Cell Phone Location Information: Not Voluntarily Conveyed
Urging the Legislature to Reestablish Privacy Rights After United States v. Graham

Nicholaus E. Johnson*

Introduction ............................................................................................ 154
I. The Cases ............................................................................................ 155
   A. The Fifth Circuit: In re Application of U.S. for Historical Cell
      Site Data .............................................................................. 156
   B. The Eleventh Circuit: United States v. Davis ...................... 156
   C. The Fourth Circuit: United States v. Graham ...................... 156
II. Analysis .............................................................................................. 157
   A. The Third-Party Doctrine..................................................... 157
   B. This Nation is Better Served by Extending Fourth
      Amendment Protections to CSLI ......................................... 160
   C. A Suggested Change to the Law .......................................... 161
Conclusion .............................................................................................. 163

DOI: http://dx.doi.org/10.15779/Z38TS01
Copyright © 2016 California Law Review, Inc. California Law Review, Inc. (CLR) is a
California nonprofit corporation. CLR and the authors are solely responsible for the content of their
publications.
* J.D., University of California, Berkeley, School of Law, 2017; B.S., University of Southern
California, Los Angeles, Marshall School of Business, 2014.
INTRODUCTION

Stop. Look at your phone. When was the last time it notified you about anything? How many times a day does it send you a notification? Did you intend to give your location to your service provider each time you heard a beep or felt a vibration? Well, regardless of whether you voluntarily offered up that information, they have it, and until modern precedent matches today’s technology, you may have given up your right to privacy along with the information.1

On many occasions, the government has obtained Cell Site Location Information (CSLI) through court orders,2 bypassing the rigorous process of obtaining a warrant3 authorized under the Fourth Amendment to protect Americans’ rights against unlawful search and seizure.4 CSLI is a small piece of the endless points of data a cell service provider maintains on each cell phone user.5 Each time your phone makes a connection with the service provider’s network, the provider logs that connection and its approximate location—the location information—based on the physical network antenna to which your phone connected—the cell site.6

Lower courts have considered the validity of cell phone users’ expectations of privacy to this information.7 According to the Fifth and Eleventh Circuits, there is none because cell phone users “voluntarily convey” this information to their service providers by simply using their cell phones.8 Because cell phone use sends location information to cell service antennas, these circuit courts place CSLI under an exception to the Fourth Amendment called the third-party

---

1. See infra Part II.
2. In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) [hereinafter In Re Application]; United States v. Davis, 785 F.3d 498 (11th Cir. 2015); United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016) [hereinafter En Banc Rehearing] (en banc) (relying on the facts set out “in great detail” by the panel opinion in United States v. Graham, 796 F.3d 332 (4th Cir. 2015)).
3. Per the Stored Communications Act, codified at 18 U.S.C. § 2701–12 (2009), governmental entities may petition a court to compel disclosure of CSLI through one of two mechanisms: a warrant under section 2703(c)(1)(A) or a court order under section 2703(d). In this process, law enforcement provides “articulable facts” to an issuing court showing that the information sought would assist in a criminal investigation. The court then assesses those facts to see if they meet or exceed a set legal standard for the mechanism requested. Law enforcement prefers court orders because section 2703(d) sets the legal standard at “reasonable suspicion”—an easily satisfied standard compared to the “probable cause” necessary for a warrant. See § 2703(d); U.S. CONST. amend. IV.
4. U.S. CONST. amend. IV.
5. Davis, 785 F.3d at 501.
6. Id.
8. In re Application, 724 F.3d at 615; Davis, 785 F.3d at 512.
disclosure doctrine (or third-party doctrine)—a rule that effectively eliminates legal expectations of privacy when information is given to a third party voluntarily.9 The Fourth Circuit recently reheard en banc the third-party doctrine argument in United States v. Graham (En Banc Rehearing).10 Contrary to the panel opinion, the En Banc Rehearing held that the third-party doctrine established by Smith v. Maryland and United States v. Miller is indeed applicable to CSLI based on current precedent.11 In fact, the theme permeating the En Banc Rehearing is that “without a change in controlling law,” a warrant is not needed to obtain CSLI.12 After analyzing each of Graham’s arguments, the court in the En Banc Rehearing made clear that change must come from the Supreme Court or the Legislature.13 While a Supreme Court decision would provide universal changes to the third-party doctrine, “[t]he legislative branch is far better positioned to respond to changes in technology than are the courts.”14 Therefore, this Comment joins with the Fourth Circuit and urges the Legislature to acknowledge the unyielding progression of technology by declaring the third-party doctrine inapplicable to CSLI and requiring law enforcement to obtain a warrant before collecting CSLI.

