University of Miami Law Review

Volume 70
Number 4 *Volume 70 Number 4 (Summer 2016)*

Article 7

8-1-2016

That '70s Show: Why the 11th Circuit was Wrong to Rely on Cases from the 1970s to Decide a Cell-Phone Tracking Case

David Oscar Markus

Nathan Freed Wessler

That '70s Show: Why the 11th Circuit was Wrong to Rely on Cases from the 1970s to Decide a Cell-Phone Tracking Case

DAVID OSCAR MARKUS AND NATHAN FREED WESSLER

In light of society's increasing reliance on technology, this article explores a critical question – that of the Fourth Amendment's protection over privacy in the digital age. Specifically, this article addresses how the law currently fails to protect the privacy of one's cell phone records and its ramifications. By highlighting the antiquated precedent leading up to the Eleventh Circuit's ruling in United States v. Davis*, this article calls on the judiciary to find a more appropriate balance for protecting the right to privacy in a modern society.*

INTRODUCTION

When the Stored Communications Act ("SCA") was passed in 1986, cell phones cost over $3,000 and were the size of a brick.[1] Less than one-half of one percent of the U.S. population owned one.[2] There were only 1,000 cell phone towers in the United States.[3] A lot has changed since then. Now, almost everyone carries a cell phone, which can be tracked by our Government.

In Quartavius Davis's case, as in thousands of cases each year, the government sought and obtained the cell phone location data of a private individual pursuant to a disclosure order under the Stored Communications Act (SCA) rather than by securing a warrant.[4] Under the SCA, a disclosure order does not require a finding of probable cause.[5] Instead, the SCA authorizes the issuance of a disclosure order whenever the government "offers specific and articulable facts

---

[1] *See* Stephanie Buck, *Cell-ebration! 40 Years of Cellphone History*, MASHABLE (Apr. 3, 2013), http://mashable.com/2013/04/03/anniversary-of-cell-phone/#yNM8b.X2DEqX.

[2] *See* Andrea Meyer, *30th Anniversary of the First Commercial Cell Phone Call*, VERIZON (Oct. 11, 2013), https://www.verizonwireless.com/news/article/2013/10/30th-anniversary-cell-phone.html.

[3] *See id.*

[4] United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc). Mr. Davis's first name was misspelled in the case caption. It is Quartavius, not Quartavious. *Id.* at 500 n.1.

[5] *Id.* at 502.

showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation."[6]

As a result, the district court never made a probable cause finding before ordering Davis' service provider to disclose 67 days of Davis' cell phone location records, including more than 11,000 separate location data points.[7] Reversing a unanimous panel opinion, a majority of the *en banc* Eleventh Circuit held that there is no reasonable expectation of privacy in these location records and, even if there were such an expectation, a warrantless search would be reasonable nonetheless.[8]

The Eleventh Circuit's reasoning in *Davis* was wrong—the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 67 days is not permitted by the Fourth Amendment.

I. THE CASE OF *UNITED STATES V. DAVIS*

United States v. Davis presents a critical question: does the Fourth Amendment prevent the warrantless acquisition of electronic records which reveal the locations and movements of people over time?[9]

Davis' petition for certiorari summarized the facts of the case as follows:

> In February 2011, in the course of an investigation into seven armed robberies that occurred in the greater Miami area in 2010, an Assistant United States Attorney submitted to a federal magistrate judge an application for an order granting access to 67 days of Quartavius Davis's historical cell-phone location records. The application, which was unsworn, did not seek a warrant based on probable

---

6 18 U.S.C. § 2703(d) (2012).
7 *Davis*, 785 F.3d at 502–03, 505–06.
8 *Id.* at 516–18.
9 *Id.* at 500.

cause, but rather an order under the Stored Communications Act, 18 U.S.C. § 2703(d). Such an order may issue when the government offers specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation.

The application sought to compel a number of cellular service providers to disclose records related to several suspects in the robberies, including Davis. Specifically, the application sought stored telephone subscriber records, and phone toll records, including the corresponding geographic location data (cell site). The application recited information regarding robberies of retail businesses that occurred on August 7, August 31, September 7, September 15, September 25, September 26, and October 1, 2010, in and around Miami, Florida, and asserted that the records sought were relevant to the investigation of those offenses. Rather than restricting the request to only the days on which the robberies occurred, however, the application sought records for the period from August 1, 2010 through October 6, 2010, a total of 67 days.

The magistrate judge issued an Order for Stored Cell Site Information on February 2, 2011. The order directed MetroPCS, Davis's cellular service provider, to produce all telephone toll records and geographic location data (cell site) for Davis's phone for the period of August 1 through October 6, 2010. MetroPCS complied, providing 183 pages of Davis's cell phone records to the government. Those records show each of Davis's incoming and outgoing calls during the 67-day period, along with the cell tower ("cell site") and directional sector of the tower that Davis's phone connected to at the start and end of most of the calls, which was typically the nearest and strongest tower.

> MetroPCS also produced a list of its cell sites in Florida, providing the longitude, latitude, and physical address of each cell site, along with the directional orientation of each sector antenna. By cross-referencing the information in Davis's call detail records with MetroPCS's cell-site list, the government could identify the area in which Davis's phone was located and could thereby deduce Davis's location and movements at multiple points each day.[10]

The size of the cell site sectors in a particular area is a substantial determinant in the precision of a cell phone user's location as reported in cell site location information ("CSLI") records.[11] While the existence of towers with six sectors is becoming more prevalent, most cell sites contain three directional antennas, dividing the cell site into three sectors.[12] In geographic areas in which there is a greater density of cell towers, the coverage area of each cell site sector is smaller. As a result, urban areas that have the greatest density have the smallest coverage areas.[13]

As data usage grows with the increasing adoption of smartphones, cell site density continues to increase.[14] Carriers must erect additional cell sites to accommodate increased usage for text messages, emails, web browsing, streaming video, etc., as each cell site accommodates a fixed volume of data.[15] As a result, in dense

---

[10] Petition for Certiorari, *Davis v. United States*, 2015 WL 4607865, at *4-*6 ("*Davis* Petition"). The authors of this article were counsel for Mr. Davis on his petition for certiorari. This article expands on their work in the petition.

[11] Brief for American Civil Liberties Union, et al. as Amici Curiae in Support of Defendant-Appellant at 9, United States v. Davis, No. 12-12928 (11th Cir. Jun 01, 2012).

[12] *Davis*, 785 F.3d at 541 (Martin, J., dissenting).

[13] *Id.* at 503. For example, in 2010, MetroPCS, the carrier used by Davis, operated a total of 214 cell sites comprising 714 sector antennas within Miami-Dade County. *See* Brief for American Civil Liberties Union, *supra* note 21, at 14.

[14] *See Annual Wireless Industry Survey*, CTIA (June 2015), http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.

