government violated Katz's justifiable expectation of privacy. *Id.* at 353. Fourth Amendment law has since embraced *Katz* as the landmark case. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 947 (2012) (discussing trend in Supreme Court's Fourth Amendment jurisprudence and recognition of *Katz*); Kyllo v. United States, 533 U.S. 27, 32 (2001) (acknowledging Justice Harlan's concurring opinion in *Katz* as current framework for analyzing Fourth Amendment search); Smith v. Maryland, 442 U.S. 735, 739 (1979) (recognizing *Katz* as "lodestar" in determining occurrence of Fourth Amendment search), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, *as recognized in* Saldana v. State, 846 P.2d 604 (Wyo. 1993); *see also* Amsterdam, *supra* note 16, at 382 (opining *Katz* "marks a watershed in fourth amendment [sic] jurisprudence"); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 815 (2004) (highlighting modern Fourth Amendment interpretation of *Katz* as favoring protection for one's privacy over property). *But see* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT 435 (4th ed. 2004) (suggesting *Katz* test creates more harm than good in providing useful Fourth Amendment rule).

19. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The first requirement, the presence of a subjective expectation of privacy, concerns the intention and conduct of the person claiming Fourth Amendment protection. *See id.* (contrasting privacy expectation in activities undertaken discreetly at home with those done in plain view); Eric Dean Bender, Note, *The Fourth Amendment in the Age of Aerial Surveillance: Curtains for the Curtilage?*, 60 N.Y.U. L. REV. 725, 743–44 (1985) (arguing subjective expectation of privacy inquiry should concentrate on individual's conduct). Nonetheless, the objective, reasonable expectation of privacy prong has been recognized as the driving force of constitutional analysis. *See* Oliver v. United States, 466 U.S. 170, 177 (1984) (referring to reasonable expectation of privacy test as touchstone of Fourth Amendment analysis); Smith v. Maryland, 442 U.S. 735, 740 (1979) (indicating Fourth Amendment applicability dependent on government invasion of legitimate expectation of privacy under *Katz*), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, *as recognized in* Saldana v. State, 846 P.2d 604 (Wyo. 1993); *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 490 (2011) (labeling reasonable expectation of privacy inquiry "best-known doctrinal test" in Fourth Amendment analysis). *But see* Edmund W. Kitch, Katz v. United States*: The Limits of the Fourth Amendment*, 1968 SUP. CT. REV. 133, 134–35 (1968) (positing reasonable expectation of privacy test difficult to apply). One possible reason that the objective prong of the *Katz* framework dominates the Fourth Amendment search inquiry is the failure of the courts to give life to the subjective privacy expectation element. *See* LAFAVE, *supra* note 18, at 438 (stating little attention and interpretive guidance given to first element of *Katz* test).

The lack of a workable judicial standard to illuminate the parameters of an objectively reasonable expectation of privacy has resulted in an incongruent relationship between technology and Fourth Amendment searches.[20] In other words, technological developments, specifically those that aid police in criminal surveillance, have led to varied results in the application of the *Katz* reasonable expectation of privacy inquiry.[21] Further complicating matters is the "third-party" doctrine, which recognizes that the Fourth Amendment does not protect the government's procurement of information that is voluntarily revealed to a third party, who in turn conveys it to government authorities.[22] Under the third-party doctrine, the Supreme Court has declared that "business records" and data stored for business purposes also are not generally subject to constitutional protection.[23] Another controversial interpretation of what

20. *See* Kyllo v. United States, 533 U.S. 27, 33–34 (2001) (conceding technological advancement impacts extent of Fourth Amendment's privacy protections); *see also* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (admitting no "talisman" for consistently determining when privacy expectations objectively reasonable); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504–05 (2007) (calling reasonable expectation of privacy concept "remarkably opaque").

21. *Compare* California v. Ciraolo, 476 U.S. 207, 214 (1986) (declaring aerial surveillance of private home generally not infringement of one's expectation of privacy), *and* United States v. Knotts, 460 U.S. 276, 285 (1983) (holding tracking beeper installed on chemicals shipped to defendant did not hinder expectation of privacy), *with* Kyllo v. United States, 533 U.S. 27, 34–35 (2001) (stating thermal imaging of home erodes constitutional protection of privacy), *and* United States v. Karo, 468 U.S. 705, 713 (1984) (concluding installation of monitoring beeper within private home impaired defendant's expectation of privacy).

