No. 12-12928

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff/appellee,

v.

QUARTAVIOUS DAVIS,
Defendant/appellant.

On Appeal from the United States District Court
for the Southern District of Florida

EN BANC BRIEF OF THE APPELLANT QUARTAVIOUS DAVIS

JACQUELINE E. SHAPIRO, ESQ.
Counsel for Appellant
40 N.W. 3rd Street, PH 1
Miami, Florida 33128
Tel. (305) 403-8207
Fax: (305) 403-8209

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

United States v. Quartavious Davis
Case No. 12-12928

Appellant files this Certificate of Interested Persons and Corporate Disclosure Statement, as required by 11th Cir. R. 26.1.

ACLU Foundation

ACLU Foundation of Florida

Altman, Roy

Bascuas, Ricardo

Brown, Hon. Stephen T.

Caruso, Michael

Center for Democracy and Technology

Colan, Jonathan

Davis, Quartavious

Dube, Hon. Robert L.

Electronic Frontier Foundation

Ferrer, Wifredo A.

Fisher, Sylvester

Garber, Hon. Barry L.

Gold, Hon. Alan S.

Golembe, Stephen J.

Hayes, Anne M.

Kayanan, Maria

Korchin, Paul M.

Lenard, Hon. Joan A.

Malone, Omar

Markus, David Oscar

Martin, Michael

Martin, Jahmal A.

McAliley, Hon. Chris M.

Michaels, Alexander J.

Moss, Jr., Reginald A.

National Association of Criminal Defense Lawyers

O'Sullivan, Hon. John J.

Palermo, Hon. Peter R.

Perwin, Amanda

Quencer, Kevin

Reid, Jamarquis T.

Salyer, Kathleen M.

Schultz, Anne R.

Shapiro, Jacqueline E.

Sibila, Jorge A.

Smith, Willie

Stevenson, Benjamin

Torres, Hon. Edwin G.

Turnoff, Hon. William C.

Ungaro, Hon. Ursula

Wessler, Nathan Freed

White, Hon. Patrick A.

Williams, Hon. Kathleen M.

Zelman, Michael

TABLE OF CONTENTS

TABLE OF CITATIONS

CASES:

STATUTORY AND OTHER AUTHORITY:

STATEMENT OF JURISDICTION

The district court had jurisdiction of this case pursuant to 18 U.S.C. § 3231 because the defendant was charged with offenses against the laws of the United States. The court of appeals has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291, which gives the courts of appeals jurisdiction over all final decisions of the district courts of the United States, and 18 U.S.C. § 3742(a), which authorizes defendants to appeal their sentences. The notice of appeal was timely filed on May 29, 2012, from the final judgment and commitment order entered on May 17, 2012, that disposes of all claims between the parties.

STATEMENT OF THE *EN BANC* ISSUES

1. Whether the warrantless seizure or compelled disclosure of cell tower site data identifying the prior movements and whereabouts of a cell phone user violates the Fourth Amendment in the absence of any other exception to the warrant requirement.

2. Whether, even if the warrantless seizure of cell tower site data were not barred in all circumstances, the seizure in the present case, involving 67 consecutive days of cell tower site data, where the government, in seeking an order to compel disclosure, asserted that only seven days of cell site data met the relevance and materiality test, was unreasonable and violated the Fourth Amendment.

STATEMENT OF THE CASE

Course of Proceedings and Disposition in the District Court

Defendant–Appellant Quartavious Davis was convicted at trial of Hobbs Act robbery and conspiracy offenses. In a federal indictment returned in Miami on February 22, 2011, Davis was charged with two Hobbs Act conspiracies (Counts 1, 15) and seven Hobbs Act robbery offenses occurring on seven discrete dates in 2010—August 7 (Count 2), August 31 (Count 4), September 7 (Count 6), September 15 (Count 8), September 25 (Count 10), September 26 (Count 13), and October 1 (Count 16)—all in violation of 18 U.S.C. § 1951(a), as well as using, carrying, or

possessing a firearm in each robbery (Counts 3, 5, 7, 9, 11, 14, 17) on the same seven dates, in violation of 18 U.S.C. § 924(c). D.E. 39.