[15] *See id.* (showing that the number of cell sites in the United States nearly doubled from 2003 to 2013). *Id.* (wireless data usage increased by 9,228% between 2009 and 2013).

urban and suburban areas such as Miami, there are numerous sectors that cover small geographic areas, which as a result offer fairly precise information about a phone's location.[16]

In this particular case, the information provided by MetroPCS consisted solely of information identifying Davis's cell site and sector at the beginning and end of his calls. But carriers are developing the capability to store ever more precise location data. [17] As carriers implement millions of "small cells," which provide service to areas as small as ten meters, location precision is further increasing.[18] These "small cells" permit callers to be located with a "'high degree of precision, sometimes effectively identifying individual floors and rooms within buildings.'"[19]

In this case, the government obtained call detail records from Davis' phone that contained a wealth of location data. The "CSLI" provided by these records pertained to 5,803 phone calls, and revealed 11,606 individual location data points (because cell site location information was recorded at the start and end of each of the calls).[20] "This averages around one location data point every five and one half minutes for those sixty-seven days, assuming Mr. Davis slept eight hours a night."[21] Much sensitive and private information about Davis was revealed through this information about his locations, movements, and associations:

> The amount and type of data at issue revealed so much information about Mr. Davis's day-to-day life that most of us would consider quintessentially private. For instance, on August 13, 2010, Mr. Davis made or received 108 calls in 22 unique cell site sectors, showing his movements throughout Miami during that day. And the record reflects that many phone calls began within one cell site sector and ended in

---

[16] *See Davis*, 785 F.3d at 503.

[17] *See, e.g.*, Verizon Wireless, *Law Enforcement Resource Team (LERT) Guide*, PUB. INTELLIGENCE (Apr. 20, 2009), http://publicintelligence.net/verizon-wireless-law-enforcement-resource-team-lert-guide/ (providing sample records indicating caller's distance from cell site to within .1 of a mile).

[18] Brief for American Civil Liberties Union, *supra* note 11, at 10–11.

[19] *Id.*

[20] *Davis*, 785 F.3d at 533 (Martin, J., dissenting).

[21] *Id.* at 540 (Martin, J., dissenting).

> another, exposing his movements even during the course of a single phone call.
>
> Also, by focusing on the first and last calls in a day, law enforcement could determine from the location data where Mr. Davis lived, where he slept, and whether those two locations were the same. As a government witness testified at trial, "if you look at the majority of . . . calls over a period of time when somebody wakes up and when somebody goes to sleep, normally it is fairly simple to decipher where their home tower would be." Trial Tr. 42, Feb. 7, 2012, ECF No. 285. For example, from August 2, 2010, to August 31, 2010, Mr. Davis's first and last call of the day were either or both placed from a single sector—purportedly his home sector. But on the night of September 2, 2010, Mr. Davis made calls at 11:41pm, 6:52am, and 10:56am—all from a location that was not his home sector. Just as Justice Sotomayor warned [in *United States v. Jones*, 132 S. Ct. 945 (2012)], Mr. Davis's "movements [were] recorded and aggregated in a manner that enable[d] the Government to ascertain, more or less at will, . . . [his] sexual habits, and so on." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).[22]

As a result of this substantial invasion of Davis's privacy, he moved before trial to suppress these CSLI records, arguing that the government needed a warrant to obtain the records under the Fourth Amendment.[23] The district court summarily denied David's motion at the conclusion of the suppression hearing. The court indicated that it would subsequently issue a written opinion.[24] During trial, Davis renewed the suppression motion, but it again was summarily

---

[22] *Id.* at 540–41 (Martin, J., dissenting).

[23] *Id.* at 503.

[24] United States v. Davis, 754 F.3d 1205, 1209 (11th Cir. 2014).

denied by the court with the promise of a subsequent written opinion.[25] The court never issued any written opinion explaining its denial of the motion.[26]

The case proceeded to trial:

> At trial, the government introduced the entirety of Davis's CSLI records as evidence, and relied on them to establish Davis's location on the days of the charged robberies. A detective with the Miami-Dade Police Department testified that Davis's CSLI records placed him near the sites of six of the robberies. The detective also produced maps showing the location of Davis's phone relative to the locations of the robberies, which the government introduced into evidence. Thus, the government relied upon the information it got from MetroPCS to specifically pin Mr. Davis's location at a particular site in Miami. The prosecutor asserted to the trial judge, for example, that Mr. Davis's phone was literally right up against the America Gas Station immediately preceding and after the robbery occurred, and argued to the jury in closing that the records put Davis literally right on top of the Advance Auto Parts one minute before that robbery took place.
>
> The jury convicted Davis of two counts of conspiracy to interfere with interstate commerce by threats or violence in violation of the Hobbs Act, 18 U.S.C. § 1951(a); seven Hobbs Act robbery offenses; and seven counts of using, carrying, or possessing a firearm in each robbery in violation of 18 U.S.C. § 924(c). All but the first of the § 924(c) convictions carried mandatory consecutive minimum sentences of 25 years each. As a result, the court sentenced Davis to nearly 162 years' imprisonment. The court stated at sentencing that in light of Davis's young age (18 and 19 years old at the time of the offenses) and

---

[25] *Id.*
[26] *Id.*

> the nature of the crimes, the court believed a sentence of 40 years would have been appropriate. Because the court was afforded no discretion in sentencing, however, it sentenced Davis to 162 years in prison.[27]

On appeal to the Eleventh Circuit, a unanimous three-judge panel held that the government violated Davis's Fourth Amendment rights by requesting and obtaining his historical cell site location information without a warrant.[28] Judge Sentelle,[29] the opinion's author, stated that Davis had a reasonable expectation of privacy in his CSLI because this data revealed information about his whereabouts in private locations, thereby "convert[ing] what would otherwise be a private event into a public one."[30] As the opinion explained, "[t]here is a reasonable privacy interest in being near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute."[31] It further held that the cellular carrier's possession of Davis's CSLI did not deprive Davis of a reasonable expectation of privacy in that information because his location was not voluntarily provided to MetroPCS.[32] The Eleventh Circuit nonetheless affirmed the district court's denial of Davis's suppression motion on the basis that the government relied in good faith on the magistrate judge's order issued under the Stored Communications Act. It found that the exclusionary rule therefore did not apply.[33]

On *en banc* rehearing, a divided Eleventh Circuit vacated the panel opinion.[34] In the majority opinion, Judge Hull held that Davis

---

[27] Davis Petition at *10-*11 (internal quotations and citations omitted).

[28] *Id.* at 1217.

[29] Judge Sentelle sat on the panel by designation from the D.C. Circuit. Judges Martin and Dubina joined Judge Sentelle's opinion.

[30] *Davis*, 754 F.3d at 1216.

[31] *Id.*

[32] *Id.* at 1217.

[33] *Id.* at 1217–18.

