2015

Warrantless Access to Cell Site Location Information Takes a Hit in the Fourth Circuit: The Implications of United States v. Graham for Law Enforcement

Wesley Cheng
New York County District Attorney's Office

CENTER FOR THE ADVANCEMENT OF PUBLIC INTEGRITY

Warrantless Access to Cell Site Location Information Takes a Hit in the Fourth Circuit:

The Implications of United States v. Graham for Law Enforcement

Wesley Cheng
Assistant Attorney General
Office of the New York State Attorney General

COLUMBIA LAW SCHOOL

CENTER FOR THE ADVANCEMENT OF PUBLIC INTEGRITY

About:

Author:
Wesley Cheng is an Assistant Attorney General for the New York State Attorney General's Office, Criminal Enforcement & Financial Crimes Bureau. Prior to his current position, Wesley was an Assistant District Attorney for the New York County District Attorney's Office and the Office of the Special Narcotics Prosecutor for the City of New York, and served as an Associate General Counsel at the Office of the Metropolitan Transit Authority Inspector General. He is also an instructor for the Intensive Trial Advocacy Program at the Benjamin N. Cardozo School of Law.

What is CAPI?
The Center for the Advancement of Public Integrity is a nonprofit resource center dedicated to improving the capacity of public offices, practitioners, policymakers, and engaged citizens to deter and combat corruption. Established as partnership between the New York City Department of Investigation and Columbia Law School in 2013, CAPI is unique in its city-level focus and emphasis on *practical* lessons and tools.

Published: November, 2015 by the Center for the Advancement of Public Integrity at Columbia Law School. At **www.law.columbia.edu/CAPI.**

This publication is part of our series of community contributions; articles and reports from our expert community of practitioners, policymakers, and civil society leaders. If you have public integrity expertise you would like to share, please contact us at **CAPI@law.columbia.edu**.

The views expressed here are those of the author. They do not necessarily reflect the views of the Center for the Advancement of Public Integrity at Columbia Law School, the New York State Department of Law or the Department's Division of Criminal Justice.

Warrantless Access to Cell Site Location Information Takes a Hit in the Fourth Circuit:

The Implications of *United States v. Graham* for Law Enforcement

On August 5, 2015 the Fourth Circuit created a major ripple in Fourth Amendment law by ruling that warrantless access to cell site location information (CSLI) over a lengthy period amounted to an unconstitutional search in *United States v. Graham*.[1] While the Fourth Court ultimately upheld the defendants' convictions by applying the Fourth Amendment's "Good Faith" exception, the ruling created a clear split from the Fifth and Eleventh Circuits, making consideration of the issue by the Supreme Court much more likely.[2]

This article focuses on the facts and the Fourth Amendment arguments of the majority, concurring and dissenting opinions in *Graham*.[3] It also looks at potential implications for other services that obtain metadata similar to CSLI. Finally, it concludes that, for the time being, warrants should not be needed to access historical cell site data in New York, but that in other jurisdictions where there is no bright-line rule, it may be best to err on the side of caution and obtain a warrant.

In Brief:

There is a circuit split about whether a legal expectation of privacy applies to CSLI.

Fifth and Eleventh Circuits:

- Fourth Amendment protections do not apply
- Investigators *may* obtain CSLI without a warrant

Fourth Circuit:

- Fourth Amendment protections apply
- Investigators *may not* obtain CSLI without a warrant

Second Circuit:

- No ruling by the circuit court
- Some district court judges within the Second Circuit have endorsed warrantless acquisition of CSLI
- Investigators *may* obtain CSLI without a warrant, but legality has not yet been established at the circuit level

What is historical cell site data?