On February 2, 2011, an Assistant United States Attorney had submitted to a magistrate judge an unsworn "Application for Stored Cell Site Information." D.E. 268-1. The application did not request issuance of a warrant; instead, it requested an "order" directing a cell phone provider to disclose "stored telephone subscriber records … and corresponding geographic location data (cell site)" for Davis's telephone number (and for the telephone numbers of three other people) for the period from August 1, 2010, through October 6, 2010. D.E. 268-1:1. The government recited in the application information regarding a series of robberies and stated, erroneously, that the location data for the dates of occurrence of the robberies was relevant and material to the government's investigation of a violation of 18 U.S.C. § 2113 (bank robbery). D.E. 268-1:6. Notably, the government did not expressly state that the entire period of 67 days of cell tower site data was relevant or material to the investigation. *See* D.E. 268-1:5–6 ("The telephone records requested will assist law enforcement in determining the locations of each of the named subjects *on days when robberies in which they are suspected to have participated occurred*. The requested subscriber information and toll records will further allow law enforcement to determine whether the named subjects communicated with each other *on the days of*

the robberies and, if so, how many times. This information is relevant to the ongoing criminal investigation.") (emphasis added). The application stated it was made pursuant to 18 U.S.C. § 2703(c) and (d), although the statute does not expressly refer to disclosure of cell site data. The application made no reference to the Hobbs Act.

On February 2, 2011, the magistrate judge entered an order directing the production of more than two months of "geographic location data (cell site)" that the prosecutor had requested, finding that the government had offered "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 of a violation of Title 18, United States Code, Section 2113 [sic]." D.E. 266–1. Davis's wireless service provider complied with the order. The cell phone information was obtained exclusively on the basis of the order granting the prosecutor's *ex parte* application pursuant to the Stored Communications Act, 18 U.S.C. § 2703(c), (d) ("SCA"), and spanned the period from August 1 through October 6, 2010, D.E. 266, 268. The government used the records and information at trial to show the location of Davis's cell phone at or near the times of six of the seven alleged robberies. D.E. 285:27–38.

Prior to his trial, Davis filed a motion to suppress the warrantless seizure of the 67 days of cell phone location information. Following a hearing, the district court conditionally denied the motion, without stating a basis for the ruling. D.E. 277:45.

During trial, over Davis's repeated objections, the district court permitted the government to introduce cell site records covering the dates and times surrounding the charged robberies through the testimony of a witness with a background in police investigations. D.E. 283:214, 218, 226–27, 231; D.E. 285:26–38. The defendant renewed his motion to suppress, which was denied, again with no reason provided by the district court. D.E. 364:192 (district court indicating it would provide its reasons in a written order, but none was ever issued).

In its closing argument, the government stressed the significance of this cell phone location data in pinpointing the defendant's presence during the alleged robberies and emphasized that Davis (a teenager at the time of the relevant events) "could not have known" that his cell phone conveyed this type of location information. D.E. 287:4-5 ("But what this defendant *could not have known* was that when he was terrorizing South Florida with a pistol in his hand and a t-shirt over his face, his cell phone was *tracking his every moment*.")(emphasis added); *see also* D.E. 287:14 ("*But what's really significant about this cell site evidence*, what is almost remarkable about the cell site evidence, is that obviously [codefendant] Willie Smith, like the defendant probably, *had no idea that* by bringing their cell phones with them to these robberies they were allowing MetroPCS and *now all of you to follow their movements* on the days and at the times of the robberies, which means that in order for [defense

counsel's] story to be correct, in order for Willie Smith to have been lying about the defendant's involvement in these robberies, you would have to believe that Willie Smith blamed the robberies on a man whose cell phone it would later turn out, unbeknownst to Mr. Smith, just happened to be by some unbelievable stroke of good luck at each of those six robbery locations at the time that the robberies occurred.")(emphasis added).

Following a sentencing hearing, the district court imposed a 1,941-month (162 years) term of incarceration. D.E. 342; D.E. 366:32-33, 38. Davis appealed his convictions and 162-year sentence to this Court challenging, *inter alia*, the seizure of his cell phone location information and its admission at trial as violative of the Fourth Amendment. A panel of this Court ruled that the government violated Davis's Fourth Amendment rights when it obtained cell site location information (CSLI) without a warrant and used that information to link Davis to six of the seven alleged robberies. *United States v. Davis*, 754 F.3d 1204, 1217 (11th Cir. 2014). The panel concluded, however, that the good faith exception to the Fourth Amendment warrant requirement applied, precluding relief for the constitutional violation. *Id.* at 1217-18.