[34] *See* Petition for a Writ of Certiorari at 12 n.10, Quartavious Davis v. United States of America, 785 F.3d at 541 (No. 15-146) ("Only one member of the original panel participated in *en banc* reconsideration. Judge Sentelle was not permitted to participate because he had participated in the panel as a visitor from the D.C. Circuit. Judge Dubina has taken senior status, and opted not to participate in

had no reasonable expectation of privacy in cell phone location records held by MetroPCS, and therefore no Fourth Amendment search occurred.[35] Judge Hull concluded that use of an SCA order rather than a warrant is reasonable, even if there was a Fourth Amendment search, because of the government's compelling interest in investigating crimes and because the privacy intrusion was minor.[36]

Five of the *en banc* court's eleven judges diverged from this reasoning. Judge Jordan, joined by Judge Wilson, wrote separately to express the concern that

> [a]s technology advances, location information from cellphones (and, of course, smartphones) will undoubtedly become more precise and easier to obtain, and if there is no expectation of privacy here, I have some concerns about the government being able to conduct 24/7 electronic tracking (live or historical) in the years to come without an appropriate judicial order.[37]

Although Judge Jordan did not join the court's conclusion that there is no reasonable expectation of privacy in CSLI records, he concurred that (if conducted with an SCA order) a search of CSLI is reasonable.[38]

Judge Rosenbaum also wrote separately, offering a note of caution:

> In our time, unless a person is willing to live "off the grid," it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic

---

en banc reconsideration. *See* 11th Cir. R. 35-10."). *See also* United States v. Davis, 785 F.3d 498 (11th Cir. 2015).

[35] *Davis,* 785 F.3d at 515–16.

[36] *Id.* at 517–18. The court held in the alternative that the good-faith exception to the exclusionary rule applies. *Id.* at 518 n.20.

[37] *Id.* at 521 (Jordan, J., concurring).

[38] *Id.* at 522–23 (Jordan, J., concurring).

> protection that a warrant offers is nothing less than chilling.[39]

In a dissenting opinion, Judge Martin, joined by Judge Jill Pryor, contended that there is a reasonable expectation of privacy in CSLI, and that the government should be required to obtain a warrant before accessing this information.[40]

II. THE ELEVENTH CIRCUIT'S DECISION WAS WRONG.

In two recent landmark cases, the Supreme Court has addressed critical questions regarding how the Fourth Amendment should be applied in the digital age.[41] These cases, however, leave open the critical question of whether historical cell phone location records held by a service provider are protected by the warrant clause of the Fourth Amendment.

As Justice Sotomayor's concurrence in *United States v. Jones* discussed, location records reveal extraordinarily sensitive details of a person's life, "reflect[ing] a wealth of detail about her familial, political, professional, religious, and sexual associations."[42] Yet the Eleventh Circuit analogized to the rather limited analog data that had been addressed in the Supreme Court's third-party records decisions from the 1970s, and held that voluminous, digitized historical location records are unprotected by the Fourth Amendment.[43] This was, perhaps, unwise, as the Supreme Court recently cautioned that "any extension of . . . reasoning [from decisions concerning analog searches] to digital data has to rest on its own bottom."[44] The Eleventh Circuit nonetheless relied blindly on "pre-digital analogue[s]" risks causing "a significant diminution of privacy."[45]

---

[39] *Id.* at 525 (Rosenbaum, J., concurring).

[40] *Id.* at 533 (Martin, J., dissenting).

[41] *See generally* Riley v. California, 134 S. Ct. 2473 (2014) (warrant required for search of cell phone seized incident to lawful arrest); *see also* United States v. Jones, 132 S. Ct. 945, 948 (2012) (tracking car with GPS device is a Fourth Amendment search).

[42] *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

[43] *Davis*, 785 F.3d at 507–08 (citing Smith v. Maryland, 442 U.S. 735 (1979) and United States v. Miller, 425 U.S. 435 (1976)).

[44] *Riley*, 134 S. Ct. at 2489.

[45] *Id.* at 2493.

In seeking certiorari from the Supreme Court, Davis summarized the Court's precedent as follows:

> In *United States v. Jones*, the Supreme Court addressed the pervasive location monitoring made possible by GPS tracking technology surreptitiously and warrantlessly attached to a vehicle.[46] All members of the Court agreed that attaching a GPS device to a vehicle and tracking its movements constitutes a search under the Fourth Amendment.[47] In so holding, the Court made clear that the government's use of novel digital surveillance technologies not in existence at the framing of the Fourth Amendment does not escape the Fourth Amendment's reach.[48]
>
> In *Riley v. California*, the Court addressed Americans' privacy rights in the contents of their cell phones, unanimously holding that warrantless search of the contents of a cell phone incident to a lawful arrest violates the Fourth Amendment.[49] In so doing, the Court rejected the government's inapt analogy to other physical objects that have historically been subject to warrantless search incident to an arrest.[50]
>
> [*Davis* and similar cases] raise a hotly contested question that sits at the confluence of *Jones* and *Riley*: whether the pervasive location data generated by

---

[46] *Jones*, 132 S. Ct. at 948.

[47] *See generally Jones*, 132 S. Ct. at 945.

[48] *Jones*, 132 S. Ct. at 950–51 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) ("we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"); *See also id.* at 964 ("society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period") (Alito, J., concurring in the judgment).

[49] Riley v. California, 134 S. Ct. 2473, 2495 (2014).

[50] *Id.* at 2489 ("Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person.").

> use of a cell phone is protected from warrantless search by the Fourth Amendment.[51]

Definitive resolution of this question, on which courts around the country have disagreed, is necessary to provide guidance to law enforcement and the public about the extent of Fourth Amendment rights in the digital age.

Ready access to a complete map of a person's movements raises questions that have been long recognized as of particularly significance.[52] As Judge Kozinski has observed,

> [w]hen requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that 'such dragnet-type law enforcement practices' are already in use.[53]

The protection of a warrant is needed to ensure that the Fourth Amendment is not eviscerated as law enforcement accelerates its warrantless access to huge stores of sensitive personal location data.

The use of cell phones is now prevalent, with "more than 90% of American adults . . . own[ing] a cell phone,"[54] more than 335 million wireless subscriber accounts in the United States,[55] and 47 percent of households utilizing *only* cell phones.[56] As Justice Alito recognized in *Jones*, cell phones are "[p]erhaps most significant" of the

---

[51] Davis Petition at *15-* 16

[52] United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing *en banc*) ("The Supreme Court in [*United States v.*] *Knotts [460 U.S. 276, 283–84 (1983)]* expressly left open whether 'twenty-four hour surveillance of any citizen of this country' by means of 'dragnet-type law enforcement practices' violates the Fourth Amendment's guarantee of personal privacy.").

[53] *Id.*

[54] *Id.* at 2490.

[55] *Annual Wireless Industry Survey*, *supra* note 14.

[56] Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, January–June 2014*, CTR. FOR DISEASE CONTROL & PREVENTION (Dec. 2014),

"many new devices that permit the monitoring of a person's movements."[57] Given the near-universal adoption of cellular technology, it is no surprise that law enforcement has a growing appetite for cell phone-related data.

Indeed, the government now requests a staggering quantity of CSLI from service providers. In 2015, for example, AT&T received 76,340 requests for cell phone location data information.[58] Of those, 58,189 were for historical CSLI.[59] Verizon received approximately 20,298 requests for cell phone location data in just the second half of 2015.[60]

In the case under discussion, the government seized Davis's location data covering 67 days and 11,606 location data points.[61] This is in line with the average law enforcement request reported by one major service provider, which "asks for approximately fifty-five days of records."[62] Other recent cases involve even greater quantities of sensitive location information that was obtained without a warrant. For example, in one case, the government was able to obtain 29,659 location points for one defendant from 221 days (over seven months) of cell site location information.[63] In another, the government obtained 12,898 cell site location data points from 127 days of tracking.[64]

---

http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201412.pdf. *See also Annual Wireless Industry Survey*, *supra* note 14.