Whenever an individual uses a cell phone, the phone connects with cell sites or "base stations," which send communications to and receive communications from the cell phone.[4] When a call is placed or received or a text message is sent or received by a phone, that phone connects to the cell site with the strongest signal, typically the nearest cell site.[5] If the phone physically moves through a particular coverage area, the cell phone may connect to different cell sites as it moves.[6] A service provider automatically retains a record of which cell site the cell phone was connecting to at any given time, thereby allowing investigators to "approximate the whereabouts of the cell phone at the particular points in the time in which transmissions are made."[7]

Cell site location data was used in the prosecutions of defendants Aaron Graham and Eric Jordan, who were charged in a pattern of armed robberies in the Baltimore area in 2011.[8] Police arrested Graham during the last robbery, and while executing a search warrant in his residence recovered a pair of cell phones.[9]

Investigators obtained two court orders directed at Sprint/Nextel for CSLI records of the phones to try to determine where the defendants were physically located at the time of the robberies.[10] While the initial court order authorized 14 days of data, the second one covered 221 days. In all, 29,659 location data points were obtained for Graham, and 28,410 were obtained for Jordan.[11] At trial, these records were admitted into evidence to show that the defendants were at, or near, the sites of several of the robberies, or that they were near each other during the string of robberies.[12] The defendants were found guilty after trial.[13]

Legal Analysis of *United States v. Graham*

Senior Judge Andre Davis, joined by Judge Stephanie Thacker, held that the government investigators' actions in obtaining CSLI for the extended period of time at issue here constituted an unreasonable search under the Fourth Amendment.[14] Ultimately, however, the majority upheld the use of the cell-site data because of the government's good faith in relying on the Stored Communications Act ("SCA") and two court orders.[15]

I. Judge Davis' majority opinion

The majority opinion breaks down into three separate parts: (1) Finding that obtaining historical cell site data in this case constituted a search;[16] (2) Outlining, and then rejecting, three counterarguments;[17] and (3) Ultimately ruling that the use of historical cell-site data fell under the Good Faith exception to the Fourth Amendment.[18]

"If anything, Judge Davis argued, the use of CSLI in the *Graham* case would reveal even more private information about an individual than the use of a GPS device as discussed in *Jones*"

In recognizing a privacy interest in the comprehensive accounts of one's movements and location over an extended period of time, Justice Davis drew his support from four Supreme Court cases. In *United States v. Knotts*, the Supreme Court deemed constitutional a search involving a radio transmitter to track the defendant's movements.[19] The search was upheld, however, only after the *Knotts* Court deemed it "limited" because it tracked only movements on public roads.[20] In *United States v. Karo*, the Court held that the same kind of radio transmitter was an unconstitutional search because the government was able to track movements in places where the suspect had a reasonable expectation of privacy.[21] In *Kyllo v. United States*, evidence obtained by a thermal imaging camera was suppressed because it allowed investigators to obtain information hidden inside a private home by using technology not in general use.[22]

These three cases form the backdrop for the Court's most recent ruling in *United States v. Jones*, where the Court concluded that a GPS device affixed to a vehicle constituted a search that required a warrant.[23] In suppressing evidence from the GPS device, the *Jones* Court reasoned that the information gathered over a 28-day period would reveal an "intimate" picture of an individual's life that society was not willing to accept as a reasonable intrusion.[24]

If anything, Judge Davis argued, the use of CSLI in the *Graham* case would reveal even more private information about an individual than the use of a GPS device as discussed in *Jones*.[25] The kind of tracking in *Jones* was limited to the use of an automobile on public roads.[26] In contrast, a cell phone stays with a person the majority of the time, and gives the ability to monitor an individual's movements in private spaces that an automobile would not be able to access.[27] The cell phone in *Graham*, then, was more like the beeper in *Karo* and *Knotts*, allowing investigators to track an individual in a "home" and "other private locations" at any given time.[28] Additionally, like in *Kyllo*, CSLI is not a technology in general use, and therefore the majority opinion deemed this a search within the meaning of the Fourth Amendment.[29]

Of particular note in the decision was the "extended" period of time for which the government obtained CSLI.[30] During the 14 and then 221 days that investigators obtained CSLI in the *Graham* case, there was a high probability that the CSLI tracked the phone user's movements in private spaces.[31] Thus, for "an extended time period like 14 or 221 days," the government had engaged in a Fourth Amendment search.[32] The Court did not, however, enact a bright-line rule specifying how many days, hours or minutes would constitute a search.[33]