I. THE CASES

This Comment focuses on three different decisions from the circuit courts. First, the Fifth Circuit in In re Application of U.S. for Historical Cell Site Data held that cell phone users do voluntarily convey CSLI, making it unprotected information available to the government by a simple court order.15 Second, the Eleventh Circuit in United States v. Davis held in accordance with the Fifth Circuit that cell phone users voluntarily convey CSLI.16 Finally, the Fourth Circuit in United States v. Graham first held in a panel opinion that cell phone users do not voluntarily convey CSLI, protecting it from court-ordered collection, and then in the En Banc Rehearing, held that users voluntarily convey CSLI, eliminating Fourth Amendment protections.17

9. In re Application, 724 F.3d at 615; Davis, 785 F.3d at 512.
10. En Banc Rehearing, 824 F.3d 421.
11. Compare Graham, 796 F.3d at 353, with En Banc Rehearing, 824 F.3d at 430–31 (discussing the third-party doctrine established in United States v. Miller, 425 U.S. 435, 442 (1976) and Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).
12. En Banc Rehearing, 824 F.3d at 425 (“The Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case.”).
13. Id. at 426, 437 (“Congress remains free to require greater privacy protection if it believes that desirable”; “we are bound by the contours of the third-party doctrine as articulated by the Court.”).
14. Id. at 436.
15. See infra Part I.A.
16. See infra Part I.B.
17. See infra Part I.C.
A. The Fifth Circuit: In re Application of U.S. for Historical Cell Site Data

In October 2010, the United States sought court orders granting CSLI for three separate investigations. After the cell phone providers disclosed the CSLI, the government requested permission from a magistrate judge to use the data in all three investigations even though the government obtained it by a court order, not with a warrant. The magistrate judge felt that warrantless disclosure of CSLI violated Fourth Amendment protections—a conclusion with which the district judge agreed. The government appealed to the Fifth Circuit, which found that cell phone users voluntarily convey their location information to their cell service providers when placing a call. This decision created precedent in the Fifth Circuit that law enforcement may obtain CSLI through court orders without violating a defendant’s Fourth Amendment rights.

B. The Eleventh Circuit: United States v. Davis

Quartavius Davis and several others were charged with committing seven robberies over the course of two months. An essential piece of evidence connecting Davis to the scene of all seven robberies was CSLI. The government obtained 67 days of CSLI from Davis’s cell phone service provider, MetroPCS, by court order and used that information to approximate his location in relation to the robberies. The jury convicted Davis on sixteen counts. On appeal, Davis claimed that the government violated his Fourth Amendment right to privacy by obtaining his CSLI without a warrant. The Eleventh Circuit disagreed, holding that the third-party doctrine was controlling and that the government did not need a warrant to obtain Davis’s CSLI.

C. The Fourth Circuit: United States v. Graham

After allegedly committing a series of six armed robberies throughout Baltimore City and Baltimore, Maryland, Aaron Graham and Eric Jordan were arrested and convicted on several counts. During their arrest, officers searched the getaway vehicle and found two cell phones with numbers registered to

---

18. In re Application, 724 F.3d 600, 602 (5th Cir. 2013).
19. Id.
20. Id.
21. Id. at 615.
22. Id.
23. United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015).
24. Id. at 501.
25. Id.
26. Id. at 500.
27. Id. at 505.
28. Id. at 512.
Graham and Jordan. The government obtained 221 days of CSLI from Sprint/Nextel’s records through a court order. During its case-in-chief, the government used that data to approximate Graham and Jordan’s locations during the robberies. On appeal, both Graham and Jordan argued that the court should not have admitted the CSLI because the government violated their Fourth Amendment rights to privacy by obtaining the location information without a warrant. The Fourth Circuit’s panel opinion agreed with this argument, holding that CSLI is protected under the Fourth Amendment and is not subject to the third-party doctrine. The government then asked the Fourth Circuit to rehear the arguments en banc. The court in the En Banc Rehearing reversed the panel’s decision, asserting that it is constrained by Supreme Court precedent and finding that CSLI does not require a warrant because it is voluntarily conveyed to cell phone providers.