[57] United States v. Jones, 132 S. Ct. 945, 963 (Alito, J., concurring).

[58] *Transparency Report*, AT&T 4 (2016), http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_Jan%202016.pdf.

[59] *Id.*

[60] *Verizon's Transparency Report for the 2nd Half of 2015*, VERIZON 5 (2016), http://www.verizon.com/about/portal/transparency-report/us-report/ (last visited Mar. 25, 2016).

[61] United States v. Davis, 785 F.3d 498, 533 (11th Cir. 2015) (en banc) (Martin, J., dissenting).

[62] *Transparency Report for 2013 & 2014*, T-MOBILE 5 (2015), http://newsroom.t-mobile.com/content/1020/files/ NewTransparencyReport.pdf.

[63] United States v. Graham, 796 F.3d 332, 350 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

[64] Brief for American Civil Liberties Union, et al. as Amici Curiae in Support of Defendant-Appellant at 9, United States v. Carpenter, 2015 WL 1138148, No. 14-1572 (6th Cir. Mar. 9, 2015).

Despite the breadth of these requests, law enforcement agencies frequently obtain the CSLI data without a probable cause warrant. One survey of public records request responses from roughly 250 local law enforcement agencies showed that "only a tiny minority reported consistently obtaining a warrant and demonstrating probable cause" for CSLI.[65] Given the ubiquity of cell phone usage, and the heavy reliance on CSLI requests, it is important that courts settle the question in a way that appropriately protects Fourth Amendment rights.

Davis and similar cases are not only about the Fourth Amendment status of CSLI, but also address how the protections of the Fourth Amendment apply to other sensitive and private data in the hands of trusted third-parties.

As Justice Sotomayor noted in *Jones*,

> it 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.[66]

Applying the Fourth Amendment's warrant requirement in *Davis* would not have required a wholesale reassessment of the third-party doctrine. But the courts must clarify how analog-age precedents in this area can be applied to digital surveillance techniques.

In the *Davis* panel decision, the court found that the third-party doctrine does not apply to CSLI because the data was not voluntarily conveyed to carriers, and because of the sensitivity of the data.[67] In the *en banc* dissent, Judge Martin agreed, expressing alarm that "the

---

[65] *Cell Phone Location Tracking Public Records Request*, ACLU (Mar. 25, 2013), https://www.aclu.org/cases/cell-phone-location-tracking-public-records-request.

[66] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[67] United States v. Davis, 754 F.3d 1205, 1216 (stating that "there is reasonable privacy interest in being near the home of a lover, or a dispensary of medication, or a place of worship . . . we do not see the factual distinction as taking Davis's location outside his expectation of privacy.").

majority's blunt application of the third-party doctrine threatens to allow the government access to a staggering amount of information that surely must be protected under the Fourth Amendment."[68] Yet the *en banc* majority resolved the case with a straight application of *Smith*, ignoring the significant changes over the intervening 35 years in technology and expectations of privacy.[69] Three concurring judges wrote separately to register their concerns about exempting the CSLI records at issue from Fourth Amendment protections, inviting the Court to clarify the scope of the rule announced in *Miller* and *Smith*.[70] Other courts are similarly divided.[71]

This struggle in applying pre-digital precedents from *United States v. Miller* and *Smith v. Maryland* is seen throughout the lower courts.[72] The principle taken from these cases, known as the "third-party doctrine," provides that certain records or information shared with third parties do not deserve Fourth Amendment protection.[73] *Smith* involved short-term use of a pen register to capture the telephone numbers that a person dials, finding this not to be a Fourth Amendment search.[74] The decision was based in large part on the fact that by dialing a number, the caller "voluntarily convey[s] numerical information to the telephone company."[75] In addition, the *Smith* court evaluated the degree of invasiveness of the surveillance

---

[68] Davis, 785 F.3d at 535 (Martin, J., dissenting).

[69] *Id.* at 508.

[70] *Id.* at 521 (Jordan, J., concurring); *Id.* at 524–25 (Rosenbaum, J., concurring).

[71] *Compare In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 612–13 (5th Cir. 2013) (no expectation of privacy in CSLI under *Smith*) *and* United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc) (same), *with In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (distinguishing *Smith* and holding that cell phone users may retain a reasonable expectation of privacy in CSLI), *and* Graham, 824 F.3d at 444 (Wynn, J., dissenting) ("CSLI is not 'voluntarily conveyed' by a cell phone user, and therefore is not subject to the third-party doctrine.").

[72] *See generally* United States v. Miller, 425 U.S. 435 (1976) and Smith v. Maryland, 442 U.S. 735 (1979).

[73] United States v. Davis, 785 F.3d 498, 512 (noting the application of the third-party doctrine and that "cell phone users voluntarily convey cell tower location information to telephone companies in the course of making and receiving calls on their cell phones.").

[74] *Smith*, 442 U.S. at 742.

[75] *Id.* at 744.

in order to determine whether the user had a reasonable expectation of privacy.[76] For example, the Court noted the "pen register's limited capabilities,"[77] explaining that "'a law enforcement official could not even determine from the use of a pen register whether a communication existed.'"[78] *Miller*, a case involving bank depositor transaction records voluntarily provided to the bank, resolved similarly.[79]

The struggle in defining the scope of the Fourth Amendment's protections for newer forms of sensitive digital data are reflected in widespread scholarly criticism of the expansive application of the third-party doctrine beyond the kinds of records at issue in *Smith* and *Miller*.[80] Scholars and judges have asked the Supreme Court to ensure that Fourth Amendment jurisprudence keeps pace with technology's rapid advance.

The *Davis* case offered the Supreme Court an opportunity to address the application of the Fourth Amendment warrant requirement to sensitive and private records held by a third party. Deprived of this guidance, a cell phone user "cannot know the scope of his constitutional protection, nor can a policeman know the scope of his authority."[81] It is becoming increasingly urgent that the Court provide a clear constitution rule governing location data and other sensitive digital records.

A. *The Federal Courts of Appeals and State High Courts Are Divided.*

The *Davis en banc* opinion further broadens the conflict over whether and when sensitive cell phone location data held by a service provider is protected by a warrant requirement.

---

[76] *Id.* at 741–42.

[77] *Id.* at 742.

[78] *Id.* at 741.

[79] *Miller*, 425 U.S. at 440–42 (finding "no intrusion into any area in which respondent had a protected Fourth Amendment interest").

[80] *See, e.g.*, Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002); Daniel Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1151–52 (2002).

[81] New York v. Belton, 453 U.S. 454, 459–60 (1981).

1. IN FLORIDA, STATE AND FEDERAL COURTS ARE SPLIT OVER THE EXISTENCE OF A REASONABLE EXPECTATION OF PRIVACY IN CSLI.

Florida law enforcement agents are now faced with a difficult decision. They now must choose whether to follow the holding of the state supreme court in *Tracey v. State*, and obtain a warrant before seizing CSLI, or whether to follow the Eleventh Circuit's holding in *Davis* and proceed without a warrant. In *Tracey*, the Supreme Court of Florida held that there is a reasonable expectation of privacy under the Fourth Amendment in real-time cell phone location data, and that accordingly a warrant is required.[82] Historical CSLI records were not at issue in *Tracey*,[83] but the court found that the same principles that courts have held to create a reasonable expectation of privacy in historical CSLI also require protection of real–time CSLI.[84] Indeed, there is little meaningful difference between historical and real-time records. Both offer information about a person's private location, and both permit law enforcement to discover a large quantity of private information about a person's movements. The historical records, if anything, are more intrusive because they provide a window back in time.