In a petition for rehearing, Davis challenged the panel's ruling, *inter alia*, with respect to the applicability of the good faith exception to the Fourth Amendment warrant requirement. The government sought rehearing *en banc* challenging the

panel's ruling that the government's warrantless acquisition of Mr. Davis's cell site location information violated the Fourth Amendment.

On September 4, 2014, this Court granted rehearing *en banc* and vacated the panel decision. *United States v. Davis*, 573 Fed.Appx. 925 (11th Cir. Sept. 4, 2014) (*en banc*). Thereafter, the Court set a briefing and oral argument schedule, directing the parties to focus in their *en banc* briefs on whether the Stored Communications Act (SCA), 18 U.S.C. § 2703(c)(1)(B), (d), is unconstitutional under the Fourth Amendment in authorizing government acquisition of historical cell site location information from a telephone service provider; and whether, on the facts of this case, the government's acquisition of this information violated Davis's Fourth Amendment rights against unreasonable search and seizure.

Statement of Facts

Quartavious Davis was charged with two separate conspiracies to commit robberies of businesses. D.E. 39:1–2, 9–10. The first conspiracy encompassed the first six charged robberies. *See* D.E. 39:2–8. And the second conspiracy, with different alleged participants, concerned solely the seventh charged robbery, involving a Mayor's jewelry store. The defendant's conviction of each individual robbery was particularly significant, because with each additional (second or subsequent)

conviction under § 924(c), a mandatory consecutive sentence of 25 years imprisonment was imposed.

At trial, the government presented the testimony of two codefendants, Willie Smith and Michael Martin. Smith testified as to the first alleged conspiracy involving six robberies (at a Little Caesar's restaurant, an Amerika gas station, a Walgreen's drug store, an Advance Auto Parts store, a Universal Beauty Salon, and a Wendy's restaurant); and Martin testified as to the second charged conspiracy comprising the Mayor's Jewelry store robbery. The government also presented testimony of Edwin Negron, an eyewitness to the Universal Beauty Salon robbery and an adjoining Tae Kwon Do studio, and of Antonio Brooks, an eyewitness outside the Wendy's restaurant following the robbery there. *Neither Negron nor Brooks identified Davis*. The prosecution also introduced surveillance videos from four of the robbery scenes that were indistinct, but which the government argued included an individual matching Davis's description. In addition, the government submitted records obtained from cell phone service providers indicating that Davis and his codefendants had placed and received cell phone calls at locations close to the initial six of the alleged robberies around the times those robberies occurred. *Davis*, 754 F.3d at 1209–10; *see also* DE:281:173–77; DE:283:82–84.

In closing argument, the government stressed the importance of the evidence linking Davis's cell phone, and hence Davis's location, to specific cell towers. D.E. 287:4–5, 12–15, 20. References to this evidence continued throughout the government's closing argument. D.E. 287:4–5, 12–15, 20, 27, 62–64, 73, 75.

Reflecting the significant credibility issues inherent in presenting the testimony of Willie Smith and Michael Martin, the two government witnesses who admitted participating in the charged robberies, as well as the ambiguous impact of evidence that Davis's DNA was found in the vehicles used by the conspirators, the government devoted much of the rest of its initial closing argument to shoring up the credibility of Martin and Smith, asserting that "Mr. Smith and Mr. Martin told the truth" about their own involvement and the involvement of Jamahl Martin, Jamarquis Reid, and Sylvester Fisher, and that their testimony about these men "was all true." D.E. 287:23. The government further asserted that defense counsel wanted the jury to believe that Smith and Martin testified truthfully "99.9 percent of the way," but lied only in their testimony about Davis. D.E. 287:23–24. Regarding Martin, the government stated, "[H]e came clean and confessed 100 percent and told the police precisely the same story that he told all of you, the same story he has told me 100 times since." D.E. 287:26.