Judge Davis next responded to three main counterarguments presented by the government: (1) that the privacy policy at Sprint/Nextel gave users notice of the collection of CSLI;[34] (2) that the third party doctrine allowed for a warrantless search;[35] and (3) that CSLI was less intrusive than other forms of electronic surveillance.[36]

First, the government argued that, by accepting Sprint/Nextel's terms of use for its cell phones, the defendants waived any expectation of privacy.[37] Specifically, the user agreement stated that the device would collect information about "where it (the cell phone) is located."[38] Judge Davis rejected this claim, finding that the user only agreed to Sprint/Nextel collecting the information, not sharing it with the government.[39] Furthermore, there was no evidence that the defendants "read or understood" the policy.[40]

Judge Davis next determined that the third-party doctrine was inapplicable to the facts of the *Graham* case.[41] In *United States v. Miller* (bank records) and *Smith v. Maryland* (pen register), the United States Supreme Court held that a person relinquishes any reasonable expectation of privacy in information conveyed to a third party.[42] Judge Davis noted that these cases were inapplicable because cell phone users did not "voluntarily convey their CSLI to their service providers."[43] Instead, cell phones automatically connected to the provider's network, at times "without the user's active participation."[44]

Finally, the majority opinion rejected the government's argument that CSLI was less intrusive than a real-time GPS that allowed investigators to track a suspect 24 hours a day.[45] Judge Davis called this argument "constitutionally insignificant" because had the defendants been constantly using their phones, the CSLI would have approached the level of monitoring of a GPS.[46] Indeed, the data points received by investigators in this case amounted to well over 100 per day on average.[47]

Having deemed the CSLI the fruits of an unlawful search, Judge Davis nevertheless declined to apply the exclusionary rule because of the Good Faith exception.[48] The government, Judge Davis wrote, had a good faith reliance on the SCA as well as the two judicially authorized orders for obtaining CSLI.[49] The government did not obtain the order under a "clearly unconstitutional" statute, nor was the issuance of the order "clearly defective."[50] Thus, the majority opinion affirmed the lower court and denied the defendants' motion to suppress.[51]

II. Judge Thacker's concurrence

The concurring opinion focused on Judge Thacker's concern for the "erosion of privacy in this era of rapid technological development."[52] More than two-thirds of Americans own smartphones now, and these phones can be used to track an individual regardless of whether or not the person is actually using his phone.[53] Thus, Judge Thacker wrote, it is better for judges to err on the side of protecting individual rights and privacy.[54] After all, "obtaining a warrant is the rule, not the exception."[55]

"[O]btaining a warrant is the rule, not the exception."

– Judge Stephanie Thacker

III. Judge Motz's dissent

In her dissent, Judge Diana Gribbon Motz followed the reasoning of the Fifth and Eleventh Circuits, both of which found that there was no search within the confines of the Fourth Amendment when it came to CSLI.[56] Judge Motz argued that the majority erroneously relied on cases (*Jones*, *Karo* and *Kyllo*) that involved direct conduct intrusions by the government rather than the conduct of a third party.[57] According to Judge Motz, the question was better framed as a third-party doctrine case, and when, as in *Graham*, CSLI had clearly been turned over to a third party, that information should not be subject to the protections of the Fourth Amendment.[58]

Judge Motz also rejected the majority's argument that cell phone users are unaware that they are conveying information to a cell tower as they carry and use their phones.[59] She determined that by the very nature of expecting a cell phone to work, a cell phone user is necessarily voluntarily conveying information such as CSLI.[60]

Judge Motz also argued that the majority did not properly analyze what kind of data the government was receiving with CSLI.[61] She noted the difference between actual content of communications (emails, wiretaps) and non-content information about the communication (email metadata, pen registers).[62] Judge Motz determined that the majority had mistakenly ruled that CSLI should be afforded the same protection as is applied to content communication, when in reality CSLI "undeniably" belongs in the non-content category.[63]

Judge Motz concluded by opining that the Supreme Court and/or Congress should be the first to strike the "proper balance between technology and privacy."[64]

Read the Rulings:

Fourth Circuit:
United States v. Graham, 2015 U.S. App. (4th Cir. 2015)

Fifth Circuit:
In re: Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013)

Eleventh Circuit:
United States v. Davis, 2015 U.S App. (5th Cir. 2015)

Legal Significance of the Opinion

The most obvious consequence of the *Graham* opinion is now there is a split among the circuits on whether a legal expectation of privacy applies to CSLI. The Fifth and Eleventh Circuits both found that the third party doctrine applied to CSLI and therefore that Fourth Amendment protections did not apply to CSLI, while the Fourth Circuit in the present case has ruled that the Fourth Amendment does apply, requiring investigators to obtain a warrant to receive CSLI.[65] The defendant in the Eleventh Circuit case filed a writ of certiorari in July, 2015,[66] which may result in Supreme Court review.

In terms of the law in New York, the Second Circuit has yet to rule, but the Southern District of New York has endorsed the warrantless acquisition of CSLI on a similar theory to that of the third party doctrine.[67] On the state level, the Court of Appeals has not addressed the issue, but the First Department ruled that a warrant was not necessary for CSLI in *People v. Hall*.[68]

Another issue that will need to be resolved in the future is what constitutes an overly extended period of time as it relates to CSLI. Judge Davis noted that even the 14 days of the first data period was enough time to constitute a search requiring investigators to obtain a warrant.[69] The majority opinion, however, did not provide a bright line rule on the length of time short of 14 days that would turn the collection of CSLI into a search.[70] The *Hall* court did not reach this issue either, but did take note that if prolonged surveillance required a warrant under federal law, three days of CSLI records would not "constitute a protracted surveillance."[71]

CSLI is only the tip of the iceberg in this area. As technology advances, more and more services are collecting personal data on users. For example, online streaming provider Netflix keeps track of a user's personal preference for movies. The recently released Apple Watch has the ability to track an individual much in the same way that smartphones can. eBay and Amazon track personal shopping habits. Thus, any ruling that deals with this sort of passive metadata collection will have a significant impact on the development of the law.

Impact on Practitioners

The *Graham* decision – or something factually and legally similar -- will likely make its way to the Supreme Court at some point. The split in the circuits in this area necessitates an eventual ruling. However, until that decision is rendered, there are bright-line rules in the Fourth, Fifth and Eleventh Circuits, and practitioners should follow the rules in their jurisdictions. In New York, the Second Circuit and the Court of Appeals have not ruled on the matter, but lower courts have endorsed government investigators obtaining CSLI data without a warrant.

Endnotes

[1] *See United States v. Graham*, 2015 U.S. App. LEXIS 13653 (4th Cir. 2015).
[2] *Compare United States v. Graham*, 2015 U.S. App. LEXIS 13653 (4th Cir. 2015) (requiring a warrant for historical cell site orders), with *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (government can access cell site records without a warrant), *and United States v. Davis*, 779 F.3d 1305 (11th Cir. 2015) (same).
[3] The 134 page opinion touches on a variety of other subjects related to the defendants' convictions, but this article only addresses the Fourth Amendment issue that arise from the use of CSLI.
[4] *See Graham*, 2015 U.S. App. LEXIS 13653 at *15-16.
[5] *Id.* at *16.
[6] *Id.* at *16-17.
[7] *Id.*
[8] *Id.* at *3-4.
[9] *Id.* at *8.
[10] *Id.* at *9-10.
[11] *Id.* at *35.
[12] *Id.* at *11.
[13] *Id.* at *2.
[14] *Id.*
[15] *Id.*
[16] *Id.* at *33.
[17] *Id.* at *34-67.
[18] *Id.* at *67-68.
[19] *See United States v. Knotts*, 460 U.S. 276 (1983) (holding that a person traveling in public has no expectation of privacy in his movements. In *Knotts*, a 'beeper' device attached to a drum inside the defendant's vehicle was determined not to have violated a legitimate expectation of privacy; it was also found that the beeper's installation did not require a warrant).
[20] *See Graham*, 2015 U.S. App. LEXIS 13653 at *22. Although the government tracked the container to a defendant's private home, there was no indication that the officers continued to monitor the container inside the private space after its public journey had ended. *Id.* (citing *Knotts*, 460 U.S. at 285).
[21] *See United States v. Karo*, 468 U.S. 705 (1984) (finding the installation of a beeper in a can of ether did not constitute a "search' or "seizure," and the Fourth Amendment was not implicated until the beeper was turned on and used to track the ether shipment on private property).
[22] *See Kyllo v. United States*, 533 U.S. 27 (2001) (holding that the use of a thermal imaging sensor from a public area to monitor the radiation of heat from a home was a search under the Fourth Amendment).
[23] *See United States v. Jones*, 132 S. Ct. 945 (2012) (holding that surreptitious physical installation of a tracking device on defendant's car establishes an intrusion of a constitutionally protected area).
[24] *See Graham*, 2015 U.S. App. LEXIS 13653 at *25-26. Often referred to as the "Mosaic Theory," the Court stated that a reasonable individual would not expect that the sum of her movements in public over a month would be observed by a stranger, and (2) this information could reveal "an intimate picture" of her life not disclosed by any one of her movements viewed individually. *Id.* (citing *Jones*, 132 S. Ct. at 948).
[25] *See Graham*, 2015 U.S. App. LEXIS 13653 at *29.
[26] *See id.* at *29 (citing *Jones*, 132 S. Ct. at 948).
[27] *See id.*at *29.