Likewise, a number of states require a warrant for historical CSLI by statute or under their state constitution as interpreted by the state's highest court.[85] Additional states require a warrant for real-time cell phone location data.[86] Requiring a warrant for CSLI as a matter of federal constitutional law would harmonize the protections available in state and federal investigations in these states as well.

Even if state and local law enforcement agencies elect to follow *Tracey*, residents of Florida are nonetheless subject to varying

---

[82] Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014).

[83] *Id.* at 516.

[84] *Id.* at 523.

[85] *See* Commonwealth v. Augustine, 4 N.E.3d 846, 866 (Mass. 2014); CAL. PENAL CODE §1546.1(b)(1) (2016); COLO. REV. STAT. § 16-3-303.5(2) (2014); ME. REV. STAT. tit. 16, § 648 (2014); MINN. STAT. §§ 626A.28(3)(d), 626A.42(2) (2014); MONT. CODE § 46-5-110(1)(a) (2015); N.H. REV. STAT. § 644-A:2 (2015); UTAH CODE § 77-23c-102(1)(a) (2015); VT. STAT. ANN. tit. 13, § 8102(b)(1).

[86] *See, e.g.*, State v. Earls, 70 A.3d 630, 644 (N.J. 2013); 725 ILL. COMP. STAT. § 168/10 (2014); IND. CODE § 35-33-5-12 (2014); MD. CODE CRIM. PROC. § 1-203.1(b) (2015); VA. CODE § 19.2-70.3(C) (2015).

Fourth Amendment protections depending on whether they are investigated by state or federal agents. This variation, based on the luck of the draw as to which agency investigates, is unacceptable.

2. THERE IS A CIRCUIT SPLIT REGARDING WHETHER THE THIRD-PARTY DOCTRINE CIRCUMVENTS THE REASONABLE EXPECTATION OF PRIVACY IN A PERSON'S HISTORICAL CSLI.

Like the Fifth Circuit, the Eleventh Circuit now holds that there is no reasonable expectation of privacy in historical cell site location information under the Fourth Amendment, and therefore that no warrant is required.[87] *In re Application of the U.S. for Historical Cell Site Data*, involved a magistrate judge who rejected a government application for an order seeking historical CSLI, pursuant to the Stored Communications Act, 18 U.S.C. § 2703(d).[88] The judge held that the Fourth Amendment requires a warrant.[89] On appeal, the Fifth Circuit rejected the argument that cell users maintain an expectation of privacy in the data because they do not voluntarily convey to the service provider their location information.[90] The Fifth Circuit found that the cell service provider's creation and possession of the records eliminates any expectation of privacy in CSLI.[91] More recently, a divided panel of the Sixth Circuit and a divided en banc Fourth Circuit reached the same conclusion.[92]

---

[87] *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).

[88] *Id.*

[89] *Id.*

[90] *Id.* at 613–14; *see also* United States v. Guerrero, 768 F.3d 351, 358–59 (5th Cir. 2014) (applying *Historical Site* in the context of a suppression motion). The Sixth Circuit has held that the Fourth Amendment does not apply to shorter-term real-time tracking of a cell phone user's location during a single three-day multi-state trip on public highways. United States v. Skinner, 690 F.3d 772, 777–781 (6th Cir. 2012). The court reserved decision about "situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes." *Id.* at 780 (citing United States v. Jones, 132 S. Ct. 945, 957–64 (2012)).

[91] *Id.* at 613.

[92] United States v. Carpenter, 819 F. 3d 880 (6th Cir. 2016); United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc).

Other courts disagree. The Third Circuit has held that magistrate judges have discretion to require a warrant for historical CSLI, in those circumstances in which the location information implicates an individual's Fourth Amendment privacy rights by, for example, revealing when a person is inside a constitutionally protected space.[93] The Third Circuit rejected the argument that a cell phone user's expectation of privacy is eviscerated by the carrier's ability to access that information:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. [. . .] [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."[94]

For this reason, the court found that the third-party doctrine does not apply to historical CSLI records.[95] A divided panel of the Fourth Circuit agreed with this view, "declin[ing] to apply the third-party doctrine in the present case because a cell phone user does not 'convey' CSLI to her service provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement."[96] *En banc* reconsideration of the panel opinion is pending.

---

[93] *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3rd Cir. 2010).

[94] *Id.* at 317–18.

[95] *Id.*

3. THERE IS A CIRCUIT SPLIT REGARDING WHETHER THERE IS A REASONABLE EXPECTATION OF PRIVACY IN LONGER-TERM LOCATION INFORMATION COLLECTED ELECTRONICALLY.

Circuits also are split over the question of expectation of privacy in longer-term electronic data. The D.C. Circuit held in *United States v. Maynard* that surreptitiously tracking a car over 28 days using a GPS device violates reasonable expectations of privacy and therefore constitutes a Fourth Amendment search.[97] The court explained that

> "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation."[98]

The court recognized that people have a reasonable expectation of privacy in the private information revealed by "prolonged GPS monitoring."[99]

This holding remains controlling law in the D.C. Circuit (though the Supreme Court affirmed on other grounds, relying on a trespass-based rationale.).[100] The holding is not dependent on the particular type of tracking technology at issue, as extended electronic surveillance of the location of a person's cell phone is at least as invasive as prolonged electronic surveillance of the location of a person's vehicle.[101]

---

[97] United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010), *aff'd on other grounds sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[98] *Id.* at 562.

[99] *Id.* at 563.

[100] *See* Will Baude, *Further Thoughts on the Precedential Status of Decisions Affirmed on Alternate Grounds*, THE VOLOKH CONSPIRACY (Dec. 3, 2013, 7:27 PM), http://volokh.com/2013/12/03/thoughts-precedential-status-decisions-affirmed-alternate-grounds/.

[101] *See* United States v. Jones, 132 S. Ct. 945, 963 (Alito, J., concurring) (explaining that law enforcement access to cell phone location information is "[p]erhaps most significant" of the "many new devices that permit the monitoring of a person's movements.").

In *Davis*, the Eleventh Circuit went a different way, rejecting this reasoning and opining that "reasonable expectations of privacy under the Fourth Amendment do not turn on the quantity of non-content information MetroPCS collected in its historical cell tower location records."[102] The decision widened the circuit split over whether people have a reasonable expectation of privacy in their longer-term location information[103]

4. THERE IS A CIRCUIT SPLIT REGARDING WHETHER THE WARRANT REQUIREMENT APPLIES WHEN THERE IS A REASONABLE EXPECTATION OF PRIVACY IN CSLI OR OTHER ELECTRONICALLY COLLECTED LOCATION INFORMATION.