In rebuttal closing argument, the government argued that cell tower site evidence did not place Davis at the site of the Mayor's robbery because, prior to that time, he gave his cell phone to someone else. D.E. 287:65–66. Defense counsel objected that there was no evidence that Davis had given away his phone, but the district court overruled the objection. D.E. 287:65. And the government reiterated the importance of the cell phone tower data: "In the end, all Willie Smith and Michael Martin do is say things that are already corroborated in the evidence." D.E. 287:66. Finally, the government referred to Davis's defense as "this story that [defense counsel] has come up with." D.E. 287:71.

Standard of Review

This Court reviews a district court's legal conclusions on Fourth Amendment claims *de novo*, and it reviews factual findings for clear error. *United States v. Davis*, 313 F.3d 1300, 1302 (11th Cir. 2002).

SUMMARY OF THE *EN BANC* ARGUMENT

The government violated Davis's Fourth Amendment rights by obtaining cell tower site data without a warrant. This data, reflecting Davis's whereabouts and movements over the course of more than two months, enabled the government to place Davis at the locations of the robbery offenses and carried great weight at trial, both independently and in bolstering the testimony of criminal-participant witnesses, as seen in the government's reliance on the cell tower location evidence in closing argument.

Davis had a reasonable expectation of privacy as to the electronic tracking of his movements, particularly the long-term intrusion on his privacy that occurred in this case and particularly given the government's acknowledgment at trial that the defendant had no idea that his location and movements were being electronically tracked due to his possession of a cell phone. The government's seizure of the location data had the same effect as seizing a diary of the defendant's movements for more than two months, much the same as if Davis's cell phone were converted into a Global Positioning System (GPS) tracker attached to his person.

Unlike cases involving mere business records or information expressly stated, or digitally entered and sent, to a service provider, or other information *self-evidently* shared with unrelated third parties, the pinpoint tracking of a person's location and

movements based merely on the possession or use of a cell phone is particularly invasive and undermines traditional notions of privacy. Like the GPS tracking information the Supreme Court considered in *United States v. Jones*, 132 S. Ct. 945 (2012), location data reveals intimate information about users' personal lives and intrudes on reasonable expectations of privacy. As with wiretapping, acquisition of location data is hidden, continuous, indiscriminate, and intrusive. As a result, such acquisition must be subject to the rigorous judicial oversight that the warrant requirement provides.

The maintaining of location data by cell phone providers does not detract from reasonable expectations of privacy. A person can always be deemed to have shared, directly or circumstantially, indicia of the person's location with third parties—such as by being observed by passers-by in the street—but that type of ubiquitous and unavoidable sharing of potential observation does not give the government a right to warrantlessly track a person's movements via electronic means, whether by real-time monitoring or by collecting the historical data that cell phone providers, operating within a government-regulated environment, are compelled to turn over to the government.

The government's theory that the defendant consented to the electronic tracking is refuted not merely by the position the government advanced at trial—that the

defendant had no idea that such location information was being transmitted or provided and recorded for later use, upon demand, by the government—but also by the absence of any showing that people generally believe that the *government* has warrantless access to location information conveyed by their cell phones or other mobile devices or indeed that people are aware of the *extent* of location information transmitted, and continuous nature of the transmission, due merely to the possession or use of a cell phone.

Unlike a pen register, for which there is a long historical understanding that numbers dialed—or directly provided to a telephone operator as in the original operation of wired telephone services—are part of the records belonging to the telephone company, used and maintained for billing and other purposes, and unlike the outside of a mailed envelope, where the addressing is plainly shared with the governmental postal service and the letter recipient with no expectation of privacy, electronic tracking of movements and location through cell tower data intrudes into basic notions of privacy in ways that expert witnesses are called upon to explain in trials. The Fourth Amendment would be unduly eroded by permitting warrantless accessing of such personal data electronically conveyed due to the necessity of cell phone usage.

The violation of Davis's Fourth Amendment rights resulted in severe, unfair prejudice at trial. The government relied heavily on the location evidence to support its theory that Davis was at the scene of six of the seven charged robberies. The remaining evidence of Davis's presence was dubious and highly disputed. Absent the cell site evidence, it is unlikely the jury would have convicted Davis and even more unlikely that a conviction would have resulted as to all of the charged robberies.