II. ANALYSIS

This Comment focuses on the third-party doctrine as an essential instrument for limiting the privacy expectations of CSLI. First, this Comment examines the doctrine’s meaning and application. Second, it explores and refutes the doctrine’s applicability to modern technology. Lastly, this Comment makes a suggestion for the Legislature to provide Fourth Amendment protections to CSLI.

A. The Third-Party Doctrine

The third-party doctrine says that voluntarily conveying information to a third party effectively eliminates any expectation of privacy. The doctrine arose out of two cases: Smith v. Maryland and U.S. v. Miller. In Smith, the Court found that information gathered through a pen register device used to collect dialed phone numbers did not constitute a search under the Fourth Amendment. This holding relied on an inferential chain that telephone users knowingly convey phone numbers to telephone companies that have facilities built to record

30. Id. at 340.
31. Id. at 341.
32. Id.
33. Id. at 342.
34. Id. at 353.
35. En Banc Rehearing, 824 F.3d 421, 423 (4th Cir. 2016).
36. Id. at 438.
37. See infra Part II.A.
38. See infra Part II.B.
39. See infra Part II.C.
40. United States v. Graham, 796 F.3d 332, 353 (4th Cir. 2015).
41. Id.
dialed numbers. The chain posits that phone users understand that phone companies must log the numbers they dial in order to connect calls through switching facilities. Because phone use is not free, these facilities log and document the numbers dialed. When phone users make a long distance call in particular, they become keenly aware that they conveyed the dialed phone numbers to the phone company because the numbers themselves arrive in the monthly bill. Using this reasoning, the Court found dialing phone numbers to be a voluntary conveyance and, under the third-party doctrine, not subject to Fourth Amendment privacy protections. In Miller, the Court found no Fourth Amendment search occurred when the Government obtained information conveyed to banks because that information was “voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”

Together, Smith and Miller have defined the third-party doctrine to mean that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,” even if “the information is revealed on the assumption that it will be only for a limited purpose and the confidence placed in the third party will not be betrayed.” Practically, this rule makes sense. A person cannot claim a legitimate expectation of privacy in information voluntarily conveyed to others. But one only gives up a reasonable privacy expectation through voluntary conveyance. Therefore, the operative phrase for determining whether the Fourth Amendment protects CSLI is “voluntary conveyance.” Unfortunately, an antiquated definition forces courts to fit modern facts into outdated precedent.

In an age where advances in technology have led to the ubiquity of cell phones, older definitions of voluntary conveyance are limited in application. For this reason, this Comment looks to the definitions used by the courts. For example, the Fifth Circuit’s definition relies on a chain of inferences similar to Smith, which the Court believes the conveyor is aware of:

[A] cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he

---

43. Id. at 742.
44. Id.
45. Id.
46. Id.
47. Id. at 746.
49. Smith, 442 U.S. at 743–44.
50. Miller, 425 U.S. at 443 (holding that a Fourth Amendment search does not occur when the government obtains records from banks including checks, deposit slips, and other information conveyed by bank customers to their banks because this information is “voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business”).
52. Id. at 354.
voluntarily conveys his cell site data each time he makes a call.\textsuperscript{53}

The Eleventh Circuit also defines voluntary conveyance as involving this inferential chain.\textsuperscript{54} In its panel decision, the Fourth Circuit defined voluntary conveyance as something more than an affirmative act.\textsuperscript{55} Unfortunately, the Fourth Circuit abandoned this straightforward definition in its \textit{En Banc Rehearing}:

A cell phone user voluntarily enters an arrangement with his service provider in which he knows that he must maintain proximity to the provider’s cell towers in order for his phone to function . . . . Whenever he expects his phone to work, he is permitting—indeed, requesting—his service provider to establish a connection between his phone and a nearby cell tower.\textsuperscript{56}

How can these definitions be correct in today’s modern age? Assuming “users know that they convey information about their location to their service providers when they make a call,”\textsuperscript{57} and that users are generally aware that data about the call are stored by service providers,\textsuperscript{58} can users be said to voluntarily convey their locations to those providers? Unfortunately, the \textit{En Banc Rehearing} has made it clear that current precedent binds the courts, forcing the answer to be a resounding yes.\textsuperscript{59} But users have no idea which cell sites transmit their communications or where those sites are located.\textsuperscript{60} Experts only know that the closest cell tower will usually transmit the data and that the data transmitted will be a location somewhere to the north, south, east, or west of the tower, so long as the cell phone is within a circular coverage area, which varies in size based on the strength of the particular tower’s signal.\textsuperscript{61} If that seems complicated, imagine a cell phone user actively attempting to convey specific CSLI to her cell service provider in a manner similar to a caller voluntarily conveying dialed numbers to a phone company or a customer voluntarily conveying information to a bank. She would need to know the location of her provider’s nearest cell tower, learn the signal strength and coverage area of that tower, stand in that coverage area, and hope that no other cell tower transmits her location instead.\textsuperscript{62}