A circuit split also exists over whether a warrant is required when there is, in fact, a reasonable expectation of privacy in CSLI data. The *en banc* majority in *Davis* held that the government's warrantless seizure and search of the records was reasonable, *even if* Davis had a reasonable expectation of privacy in his CSLI.[104] This alternative holding cannot be squared with the Supreme Court's longstanding proscription that warrantless searches are "'*per se* unreasonable.'"[105]

---

[102] United States v. Davis, 785 F.3d 498, 515 (11th Cir. 2015).

[103] *Compare* United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) (prolonged electronic location tracking is a search under the Fourth Amendment), *with* United States v. Pineda-Moreno, 591 F.3d 1212, 1216–17 (D.C. Cir. 2010) (holding that the "police did not conduct an impermissible search of Pineda-Moreno's car by monitoring its location with mobile tracking devices"), United States v. Garcia, 474 F.3d 994, 996–99 (7th Cir. 2007) (prolonged electronic location tracking is not a search under the Fourth Amendment), *and* United States v. Marquez, 605 F.3d 604, 609 (8th Cir. 2010) ("A person traveling via automobile on public streets has no reasonable expectation of privacy in his movements from one locale to another.").

[104] *Davis*, 785 F.3d at 515.

[105] City of Los Angeles v. Patel, 135 S. Ct. 2443 (2015) (quoting Arizona v. Gant, 556 U.S. 332, 338 (2009)). *See* Orin Kerr, *Eleventh Circuit Rules for the Feds on Cell-Site Records – But Then Overreaches*, WASH. POST (May 5, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/05/eleventh-circuit-rules-for-the-feds-on-cell-site-records-but-then-overreaches/ ("[T]he en banc court's alternative holding . . . [is] a novel development of the law that cuts against a lot of practice and precedent.").

Certain searches conducted outside the scope of traditional law enforcement, or aimed at categories of people in specific circumstances where the expectation of privacy is reduced, may not require probable cause warrants.[106] In the CSLI cases, neither of these exceptions apply; no "special need" beyond regular normal law enforcement operation is served by the data requests. Indeed, even the *en banc* Eleventh Circuit recognized that the government's search of Davis's CSLI was in furtherance of "[t]he societal interest in promptly apprehending criminals and preventing them from committing future offenses."[107] Neither Davis nor any other similarly situated criminal suspect have a reduced expectation of privacy justifying rejection of the warrant requirement.[108]

The Eleventh Circuit's alternate holding not only conflicts with prior decisions of the Supreme Court, but also creates a split with the courts that have required a warrant for law enforcement access to CSLI and that have found there is a reasonable expectation of privacy in CSLI or other electronically collected location information.[109]

B. *The En Banc Eleventh Circuit Erred In Holding That Accessing Historical Cell Site Location Records From A Service Prodicer Was Not A Search*

The Eleventh Circuit majority found Davis' position to be unsustainable merely because the government obtained the CSLI records from Davis's cell carrier rather than directly from Davis, in light of *United States v. Miller* and *Smith v. Maryland*.[110] This is a

---

106 *See* City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000).

107 *Davis*, 785 F.3d at 518.

108 *Cf.* Samson v. California, 547 U.S. 843, 850 (2006) (parolees); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664 (1995) (student athletes).

109 *See* Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (probable cause warrant required for tracking CSLI); Commonwealth v. Augustine, 4 N.E.3d 846, 866 (Mass. 2014) (same, under state constitution); State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (same); *see also* United States v. Maynard, 615 F.3d 544, 566–67 (D.C. Cir. 2010) (holding that warrant is required for prolonged GPS tracking of a car and rejecting application of the automobile exception to the warrant requirement); People v. Weaver, 909 N.E.2d 1195, 1203 (N.Y. 2009) (warrant required for GPS tracking under state constitution).

110 United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015).

misreading of applicable law. The Supreme Court should clarify that a user's reasonable expectation of privacy in his location data is not eliminated, in and of itself, by a service provider's access to that data. While a third-party's access to records may be a factor relevant to the *Katz* reasonable-expectation-of-privacy analysis, the third-party doctrine set forth in *Miller* and *Smith* does not make the fact of such access the sine qua non of Fourth Amendment protection. As the Court has repeatedly explained, limited third-party access to information or locations does not destroy otherwise-reasonable expectations of privacy.[111]

Instead, the reasonable-expectation-of-privacy test relies on a totality-of-the-circumstances analysis. The mechanical application of holdings from the analog age is improper in this new era involving highly sensitive and voluminous digitized records.[112] "[I]t is virtually impossible to participate fully in modern life without leaving a trail of digital breadcrumbs that create a pervasive record of the most sensitive aspects of our lives. Ensuring that technological advances

---

[111] *See* Florida v. Jardines, 133 S. Ct. 1409, 1418–19 (2013) (Kagan, J., concurring) (expectation of privacy in odors detectable by a police dog that emanate from a home); United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) (information about location and movement in public, even though exposed to public view); Kyllo v. United States, 533 U.S. 27, 29 (2001) (thermal signatures emanating from a home); Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) ("The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."); Bond v. United States, 529 U.S. 334, 336 (2000) (bag exposed to the public on luggage rack of bus); Minnesota v. Olson, 495 U.S. 91, 98–99 (1990) ("an overnight guest has a legitimate expectation of privacy in his host's home" even though his possessions may be disturbed by "his host and those his host allows inside"); United States v. Jacobsen, 466 U.S. 109, 114–15 (1984) (reasonable expectation of privacy in letters and sealed packages entrusted to private freight carrier); Katz v. United States, 389 U.S. 347, 358–59 (1967) (reasonable expectation of privacy in contents of phone call even though call is conducted over private companies' networks); Stoner v. California, 376 U.S. 483, 487–90 (1964) (implicit consent to janitorial personnel to enter motel room does not amount to consent for police to search room); Chapman v. United States, 365 U.S. 610, 616–17 (1961) (search of a house invaded tenant's Fourth Amendment rights even though landlord had authority to enter house for some purposes).

[112] *See* Riley v. California, 134 S. Ct. 2473, 2489 (2014).

do not erode the privacy guaranteed by the Fourth Amendment,[113] requires nuanced applications of analog-age precedents."[114]

The conclusion that Davis retained a reasonable expectation of privacy in his CSLI does not require rejection of *Smith* and *Miller*, but rather can be squared with those cases' plain terms. The Supreme Court has looked to factors such as whether the records were "voluntarily conveyed,"[115] and what privacy interest a person has in the information,[116] when evaluating an individual's expectation of privacy in records held by a third party. As opposed to the dialed phone numbers and limited bank records at issue in *Smith* and *Miller*, "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[117] The location information that is tracked is not voluntarily entered by the user into the phone, nor otherwise in any way affirmatively transmitted to the carrier. This is even more the case when a person receives a call, thereby taking *no* action that would knowingly or voluntarily reveal location.

In addition the location records contained in CSLI are exceedingly sensitive and private. First, because people carry their phones virtually everywhere they go, including inside their homes and other constitutionally protected spaces, cell phone location records can reveal information about presence, location, and activity in those spaces.