The good faith exception to the warrant requirement does not apply here. First, the application and order were facially defective, failing to identify accurately any violation of federal law. More importantly, the statute on which the government relied for the warrantless seizure is ambiguous and contradictory: one section requires the government to obtain a warrant for historic CSLI, while the very next section allows the government to obtain CSLI on a lesser showing. This internal conflict is ambiguous in its authorization to conduct a warrantless search. Further, judicial precedent interpreting warrantless searches in this context pointed in conflicting directions. In light of the statutory ambiguity and the evolving, unsettled nature of pertinent case law, good faith requires erring on the side of complying with the Fourth Amendment's warrant requirement. Moreover, applying the exclusionary rule in this context would have the required deterrent effect because the discretionary choice at issue was a law enforcement decision to pursue a warrantless search, not a magistrate's

legal determination that a particular warrant adequately expressed probable cause. The government attorney made a strategic choice to conduct a warrantless search based on a defective and overbroad request. That choice cannot now be insulated from reversal on appeal because the Assistant United States Attorney submitted an unsworn application to a magistrate judge stating a need for further investigation. The district court did not make a good faith finding in Davis's case, requiring at the least a remand for that determination.

EN BANC ARGUMENT AND CITATIONS OF AUTHORITY

I.

WARRANTLESS SEIZURE OF CELL TOWER SITE DATA VIOLATES THE FOURTH AMENDMENT RIGHTS OF CELL PHONE SUBSCRIBERS, WHO HAVE A REASONABLE EXPECTATION OF PRIVACY IN THEIR LOCATION INFORMATION.

1. The Fourth Amendment protects the individual's reasonable expectation of privacy against governmental intrusion and applies to emerging technologies.

Addressing the significant privacy issues pertaining to the search of an individual cell phone's stored data, the Supreme Court recently observed that "certain types of data," such as historical location data that "can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building" are "qualitatively different" than ordinary records and are deserving of special protection from governmental intrusion. *Riley v. California*, __ U.S. __, 134 S.Ct. 2473, 2490 (2014). The same heightened privacy information is at issue in this case, albeit obtained not directly from the defendant's phone, but from the service provider on whom the defendant, like any cell phone user, necessarily relied.

The defendant's position of reliance on a cell service provider is not unusual. As the Supreme Court noted in *Riley*, 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." *Id*. at 2484.

In declining to extend the search-incident-to-arrest doctrine to "searches of data on cell phones," the Supreme Court in *Riley* held "that officers must generally secure a warrant before conducting such a search." *Id*. at 2485. The Supreme Court thereby set a guidepost and a barrier between rapid technological advances and the erosion of privacy interests. *Riley* enforces the premise that "[t]he 'reasonableness' of an individual's expectation of privacy is not defined solely by technological progress." *People v. Cook*, 710 P.2d 299, 305 (Cal. 1985) ("We reject the Orwellian notion that precious liberties derived from the framers simply shrink as the government acquires new means of infringing them."); *see* Wayne LaFave, *The Forgotten Motto of Obsta Principiis in Fourth Amendment Jurisprudence*, 28 Ariz. L. Rev. 291, 307 (1986) ("it hardly makes sense to read *Katz* [*v. United States*, 389 U.S. 347, 88 S.Ct. 507 (1967)] as meaning that we assume the risk of whatever technology the government can bring to bear upon its investigative efforts").

The Fourth Amendment unequivocally protects individuals against governmental intrusion on their reasonable expectations of privacy. *See, e.g., Bond v. United States*, 529 U.S. 334, 340, 120 S.Ct. 1462, 1466 (2000) (citing *Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 2580 (1979), in turn quoting *Katz v.*

United States, 389 U.S. 347, 361, 88 S.Ct. 507, 516 (1967) (Harlan, J., concurring)). The Supreme Court has recognized that the government may not exploit evolving technologies to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo v. United States*, 533 U.S. 27, 34, 121 S.Ct. 2038, 2043 (2001). The government, if it employs technology to learn information that would be available otherwise only by means of a warrant, has engaged in a search in violation of the Fourth Amendment. *United States v. Karo*, 468 U.S. 705, 715–16, 104 S.Ct. 3296, 3303–04 (1984).