Assuming that cell phone users know the intricacies of CSLI is unreasonable.\textsuperscript{63} Assuming they know the basics, less so; however, even

\begin{itemize}
\item \textsuperscript{53} In re Application, 724 F.3d 600, 614 (5th Cir. 2013).
\item \textsuperscript{54} United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015).
\item \textsuperscript{55} Graham, 796 F.3d at 355.
\item \textsuperscript{56} En Banc Rehearing, 824 F.3d 421, 430 (4th Cir. 2016).
\item \textsuperscript{57} In re Application, 724 F.3d at 612.
\item \textsuperscript{58} Davis, 785 F.3d at 511.
\item \textsuperscript{59} En Banc Rehearing, 824 F.3d at 432–33 (rejecting the defendant’s claim that the ubiquitous nature of cell phones and the accompanying CSLI should receive Fourth Amendment protection by concluding, “[u]ntil the [Supreme] Court says otherwise, these holdings bind us.”).
\item \textsuperscript{60} Graham, 796 F.3d at 356.
\item \textsuperscript{61} Davis, 785 F.3d at 501–02.
\item \textsuperscript{62} See id.
\item \textsuperscript{63} See Graham, 796 F.3d at 356; Davis, 785 F.3d at 501–02.
\end{itemize}
advanced knowledge about how service providers obtain CSLI is not enough for a user to reliably convey their location information.\textsuperscript{64} Because cell phone users do not voluntarily convey their location information\textsuperscript{65} and because there exists an expectation of privacy in users' locations, the \textit{En Banc Rehearing} necessitates legislative action explicitly requiring warrants for CLSI.

\textbf{B. This Nation Is Better Served by Extending Fourth Amendment Protections to CSLI}

Our democracy cannot allow Fourth Amendment protections to disappear simply because Supreme Court case law has not kept up with technology. In her concurrence in \textit{United States v. Jones}, Justice Sotomayor cautioned:

[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.\textsuperscript{66}

Cell phones are ubiquitous with life today.\textsuperscript{67} Over 90 percent of American adults own a cell phone\textsuperscript{68} with over 45 million of those Americans using cell phones as their primary Internet access device.\textsuperscript{69} These statistics are significant because service providers automatically generate CSLI based on connections between phones and their network without active participation by users.\textsuperscript{70} Moreover, the advent of smart phones has brought a dramatic increase in the relaying of location information not only when a user intentionally makes a call, text, or goes online, but also when she unintentionally has information “pushed” to her phone.\textsuperscript{71} Common examples of “pushed” information are when a cell phone user is sent an email, receives a text, updates an app automatically, or even when an app loads an ad.

In 2010, 62.6 million Americans used smart phones.\textsuperscript{72} In 2015, that number grew to 164.2 million and is expected to increase to 229.2 million in 2018.\textsuperscript{73} This means that in 2018, over 60 percent of the U.S. population will use

\begin{footnotesize}
\begin{enumerate}
\item See Davis, 785 F.3d at 501–02.
\item See supra Part II.A and accompanying discussion.
\item Graham, 796 F.3d at 355–56.
\item Mobile Technology Fact Sheet, PEW RES. CTR. (Dec. 27, 2013), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.
\item Graham, 796 F.3d at 354.
\item Id.
\end{enumerate}
\end{footnotesize}
smartphones. With smartphones comprising 77 percent of the traffic on today’s wireless networks, service providers will store over 60 percent of the population’s moment-by-moment locations by 2018.