22. United States v. Miller, 425 U.S. 435, 443 (1976), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 95-630, 92 Stat. 3697 (codified at 12 U.S.C. §§ 3401-3421), *as recognized in* Hancock v. Marshall, 86 F.R.D. 209 (D.D.C. 1980); *see* United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding no legitimate expectation of privacy in internet subscriber information voluntarily conveyed to internet company); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009) (third-party doctrine means "information loses Fourth Amendment protection when it is knowingly revealed to a third party"). The Fourth Circuit's decision in *Bynum* exemplifies the third-party doctrine's underlying rationale. United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010). Bynum was convicted in federal court of transporting and possessing child pornography. *Id.* at 162. At issue in the case was an FBI administrative subpoena served on an internet provider that yielded Bynum's subscriber information and linked him to a child pornography internet group. *Id.* at 162–63. In upholding his conviction, the Fourth Circuit stated that Bynum had no reasonable expectation of privacy in his internet subscriber information because he voluntarily conveyed it to both his internet and phone service providers. *Id.* at 164; *cf.* United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (noting internet subscriber information yet to be afforded Fourth Amendment protection in federal court).

23. *See* United States v. Miller, 425 U.S. 435, 440 (1976) (concluding defendant's bank records constituted business records voluntarily conveyed to third-party disclosing bank), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 95-630, 92 Stat. 3697 (codified at 12 U.S.C. §§ 3401-3421), *as recognized in* Hancock v. Marshall, 86 F.R.D. 209 (D.D.C. 1980); *cf.* Smith v. Maryland, 442 U.S. 735, 744 (1979) (stating dialing phone numbers entails voluntarily conveying them to phone company during course of business), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, *as recognized in* Saldana v. State, 846 P.2d 604 (Wyo. 1993). In *Miller*, Miller was convicted of various federal offenses pertaining to an illegal alcohol manufacturing operation. United States v. Miller, 425 U.S. 435, 436 (1976), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 95-630, 92 Stat. 3697 (codified at 12 U.S.C. §§ 3401-3421), *as recognized in* Hancock v. Marshall, 86 F.R.D. 209 (D.D.C. 1980). Before trial, Miller objected to the government's introduction of his bank records, which federal authorities obtained via a defective subpoena, and filed a motion to suppress. *Id.* at 436–37.

constitutes a reasonable expectation of privacy is the "mosaic" approach, which considers the extent of government surveillance in determining whether it amounts to a search under the Fourth Amendment.[24] Recognizing the need to uphold constitutional protections for information shared with another through wireless communication, Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA).[25]

Thus far, the federal district courts have been tasked with trying to square the SCA with the Supreme Court's Fourth Amendment jurisprudence.[26]

Ultimately, Miller's motion was denied and the records were used as evidence to secure his conviction. *Id.* The Fifth Circuit deemed the improperly subpoenaed bank records subject to Fourth Amendment protection and reversed Miller's conviction. *Id.* at 437. The Supreme Court subsequently overturned the Fifth Circuit and held that there was no governmental intrusion into any constitutionally protected interest. *Id.* at 440. The rationale for the *Miller* Court's decision was based on its inability to conceptualize a legitimate expectation of privacy in bank records and the notion that Miller assumed the risk that they might be turned over to the government when he revealed them to the bank in the course of business. *Id.* at 442–43. *But see* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 734 (2011) (calling for narrow reading of *Miller* decision based on nature of records sought). In *Smith v. Maryland*, Smith was convicted of robbery in a Maryland state court. 442 U.S. 735, 737–38 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, *as recognized in* Saldana v. State, 846 P.2d 604 (Wyo. 1993). The police requested that the telephone company install a pen register to monitor his phone calls because the robbery victim indicated that Smith had been making threatening phone calls to her in which he identified himself as the man who robbed her. *See id.* at 737 (suggesting police identified Smith as person of interest following victim's description and subsequent police investigation). The *Smith* Court reasoned that when one voluntarily conveys information to a third party, one assumes the risk that the third party may subsequently reveal the information to the police, nullifying any reasonable expectation of privacy, and thereby held that the police's use of the pen register did not constitute an unconstitutional search. *Id.* at 744; *see* Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 390 (2003) (contending callers risk call information reaching police by virtue of using telephone).

24. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012). At issue in *Maynard* was the constitutionality of a GPS monitoring device that police attached to the defendant's car without a warrant or a court order pursuant to the SCA. *Id.* at 555; *see* Erin Smith Dennis, Notes, *A Mosaic Shield:* Maynard*, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 738 (2011) ("Under the mosaic theory of privacy espoused by the [*Maynard*] court, individual actions of law enforcement that are not searches for Fourth Amendment purposes may become searches when taken together en masse."). Consequently, the *Maynard* court held that the defendant did have a legitimate expectation of privacy, which the government violated through the extensive surveillance it conducted via the GPS tracking device. United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

25. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). The SCA came into existence in 1986 as a portion of the ECPA, which was enacted to promulgate privacy protections in light of "dramatic changes in . . . telecommunications technologies." S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. The SCA serves dual functions of allowing the government access to useful information for law-enforcement purposes, and protecting users from unwarranted government intrusion. *See* S. REP. NO. 99-541, at 5 (referencing congressional intent to balance government's law enforcement interests with citizens' privacy protections); *see also* Kerr, *supra* note 11, at 1223 (summarizing key SCA rules and disclosure provisions). In its report on the ECPA, the Senate Judiciary Committee stated, "the law must advance with the technology to ensure the continued vitality of the fourth amendment [sic]." S. REP. NO. 99-541, at 5.

26. *See* Dennis, *supra* note 24, at 759–60 (discussing federal courts' varied interpretations of SCA following *Maynard* decision).

District courts are split as to whether the Fourth Amendment's protections are implicated when the government seeks CSLI pursuant to the SCA.[27] As a result, the constitutional protections limiting the reach of the SCA are seemingly guaranteed only by the latitude afforded to judges to deny the government's applications for want of a showing of probable cause, even if the SCA's specific and articulable facts standard is met.[28] Although the Supreme Court has yet to take up the issue of whether a court-ordered CSLI disclosure pursuant to the SCA can rise to the level of a Fourth Amendment search, at least one recent Court decision, *United States v. Jones,* is instructive.[29]

In *United States v. Graham*, the court considered the defendants' motion to

27. *Compare In re* Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) (extending Fourth Amendment protections to CSLI), *and In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 845–46 (S.D. Tex. 2010) (concluding CSLI not voluntarily conveyed business records and therefore warranting constitutional protection), *and In re* Application of U.S. for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 578–79 (E.D.N.Y. 2010) (denying order to compel cell-site data disclosure for lack of probable-cause-based warrant), *rev'd*, No. 10-MC-0550 (E.D.N.Y Nov. 29, 2010), *with* United States v. Dye, No. 1:10CR221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011) (refusing to recognize reasonable expectation of privacy in cell phone records), *and* United States v. Velasquez, No. CR 08-0730 WHA, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010) (stating no legitimate expectation of privacy in telephone numbers voluntarily conveyed to service provider), *and* United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010) (maintaining no reasonable expectation of privacy in records communicated to third-party cell-phone company), *and* United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *10–11 (N.D. Ga. Apr. 21, 2008) (finding government's acquisition of CSLI did not amount to Fourth Amendment search), *and In re* Applications of U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F. Supp. 2d 76, 80 (D. Mass. 2007) (deciding Fourth Amendment's probable cause requirement does not preempt SCA's CSLI disclosure provisions).

28. *See In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313, 319 (3d Cir. 2010) (declaring SCA affords judge option to require warrant on showing of probable cause); Dennis, *supra* note 24, at 770 (stating federal court's prerogative may be to require probable cause showing or adhere to SCA). *But see In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 320 (3d Cir. 2010) (Tashima, J., concurring) (characterizing discretion given to magistrate judges in approving or denying government's application as troubling).

29. *See* 132 S. Ct. 945, 949 (2012) (holding government's installation of GPS tracking device to defendant's vehicle amounted to Fourth Amendment search). Joining Justice Scalia's majority opinion were Chief Justice Roberts and Justices Kennedy, Thomas, and Sotomayor. *Id.* at 947. The majority opinion reasoned that because law enforcement agents physically occupied private property for the purpose of obtaining information, their actions qualified as a Fourth Amendment search. *Id.* at 949. Justice Sotomayor issued a concurring opinion favoring Justice Scalia's trespass-based disposition of the case, but also agreeing with the reasoning in Justice Alito's concurring opinion—joined by Justices Ginsburg, Breyer, and Kagan—that a reasonable expectation of privacy is infringed when the government undertakes long-term GPS monitoring. *Id.* at 954–57 (Sotomayor, J., concurring). Hence, the precedential value of the *Jones* decision for district courts adjudicating government applications pursuant to the SCA is a 4-4-1 split. *Id.* at 947. Four justices, led by Justice Scalia, rejected the mosaic approach embraced by the Justice Alito concurrence. *Id.* at 953–54. Meanwhile, four justices, led by Justice Alito, dismissed Justice Scalia's trespass analysis as antiquated and "lead[ing] to incongruous results." *Id.* at 961 (Alito, J., concurring). Justice Sotomayor emerges as the potential swing vote if the Supreme Court takes up the issue of whether the mosaic approach is applicable to Fourth Amendment search analysis due to both her recognition of the trespass doctrine's continued vitality and her acknowledgment that the extent of government surveillance is a potentially dispositive consideration in the analysis. *Id.* at 955–56 (Sotomayor, J., concurring).