2. The nature of CSLI demonstrates that cell phone users have a reasonable expectation of privacy in such information.

The government employs historical CSLI to establish a defendant's location at a particular time. *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 311 (3d Cir. 2010). If a user's phone communicates with a particular site, the logical inference is that the user has physically been within the range of the site. *See generally In Re Application of the U.S. for an Order Authorizing the Release of Historical Cell–Site Info.,* 809 F.Supp.2d 113, 115 (E.D. N.Y. 2011). "Due to advances in technology and the proliferation of cellular infrastructure, cell-site location data can place a particular cellular telephone within a range approaching the accuracy of GPS." *In re Application for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F.Supp.2d 526, 534 (D. Md. 2011).

Because cell phones are pervasive in American society and people keep them on their person, unlike land-line telephones, "cellular service providers have records of the geographical location of almost every American at almost every time of day and night." *In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.,* 809 F.Supp.2d at 115. When the government obtains CSLI, monitoring and recording people's physical movements, it can create "a map of our lives, and learn the many things we reveal about ourselves through our physical presence." *Id.*

The Florida Supreme Court has ruled that "cell phones are 'effects' as that term is used in the Fourth Amendment." *Tracey v. Florida*, __ So.2d __, 2014 WL 5285929, at *18 (Fla. Oct. 16, 2014) (recognizing, as well, "the close relationship an owner shares with his cell phone, thereby making a cell phone's movements its owner's movements, often into clearly protected areas"). On that basis, the Florida Supreme Court invalidated the seizure of realtime CSLI without a warrant supported by probable cause. Ruling that an individual has a reasonable expectation of privacy in such location data, *id.* at *19, the Court reasoned that whether or not a cell phone user is aware or should be aware that his service provider can detect the location of his cell phone for call-routing purposes, "does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes. While

a person may voluntarily convey personal information to a business or other entity for personal purposes, such disclosure cannot reasonably be considered to be disclosure for all purposes to third parties not involved in that transaction." *Id.*, at *16 (& cases cited therein). The rationale articulated by the Florida Supreme Court in *Tracey* applies equally to the seizure of historical CSLI in the present case.[1]

Just as a passenger on a common carrier does not expose luggage to police search by placing it in the custody of a carrier, *see*, *e.g.*, *Florida v. Royer*, 460 U.S. 491, 497, 103 S.Ct. 1319, 1323–24 (1983), wireless communication through the service provider's system does not imply consent to release of information as to the user's location. Cell phone customers possess an equivalent property interest in their location data. Citizens do not give a "proprietor blanket authority to authorize the

[1] The Florida Supreme Court's reluctance to convert the status of carrier and customer into an adversarial one is consistent with this Court's recognition that a form contract from a common carrier does not necessarily resolve the status and obligations of the parties, even where such a contract is actually in the record (and there is *no such contract in the present record*). *See*, *e.g.*, *Franza v. Royal Caribbean Cruises, Ltd.*, ____ F.3d ___, 2014 WL 5802293, at *10 (11th Cir. Nov. 10, 2014) ("Finally, even if we were to look to the contract at this stage, we would not consider the nurse and doctor to be independent contractors simply because that is what the cruise line calls them. *See*, *e.g.*, *Cantor v. Cochran*, 184 So.2d 173, 174 (Fla. 1966) ('While the obvious purpose to be accomplished by this document was to evince an independent contractor status, such status depends not on the statements of the parties but upon all the circumstances of their dealings with each other.'")). *See Franza,* at *1 (concluding that "the evolution of legal norms, the rise of a complex cruise industry, and the progression of modern technology" erased former limitations on the rights of a cruise passenger).

police to search" what they have only incidentally left in their host's custody. *Stoner v. California*, 376 U.S. 483, 488, 84 S.Ct. 889, 892 (1969). A cell phone user, by merely placing or receiving a call (*whether by passive or active use of the phone*), does not yield his or her reasonable expectation of privacy in historical cell location information. A cell phone customer's reasonable privacy interest in CSLI is not diminished by cell company access to location data.