Because cell phones have become a necessity to allow active participation in society, it is completely unreasonable to deem cell phone users as having voluntarily forfeited their expectations of privacy. Technology has changed so significantly that precedent is easily distinguished. It is no longer true that when people use their phones, they “voluntarily convey[] numerical information to the telephone company and ‘expose[]’ that information to its equipment in the ordinary course of business.” No modern cell phone user “assume[s] the risk” that their service provider will track their location with every connection and turn it over to the police when asked, and it is unconscionable for a court to expect citizens to choose between “full cultural and economic participation” and their right to privacy. In fact, it is common for people to hold the belief that simply owning a cell phone does not license the government to track them. Modern law enforcement needs do not justify using the third-party doctrine to extinguish phone users’ reasonable expectations of privacy, and the Legislature should ensure that courts can no longer apply the doctrine in such a way.

C. A Suggested Change to the Law

Changes to the law can occur by statute or by court decision; benefits exist for both. However, the Fourth Circuit recognized the Legislature’s unique ability to respond to technology’s fast pace, and technologies other than CSLI, such as Stingray Tracking Devices, would provide a more compelling platform for the Supreme Court to reconsider the third-party doctrine. For these reasons, this Comment urges the Legislature to revisit the Stored Communications Act (SCA) to better define the public’s privacy expectations in light of modern technology.

76. Compare Colby and Ortman, supra note 74, with Wireless Traffic Infographic, supra note 75 (with current network traffic comprised of 77 percent smartphone data, it is fair to believe the 60 percent of the population expected to be using smartphones will have their CSLI stored at ever increasing rates).
77. United States v. Graham, 796 F.3d 332, 355 (4th Cir. 2015).
79. Id.
80. Graham, 796 F.3d at 355.
81. United States v. Davis, 785 F.3d 498, 539 (11th Cir. 2015) (Martin, J., dissenting).
82. Graham, 796 F.3d at 357.
83. See supra text accompanying note 14; En Banc Rehearing, 824 F.3d 421, 436 (4th Cir. 2016) (“The legislative branch is far better positioned to respond to changes in technology than are the courts.”).
As an initial step to aligning Fourth Amendment protections with modern privacy interests, the Legislature should require warrants for the disclosure of CSLI by placing an explicit exception for CSLI into section 2703(d) of the SCA. By eliminating law enforcement’s option to choose between the higher standard of a warrant and the lower standard of a court order, the Legislature would extend Fourth Amendment privacy rights to CSLI. With such an amendment to the SCA, the third-party doctrine argument would no longer be applicable to a cell phone’s location information. And what would be the cost? Law enforcement would be forced to investigate until they can show probable cause for obtaining days, weeks, or months of constant location information. Requiring a warrant seems a fair cost for obtaining sensitive information through technological advancements that were unimaginable in 1791.

By forcing the Court to abandon the decades-old third-party doctrine argument as it applies to CSLI, the Legislature could set the stage for a federal statute modeled after California’s Electronic Communications Privacy Act (CalECPA). CalECPA “requires a probable cause warrant for all digital content, location information, metadata, and access to devices like cell phones.” A federal statute like CalECPA might draw the “reasonable distinctions based on categories of information” contemplated by Justice Alito in his concurrence to Riley v. California. Such distinctions would go a long way toward defining the Fourth Amendment protections today’s society expects of modern technology. Thus, exempting CSLI from court orders would be a narrowly tailored step toward enhancing privacy, but could pave the way to more comprehensive legislation and Fourth Amendment application in the near future.

85. See U.S. CONST. amend. IV (requiring “probable cause” before a court will issue a warrant).
86. 18 U.S.C. § 2703(d) (requiring reasonable suspicion before a court will issue a court order).
87. See supra Part II.A. The third-party doctrine is a justification for allowing disclosure of CSLI using the lower threshold of a court order. If the Legislature requires warrants to obtain CSLI, the doctrine has nothing to justify.
92. See Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring) (“I would reconsider the question presented here [whether the police may conduct a warrantless search of a cell phone seized from an individual who has been arrested] if either Congress or state legislatures, after assessing the legitimate needs of law enforcement and the privacy interests of cell phone owners, enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables.”)
CONCLUSION

In 2010, the Supreme Court cautioned that “[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.” 93 Well, emerging technology—especially cell phones capable of autonomously relaying constant location information—has made its role clear in the last six years. 94 Cell phone use is too common and relays CSLI too often to continue “evaluating its role in society.” 95 Let every incoming text message, Facebook notification, Instagram update, and Snapchat be a reminder to you; it is time for the Legislature to reestablish privacy rights by extending Fourth Amendment protections to your CSLI.

---

94. See supra Part II.B.
95. See supra Parts II.A–B.