suppress government-obtained CSLI vis-à-vis an as-applied challenge to the SCA as an infringement of their constitutionally protected legitimate expectation of privacy.[30] First, the court distinguished the case at bar from *United States v. Maynard,*[31] based on both the extent of the surveillance and the nature of the information sought.[32] The court also distinguished the absence of a probable cause showing in *Maynard* from the instant case, which met the SCA's requisite specific and articulable facts standard that was not applicable in *Maynard*.[33] Next, the court focused its Fourth Amendment analysis on the application of the *Katz* framework to the government's acquisition of CSLI pursuant to the SCA.[34] The court rejected Graham and Jordan's contention that they had a reasonable expectation of privacy in their CSLI, and applied the third-party doctrine, finding the case at bar analogous to the leading Supreme Court cases of *United States v. Miller*[35] and *Smith v. Maryland*,[36] and the Fourth Circuit's decision in *United States v. Bynum*.[37]

The court subsequently turned its attention to the Supreme Court's recent Fourth Amendment-based decision in *United States v. Jones*.[38] The *Graham*

30. 846 F. Supp. 2d at 387, 389.

31. 615 F.3d 544 (D.C. Cir. 2010).

32. 846 F. Supp. 2d at 391–92. Judge Bennett further explained that unlike in *Graham*, which focused on the government's access to and use of CSLI, *Maynard* concerned long-term vehicle surveillance via GPS tracking. *Id.* Furthermore, CSLI only reveals historical information about a suspect's location, yet the GPS technology at issue in *Maynard* exposed the suspect's location and movements in real time. *Id.* Judge Bennett considered the GPS-location data in *Maynard* more precise than the CSLI disputed in *Graham* because CSLI can only determine the general area in which a cellular telephone is used, whereas GPS technology relays precise location coordinates to the police. *Id.* at 392.

33. *See id.* (calling attention to government's surveillance activities without warrant or SCA order).

34. *Id.* at 396; *see supra* note 19 and accompanying text (discussing *Katz* framework). In *Graham*, the court construed the Supreme Court's decision in *Jones* to stand for the proposition that the *Katz* inquiry is not the universal standard for determining the existence of a Fourth Amendment search. *See* 846 F. Supp. 2d. at 396 (interpreting *Jones* decision to mean *Katz* framework applicable in absence of government's physical trespass); *see also* United States v. Jones, 132 S. Ct. 945, 953 (2012) (upholding *Katz* test for cases dealing with "transmission of electronic signals without trespass"). The *Graham* court applied the *Katz* doctrine because the CSLI at issue concerned the transmission of electronic signals and the government did not physically trespass to obtain the information. *See* 846 F. Supp. 2d at 396.

35. 425 U.S. 435 (1976), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 95-630, 92 Stat. 3697 (codified at 12 U.S.C. §§ 3401-3421), *as recognized in* Hancock v. Marshall, 86 F.R.D. 209 (D.D.C. 1980).

36. 442 U.S. 735 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, *as recognized in* Saldana v. State, 846 P.2d 604 (Wyo. 1993).

37. 604 F.3d 161 (4th Cir. 2010); *see* 846 F. Supp. 2d at 397–400. The *Graham* court likened the bank records at issue in *Miller*, the telephone numbers dialed in *Smith*, and the internet subscriber information conveyed in *Bynum* to the CSLI disclosed in *Graham*. 846 F. Supp. 2d at 400. The court reasoned that the CSLI constituted business records rather than Graham and Jordan's private records because the data was collected during the provider's "ordinary course of business." *Id. But see In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (doubting voluntariness of conveying CSLI because of users' unfamiliarity with cell-phone technology).