> In *United States v. Karo*, the [Supreme Court] held that location tracking implicates Fourth Amendment privacy interests when it may reveal information about individuals in areas where they have reasonable expectations of privacy.[118] The Court explained that using an electronic device—there, a beeper—to

---

[113] *Kyllo*, 533 U.S. at 34.

[114] Davis Petition at *30-*31 (internal quotation omitted).

[115] United States v. Miller, 425 U.S. 435, 442 (1976); Smith v. Maryland, 442 U.S. 735, 744 (1979).

[116] *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 741–42.

[117] *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3rd Cir. 2010).

[118] United States v. Karo, 468 U.S. 705, 714–15 (1984).

> infer facts about 'location[s] not open to visual surveillance,' like whether 'a particular article is actually located at a particular time in the private residence,' or to later confirm that the article remains on the premises, was just as unreasonable as physically searching the location without a warrant.[119] Such location tracking 'falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance' from a public place,[120] regardless of whether it reveals that information directly or through inference.[121]

Second, CSLI data reveals a large amount of sensitive and private information about a person's movements and activities in public and private spaces that, at least long-term, violates reasonable expectations of privacy. The majority opinion in *Jones* relied on a trespass-based rationale to find a search,[122] making clear that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* [reasonable expectation of privacy] analysis."[123] Five Justices conducted a *Katz* analysis, finding that (at least) longer-term location tracking violates reasonable expectations of privacy.[124]

This conclusion is not particularized to the type of tracking technology at issue in *Jones*. As Justice Alito identified, mobile devices are "[p]erhaps most significant" of the emerging technologies capable of location tracking.[125] The Supreme Court recently emphasized this point, explaining that cell phone location data is particularly sensitive because it "can reconstruct someone's specific movements

---

119 *Id.*

120 *Id.* at 707

121 *See* Kyllo v. United States , 533 U.S. 27, 36 (2001) (use of thermal imaging device to learn information about interior of home constitutes a search). Davis Petition at *32.

122 United States v. Jones, 132 S. Ct. 945, 949 (2012).

123 *Id.* at 953.

124 *Id.* at 964 (Alito, J., concurring); *Id.* at 955 (Sotomayor, J., concurring).

125 *Id.* at 963.

down to the minute, not only around town but also within a particular building."[126]

In *Davis*, the records obtained by the government implicated both the expectation of privacy in longer-term location information and in private spaces.[127] These records told the government when Davis slept at home and when he slept elsewhere.[128] They showed, nearly to the minute, his movements around his community.[129] They even allowed the government to learn with whom he associated and when he did so.[130]

Recent data shows that more than 80 percent of people consider "[d]etails of [their] physical location over time" to be "sensitive"—evincing greater concern for this data than for the contents of their text messages, a list of numbers they have called or websites they have visited, or their relationship history.[131] Historical CSLI enables the government to "monitor and track our cell phones, and thus ourselves, with minimal expenditure of funds and manpower, [which] is just the type of gradual and silent encroachment into the very details of our lives that we as a society must be vigilant to prevent."[132]

III. WHERE *DAVIS* LEADS

Davis and other cases concerning the Fourth Amendment's application to historical CSLI raise fundamental questions about how to apply the protections of the Bill of Rights, now more than 220 years old, to the digital age. As law enforcement agencies increasingly rely on access to sensitive troves of digital data held by third-party companies and deploy ever-more-sophisticated surveillance

---

[126] Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing *Jones,* 132 S. Ct. at 955 (Sotomayer, J., concurring)).

[127] United States v. Davis, 785 F.3d 498, 539–41 (11th Cir. 2015) (en banc) (Martin, J., Dissenting).

[128] *Davis*, 785 F.3d at 540 (Martin, J., Dissenting).

[129] *Id.*

[130] *See* Trial Transcript at 12–14, United States v. Davis, No. 10-20896-CR-GOLD (Feb. 6, 2012), ECF No. 283.

[131] *Public Perceptions of Privacy and Secuirty in the Post-Snowden Era*, PEW RESEARCH CENTER 34 (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-prviacy-perceptions/.

[132] Tracey v. State, 152 So. 3d 504, 522 (Fla. 2014).

technologies, courts are struggling to keep up. The historical CSLI cases preview a broader, percolating debate over how to apply the third-party doctrine in the digital age and how to appropriately constrain the pervasive collection of location information using surreptitious surveillance devices.[133]

Cell site location information is far from the only sensitive information held in digital storage by third parties for which Fourth Amendment protections are needed.[134] Indeed, as the dissenting judges in *Davis* wrote,

> the majority's blunt application of the third-party doctrine threatens to allow the government access to a staggering amount of information that surely must be protected under the Fourth Amendment. Consider the information that Google gets from users of its e-mail and online search functions. According to its website, Google collects information about you (name, e-mail address, telephone number, and credit card data); the things you do online (what videos you watch, what websites you access, and how you view and interact with advertisements); the devices you use (which particular phone or computer you are searching on); and your actual location . . . .Under a plain reading of the majority's rule, by allowing a third-party company access to our e-mail accounts, the websites we visit, and our search-engine history—all for legitimate business purposes—we give up any privacy interest in that information.[135]

Although, ultimately, it may fall to the Supreme Court to explain how to reconcile the analog-age third-party doctrine to digital-age realities, state and federal courts cannot escape grappling with Fourth Amendment protection for sensitive information held by a third party.[136]

---

[133] *See generally* Riley v. California, 134, S. Ct. 2473 (2014); United States v. Jones, 1132 S. Ct. 945 (2012); United States v. Davis, 785 F. 3d 498 (11th Cir. 2015).

[134] *Davis*, 785 F.3d at 535–36 (Martin, J., dissenting).

[135] *Id.*

[136] *See* Orin Kerr, *supra* note 103.

In some areas, federal and state courts have extended the warrant requirement to digital data held by a third party.[137] Courts have held, for example, that people have a reasonable expectation of privacy in the contents of email stored on service providers' servers, analogizing those records to the contents of letters entrusted to the postal service.[138] Recognizing that warrantless access to a phone company's records of the phone numbers a person dials is permitted by *Smith v. Maryland*, courts have distinguished so-called "post-cut-through dialed digits," which are "any numbers dialed from a telephone after the call is initially setup or 'cut-through,'"[139] on the basis that they may contain sensitive information tantamount to the contents of a communication.[140] A federal judge in Oregon rejected the Drug Enforcement Administration's practice of requesting prescription records held in a secure state prescription drug monitoring database with an administrative subpoena instead of a warrant. The court held that the third-party doctrine does not apply because of the sensitivity of the records and the lack of voluntary conveyance of records incident to necessary medical care.[141] State supreme courts across the country have rejected application of the third-party doc-

---

[137] *Id.*

[138] United States v. Warshak, 631 F.3d 266, 286–88 (6th Cir. 2010); *see also* Orin Kerr, *supra* note 103.

[142] *In re* Application of the United States for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 818 (S.D. Tex. 2006) (stating "[s]ometimes these digits are other telephone numbers, as when a party places a credit card call by first dialing the long distance carrier access number and then the phone number of the intended party. Sometimes these digits transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like").

[140] *Id.*; *accord In re* Application of the United States for an Order (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information, 515 F. Supp. 2d. 325, 337–39 (E.D.N.Y. 2007).