[28] *Id.* at *33.
[29] *Id.*
[30] *Id.*
[31] *Id.* It is possible that the CSLI for a particular cell phone may not be very revealing at all because, for instance, the phone has been turned off or it has made few or no connections to the cellular network. *Id.* But the government cannot know in advance of obtaining this information how revealing it will be or whether it will detail the cell phone user's movements in private spaces. *Id.*
[32] *Id.*
[33] *Id.* at *33 n.8. "This case does not require us to draw a bright line as to how long the time period for historical CSLI can be before its inspection rises to the level of a Fourth Amendment search, and we decline to do so." *Id.*
[34] *Id.* at *20-21.
[35] *Id.* at *41-43.
[36] *Id.* at *34-39.
[37] *Id.* at *20-21.
[38] *Id.* The pertinent part of the privacy policy of Sprint/Nextel is as follows: "Information we collect when we provide you with Services includes when your wireless device is turned on, how your device is functioning, device signal strength, where it is located, what device you are using, what you have purchased with your device, how you are using it, and what sites you visit." *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.* at *41-43.
[42] *See Smith v. Maryland*, 442 U.S. 735 (1979) (holding that a pen register is not a search because the defendant voluntarily conveyed numerical information to the telephone company); *United States v. Miller* 425 U.S. 435 (1976) (holding that there is no legitimate expectation of privacy in the contents of the original checks and deposit slip because they were information revealed to a third party).
[43] *See Graham*, 2015 U.S. App. LEXIS 13653 *48. Notably, the CSLI at issue in *Graham* details location information not only for those transmissions in which defendants actively participated — *i.e.*, messages or calls they made or answered — but also for messages and calls their phones received but they did not answer. *Id.* When a cell phone receives a call or message and the user does not respond, the phone's location is identified without any affirmative act by its user at all — much less, "voluntary conveyance." *Id.* (citing *In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 317 (3d Cir. 2010)).
[44] *Id.* at *47.
[45] *Id.* at *34-39.
[46] *Id.* at *35. The quantum of data collected in *Graham* is substantial enough to provide a reasonably detailed account of defendants' movements during the collection period, including movements to and from the cell-site sectors in which their homes were located. *Id.*
[47] *Id.*
[48] *Id.* at *66.
[49] *Id.* at *67.
[50] *Id.* at *67-68. The government's first § 2703(d) application requested data regarding calls and messages to and from defendants' phones during four time periods and described robberies under investigation that occurred during some of those time periods. *Id.* After learning about other similar robberies, the government submitted a second application to request records for the much broader 221-day time frame. *Id.* The second application included the same facts provided in the first application but added descriptions of additional robberies under investigation. *Id.* The defendants do not claim that the government was "dishonest or reckless" in preparing either application. *Id.*
[51] *Id.* at *72.
[52] *Id.* at *108 (Thacker, J., concurring). Cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."
[53] *Id.* at *108-09. (citing *Riley v. California*, 134 S. Ct. 2473, 2484 (2014)).
[54] *Id.* at *111.
[55] *Id.*
[56] *Id.* at *112 (Motz, J., dissenting).
[57] *Id.* at *113-14. As Judge Motz explained, the only government "activity" here is its acquisition from a phone company, Sprint/Nextel, of CSLI records -- *i.e.*, the records that the phone company created that identify which cell towers it used to route defendants' calls and messages. *Id.* The government did not surreptitiously view, listen to, record, or in any other way engage in direct surveillance of defendants to obtain this information. *Id.* Rather, it was Sprint/Nextel alone that obtained the information and generated the business records that defendants now claim are constitutionally protected. *Id.* The nature of the governmental activity here thus critically distinguishes this case from those on which the majority relies -- cases in which the government did surreptitiously collect private information. *Id.*
[58] *Id.* at *116-17. "Applying the third-party doctrine to the facts of this case, I would hold that Defendants did not have a reasonable expectation of privacy in the CSLI recorded by Sprint/Nextel." *Id.* "The Supreme Court's reasoning in *Smith* controls." *Id.*
[59] *Id.* at *123. "When an individual purchases a cell phone and chooses a service provider, he expects the provider will, at a minimum, place outgoing calls, send text messages, and route incoming calls and messages. . . . As most cell phone users know all too well, however,