38. *See* 846 F. Supp. 2d at 401–02 (interpreting *Jones* and applying to instant case); *see also supra* note 29 and accompanying text (discussing Supreme Court's decision in *Jones*).

court was reluctant to apply the mosaic theory and find a net infringement of Graham and Jordan's legitimate expectation of privacy by aggregating the amount of CSLI the government collected, noting the "varied" reasoning that the Justices of the Supreme Court employed in deciding *Jones*.[39] The *Graham* court ultimately rejected the mosaic theory promulgated in *Maynard*, finding the approach to be problematic, and further relying on the *Jones* decision and the work of Fourth Amendment scholar Professor Orin S. Kerr.[40] Finally, the court distinguished *Graham* from the Supreme Court's decisions in *United States v. Karo*[41] and *United States v. Knotts*.[42] The court read *Karo* and *Knotts* to stand for the proposition that a search occurs when law enforcement utilizes tracking technology that allows surveillance in locations that they "could not monitor in the absence of that technology."[43] The court reasoned that while CSLI could identify the nearest cellular tower to Graham and Jordan's phones, it did not provide their precise locations, unlike the surveillance in *Karo* and *Knotts*.[44]

At the threshold, the district court properly distinguished *Graham* from *Maynard* by recognizing that the SCA's specific and articulable facts standard provides a degree of procedural protection not present in *Maynard*.[45] The court also appropriately acknowledged *Katz* as the instructive rule under Fourth Amendment jurisprudence and the Supreme Court's recent *Jones* decision.[46] However, while the court properly recognized that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," it too briskly extends *Miller* and *Smith* by concluding that CSLI is voluntarily conveyed.[47] The court's assumption that users voluntarily transfer their CSLI

39. *See* 846 F. Supp. 2d at 394, 401–03 (contemplating application of mosaic theory).

40. *See id.* at 402 (disposing of mosaic theory). Judge Bennett's reluctance to apply the mosaic theory stemmed from the implications of applying the doctrine to police investigations collecting "cumulative" data, which were unclear and potentially adverse. *See id.* at 401–02 (expressing concern over how mosaic approach could undermine legitimate police investigations). Fourth Amendment scholar Professor Orin Kerr shares Judge Bennett's concerns. *See* Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search,* VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://www.volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/ (criticizing mosaic theory and warning of potentially serious consequences of incentivizing future Fourth Amendment challenges).

41. 468 U.S. 705 (1984).

42. 460 U.S. 276 (1983); *see* 846 F. Supp. 2d at 403–04 (outlining Supreme Court's electronic surveillance-based decisions).

43. 846 F. Supp. 2d at 404.

44. *See id.* (emphasizing relationship between surveillance method and resulting location information).

45. *See id.* at 392 (distinguishing absence of warrant based on probable cause in *Maynard* from SCA order in *Graham*).

46. *See id.* at 395 (pointing to *Katz* as standard for determining if Fourth Amendment search has taken place); United States v. Jones, 132 S. Ct. 945, 953 (2012) (solidifying *Katz* rule as applicable to cases based on "transmission of electronic signals without trespass"); *see also supra* note 19 and accompanying text (recognizing *Katz*'s legitimate expectation of privacy standard as controlling rule).

47. Smith v. Maryland, 442 U.S. 735, 743-44 (1979), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, *as recognized in* Saldana v. State, 846 P.2d 604

relies too heavily on the third-party doctrine, nullifying a putative defendant's legitimate expectation of privacy, and leaving the government with almost unfettered access to CSLI.[48]

In light of the *Jones* holding, the court correctly declined the opportunity to apply the mosaic approach and to find an expectation of privacy based on the pervasiveness of the government's surveillance.[49] The mosaic approach is an impotent guidepost for courts to follow in determining if one's legitimate expectation of privacy has been infringed, and is predicated on arbitrary distinctions of time and extent of surveillance.[50] After rejecting the mosaic theory, the *Graham* court distinguished the case at bar from *Karo* and *Knotts* based on the degree of precision of global positioning system (GPS) data compared with CSLI, and strayed off course, effectively subrogating CSLI's electronic surveillance value to that of GPS.[51]

Last, the court aptly recognized its judicial role and refused to legislate from the bench.[52] Instead, the court deferred to Congress to dictate the appropriate

(Wyo. 1993); *see In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information . . . in any meaningful way."); *In re* Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010) (noting cell phone user has no reason to suspect her location was revealed to anyone); Freiwald, *supra* note 23, at 736 (contending CSLI not voluntarily conveyed to third-party provider because of automatic generation); *see also supra* note 36 (analogizing facts in *Graham* to *Miller*, *Smith*, and *Bynum*); *cf.* United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting) (arguing disclosure of bank records involuntary because maintaining bank account essential to daily life), *superseded by statute*, Electronic Communications Privacy Act of 1986, Pub. L. No. 95-630, 92 Stat. 3697 (codified at 12 U.S.C. §§ 3401-3421), *as recognized in* Hancock v. Marshall, 86 F.R.D. 209 (D.D.C. 1980).