[141] Oregon Prescription Drug Monitoring Program v. U.S. Drug Enf't Admin., 998 F. Supp. 2d 957, 967 (D. Or. 2014).

trine under their states' constitutions as applied to sensitive information such as dialed telephone numbers, bank records, medical records, employment records, and other data.[142]

Yet, vast quantities of sensitive digital records are as-yet unprotected by judicial precedent. Private companies now hold copies of individuals' genetic profiles, potentially shedding light on familial relationships and genetic diseases.[143] Electricity providers retain increasingly granular power consumption data generated by "smart meters," which can show not only when a person is home, but even which appliances she is using.[144] Untold millions of family photos, sensitive documents, and private communications are stored in the cloud, on servers of companies offering the service for free or low cost.[145] AT&T retains records of every phone call to transit its network dating "as far back as 1987," laying bare a generation's worth of contacts and associations of a vast number of Americans.[146] Requests for third-party data can "allow[] the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we 'friend,' or Amazon.com what we buy, or Wikipedia.com what we research, or Match.com whom we date."[147] These records, of course, may be of acute interest to law enforcement in criminal investigations,[148] making the need for protective Fourth Amendment rules paramount.

---

[142] Stephen E. Henderson*, Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 396–99 n. 118–28 (2006).

[143] 23ANDME, https://www.23andme.com (last visited Mar. 22, 2016, 7:09 PM); ANCESTRY, http://www.ancestry.com (last visited Mar. 22, 2016; 7:17 PM).

[144] Natasha Duarte, *The Home Out of Context: The Post-Riley Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1154–55 (2015).

[145] DROPBOX, https://www.dropbox.com (last visited Mar. 22, 2016); FLICKR, https://www.flickr.com (last visited Mar. 22, 2016); GOOGLE DRIVE, https://www.google.com/drive (last visited Mar. 22, 2016).

[146] Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES (Sept. 1, 2013), http://www.nytimes.com/2013/09/02/us/drug-agents-use-vast-phone-trove-eclipsing-nsas.html.

[147] United States v. Davis, 785 F.3d 498, 536 (11th Cir. 2015) (en banc) (Martin, J., dissenting).

[148] *See*, e.g.*, Transparency Report*, 23ANDME, https://www.23andme.com/transparency-report/ (last visited Mar. 25, 2016); *An-*

Davis and similar cases also open the door to discussion of legal limits on other location tracking technologies used by law enforcement agencies directly, without the assistance of a third-party company. Law enforcement agencies across the country are increasingly bypassing cellular service providers by surreptitiously deploying "cell site simulators," also known as Stingrays, to track and precisely locate cell phones.[149] These devices mimic legitimate cell phone towers, forcing all phones within range that use the impersonated cellular network to broadcast their unique electronic serial numbers.[150] By virtue of those transmissions the devices can precisely identify phones' locations.[151] Cell site simulators raise constitutional concerns because they can learn information about location and activities within homes and other constitutionally protected spaces, and can sweep in information about large numbers of bystanders' phones in the process of searching for a particular suspect.[152] Despite the widespread use of the technology,[153] judicial consideration of the Fourth Amendment issues has been slow to materialize, largely because police have wrapped their use of cell site simulators in an incredible cloak of secrecy.[154] Courts are beginning

---

cestry 2015 Transparency Report, ANCESTRY, http://www.ancestry.com/cs/transparency/ (last visited Mar. 25, 2016); United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1117 (9th Cir. 2012) (holding that the DEA's subpoena for power consumption records sought by the DEA was "relevant to a drug investigation, was procedurally proper . . . was not overly broad, [and] complied with the Fourth Amendment."); SAN DIEGO GAS & ELEC. CO. 2014 ANNUAL PRIVACY REPORT (2015), http://www.cpuc.ca.gov/WorkArea/DownloadAsset.aspx?id=3287; *Google Transparency Report*, GOOGLE, https://www.google.com/transparencyreport/ (last visited Mar. 25, 2016).

[149] *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore:*
The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National
Security and Consumer Privacy, 28 HARV. J.L. & TECH. 1, 14, 34–35 (2014).

[150] *See id.* at 12.

[151] *See id.*

[152] *See id.*

[153] *See Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Mar. 25, 2016).

[154] *See In re* Application of the United States for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 WL 6871289, at *1 (N.D. Ill.

to address the issue, which presents the issue of the Fourth Amendment's protections for location information without the complication of the third-party doctrine.[155]

Use of automated license plate readers (ALPRs) also threatens to give law enforcement access to large volumes of information about people's locations and movements. ALPRs, which are operated both by law enforcement and private companies, can log the locations of many thousands of cars as they drive the streets, feeding those records into massive databases that can trace a whole population's movements and activities over space and time.[156] Inconspicuous pole cameras, which can be trained on private residences and record weeks or months of peoples' comings and goings raise similar concerns.[157] The rapidly expanding market for drone technology raises the specter of police departments deploying fleets of small flying surveillance platforms, containing cameras, microphones, and even cell site simulators and other electronic surveillance gear. These technologies erase the practical protections against pervasive government monitoring that we, as a society, have long relied on. As Justice Alito discussed in *United States v. Jones*,

---

Nov. 9, 2015); Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 24, 2015), http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/; Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. TIMES (Mar. 15, 2015), http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html?_r=0; Jack Gillum & Eileen Sullivan, *US Pushing Local Cops to Stay Mum on Surveillance*, ASSOCIATED PRESS (June 12, 2014), https://finance.yahoo.com/news/us-pushing-local-cops-stay-174613067.html.

[155] *See* State v. Andrews, 227 Md. App. 350 (Md. Ct. Spec. App. 2016).

[156] *You Are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements*, ACLU (July 2013), https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf; Conor Friedersdorf, *An Unprecedented Threat to Privacy*, THE ATLANTIC (Jan. 27, 2016), http://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/ ("[Vigilant Solutions] has taken roughly 2.2 billion license-plate photos to date. Each month, it captures and permanently stores about 80 million additional geotagged images.").

[157] *See* United States v. Houston, 813 F.3d 282, 285 (6th Cir. 2016); United States v. Vargas, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672, at *1 (E.D. Wash. Dec. 15, 2014), *denying reconsideration and motion to dismiss*, United States v. Vargas, 2015 U.S. Dist. LEXIS 451 (E.D. Wash., Jan. 5, 2015).

> [i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.[158]

However, with cell site simulators, networked ALPRs, pole cameras, and any number of other surveillance technologies, the power of police to amass detailed information about the movements and activities of both suspects and large numbers of Americans going about their daily lives is growing. The need for courts and legislatures to provide strong protections for location information is growing ever more pressing.

CONCLUSION

The legal system has always been playing catch up with technology. It is up to the judiciary to check the executive branch in its continuing efforts to use technology in creative and aggressive ways. Although the Supreme Court has embraced this role in recent cases involving cell phones, courts of appeals must fill the gaps around cell site location information, other forms of sensitive digital data and invasive surveillance techniques. The circuit courts should not follow the Eleventh Circuit in rotely invoking 1970s cases in ways that make no sense when applied to today's technology.

---

[158] United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in the judgment); *accord id.* at 956 (Sotomayor, J., concurring) ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'").