proximity to a cell tower is necessary to complete these tasks." *Id.* "Anyone who has stepped outside to 'get a signal,' or has warned a caller of a potential loss of service before entering an elevator, understands, on some level, that location matters." *Id.*

[60] *Id.* at *124. "Whenever he expects his phone to work, he is thus permitting -- indeed, requesting -- his service provider to establish a connection between his phone and a nearby cell tower." *Id.*

[61] *Id.* at *132-34.

[62] *Id.* "What the majority fails to acknowledge is that for each medium of communication these cases address, there is also a case expressly withholding Fourth Amendment protection from non-content information, i.e., information involving addresses and routing." *Id.*

[63] *Id.*

[64] *Id.* at *144.

[65] *See In re Application*, 724 F.3d at 600 (5th Cir. 2013). *Davis*, 779 F.3d at 1305.

[66] The writ was filed on July 30, 2015, *see*, www.aclu.org/sites/default/files/field_document/us_v_davis_cert_petition.pdf, (last visited 08/31/15).

[67] *See United States v. Serrano*, 2014 U.S. Dist. LEXIS 81478 (S.D.N.Y. Jun. 10, 2014). The Second Circuit has not yet directly addressed whether there is a reasonable expectation of a privacy interest in the type of historical cell site information at issue here. *Id.* at *8. The Second Circuit has, however, held that there is no reasonable expectation of privacy in information provided to third parties in light of the general principles set forth in *Smith* and *Miller*. *Id* (citation omitted). "There is no recognized privacy interest in information provided to third-party vendors […] and it is uncontested that the particular cell site information here at issue relates to data obtained as calls were made from the subject cell phone." *Id.* at 19-20 (citing Miller, 425 U.S at 442). "Thus, the cell site information is analogous to registers of calls as to which there is no cognizable privacy interest." *Id.* at 19.

[68] *See People v. Hall*, 86 A.D.3d 450 (1st Dept. 2011) (holding that obtaining CSLI information for a three-day period does not require that the People establish probable cause or obtain a warrant).

[69] *See Graham*, 2015 U.S. App. LEXIS 13653 at *33.

[70] *Id.* at *33 n.8.

[71] *See Hall*, 86 A.D.3d at 517.

CENTER FOR THE ADVANCEMENT OF PUBLIC INTEGRITY

Columbia Law School
435 West 116th Street
New York, NY 10027

Email | CAPI@law.columbia.edu
Phone | (212) 854-6186
Website | www.law.columbia.edu/CAPI
Twitter | @ColumbiaCAPI