48. *See* LAFAVE, *supra* note 18, at 736 (remarking *Smith* decision's application of third-party doctrine "makes a mockery of the Fourth Amendment"); *see also* Freiwald, *supra* note 23, at 739 (maintaining amount of records generated and stored comprise only limits on government's CSLI acquisition). *But see* Kerr, *supra* note 22, at 600 (defending third-party doctrine as furthering clearer Fourth Amendment rules in face of new technology).

49. *See* 846 F. Supp. 2d at 401 (justifying avoidance of mosaic theory based on Fourth Amendment law and majority opinion in *Jones*); *see also* United States v. Jones, 132 S. Ct. 945, 954 (2012) (declining opportunity to consider mosaic theory); Kerr, *supra* note 40 (discussing adverse consequences of mosaic theory). *But see* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (finding merit in mosaic theory); *see also id.* at 955 (Sotomayor, J., concurring) (agreeing with Justice Alito about how long-term monitoring could impinge expectation of privacy).

50. *See* United States v. Jones, 132 S. Ct. 945, 954 (asserting consideration of length of time in government surveillance leads to "additional thorny problems"); *see also* 846 F. Supp. 2d at 402 ("Under the mosaic theory . . . [a] collection of data would *become* a Fourth Amendment search at some undefined point."); Kerr, *supra* note 40 (highlighting difficulty in determining when surveillance significant enough to constitute search). *But see* Webb, *supra* note 2, at 790 (characterizing criticism of mosaic approach's amorphousness as over reliant on judicial certainty).

51. *Compare* 846 F. Supp. 2d at 404 (concluding CSLI too imprecise to pinpoint defendants' location), *with In re* Application of U.S. for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs., 727 F. Supp. 2d 571, 580 (W.D. Tex. 2010) (explaining advances in technology to point where CSLI can locate person within fifty feet).

52. *See* 846 F. Supp. 2d at 394 ("Until the Supreme Court . . . definitively conclude[s] that an aggregation of surveillance records infringes a Fourth Amendment legitimate expectation of privacy, this Court [sic] must

protections to be afforded to stored electronic communications data.[53] Nevertheless, there is little value in the *Graham* court's holding apart from emphasizing the confusion that exists with respect to articulating what constitutes a search within the meaning of the Fourth Amendment.[54]

In *United States v. Graham*, the court appropriately denied Graham and Jordan's motion to suppress the CSLI because there was likely no Fourth Amendment search, nor was a showing of probable cause required under the SCA. Nonetheless, while the court reached the correct result, the holding could have been arrived at more expediently by simply adhering to the language and interpretation of the SCA without such expansive reliance on the third-party doctrine. Moreover, although Judge Bennett accurately parrots Fourth Amendment scholars, as well as Justice Alito's remarks in *Jones*, that change should come about legislatively, he needlessly overextends the third-party doctrine to CSLI and relies too heavily on *Miller* and *Smith*.

*Jeremy Derman*

apply the facts of this case to the law as currently interpreted."); *see also* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.").

53. *See* 846 F. Supp. 2d at 390 (identifying CSLI privacy protections under SCA as issue meriting legislative attention); Kerr, *supra* note 18, at 805–06 (arguing legislative branch best poised to create investigative rules when technology in flux). The *Graham* court further stated, "[t]he fact of the matter is that in enacting the Stored Communications Act, Congress passed a law that rejects a warrant requirement for [CSLI]." 846 F. Supp. 2d at 401.

54. *See supra* note 16 and accompanying text (discussing lack of clearly articulated standard for unreasonable search). Given the wide range of potential police surveillance methods, and the fact that Congress cannot legislate on the myriad of necessary privacy protections, judicial intervention will be necessary to illuminate the boundaries of an unreasonable search. *See* LAFAVE, *supra* note 18, at 436 (indicating array of police practices falling within *Katz* rule and arguably implicating Fourth Amendment protection).