The third party doctrine is inapplicable in the context of CSLI and does not vitiate the privacy interest of cell phone users in CSLI. "A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 317 (3d Cir. 2010). Instead, "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." *Id.* at 317–18 (emphasis added; citation omitted). Not every transmission of information to a third party waives a reasonable expectation of privacy. *See Ex Parte Jackson*, 96 U.S. 727, 733 (1877) (explaining that letters do not lose Fourth Amendment protection despite being deposited with the post office and handled by numerous other people). The mere fact that a third party

may access information or data—and even chooses to access the information sometimes—fails "to extinguish a reasonable expectation of privacy." *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2011); *id*. at 286–87 (explaining that although people use internet service providers as an intermediary to send emails and the ISPs can access emails, people maintain a reasonable expectation of privacy and the government must obtain a warrant to access this data).

CSLI is not a mere business record; instead, as a result of a government-created surveillance environment acceded to by cell phone companies, it serves the function of a law enforcement record. The Davis trial transcript, D.E. 283:220–21, shows that the MetroPCS records custodian witness called by the government was one of three retired police officers hired by the cell phone company as a records custodian and sent to school for the purpose of being trained to testify "in cases such as this one." DE:283:220-21. The testimony went well beyond record verification and included attesting to the nature and meaning of the cell tower data with respect to location of the subscriber. The coerced cooperation of the cell phone company does not reduce the burden that the government must meet under the Fourth Amendment. And the fact that the government is investigating criminal activity does not relieve it from the warrant requirement. *See In re Application of the U.S.*, 620 F.3d at 318.

3. To the extent that the Stored Communications Act permits the seizure of CSLI without a warrant, without demonstrating probable cause, and without any time restriction, it violates the Fourth Amendment.

The Stored Communications Act ("SCA") provides for the issuance of a court order to require a provider of electronic communications service or a remote computing service to disclose records concerning electronic communication service or remote computing service upon the government's offering of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(c), (d). This standard is substantially less than what is necessary for a search warrant. *In re Application of the U.S.*, 620 F.3d at 315. The "reasonable grounds to believe" standard "is less stringent than probable cause." *Id.*; *see also In re Application*, 809 F.Supp.2d at 115 ("This showing is lower than the probable cause standard required for a search warrant."). In addition, this standard omits the requirement stated in the text of the Fourth Amendment that the facts proffered to establish probable be made under oath. *See* Fed. R. Crim. P. 41(d). Nor does the SCA establish any time limit for the extent of the records, and the period of cell phone location tracking, subject to the order.

The SCA, in permitting the seizure of historical CSLI without a warrant, intrudes on cell phone subscribers' legitimate expectations of privacy. Individuals enjoy a subjective and objectively reasonable expectation of privacy in their homes, offices, houses of worship, and other private places, even though technology enables the government to track them to and in those places without physically intruding on the private property. *Kyllo*, 533 U.S. at 34, 121 S.Ct. at 2043. CSLI provides the government with details about person's whereabouts and movements. "Location data from a cell phone is distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation." *In re Application of the U.S. for Historical Cell Site Data*, 849 F.Supp. 2d at 540; *see also id.* at 540-41 (describing that CSLI can be as accurate as GPS location, and that the technology can place a phone inside a specific home, even if locating a person there requires some inferences).

Even more intrusive, historical CSLI allows the government to retroactively observe a suspect via technology, as well as in the course of private and intimate personal, social, religious and other associations, interactions, and activities. *See Jones*, 132 S.Ct. at 955 (citing *People v. Weaver*, 909 N.E. 2d 1195, 1199 (N.Y. 2009))(Sotomayor, J., concurring)(electronic "monitoring generates a precise,

comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

A cell phone user's expectation of privacy in historical location information is at least as great as a privacy interest in realtime or prospective tracking. "The fact that the government seeks information that has already been created says nothing about whether its creator has a reasonable expectation of privacy in that information." *In re Application*, 736 F.Supp.2d 578, 585 (E.D. N.Y. 2010). For example, a person retains an expectation of privacy in the contents of a diary, even though the government seeks to read it after it was written. *Id.* Any distinction between historical, realtime, or surveillance would be impossible without technological intrusion because CSLI recreates a suspect's movements after those movements occurred.

The reasonable expectation of privacy in CSLI likewise equals or exceeds that of GPS data. In *Jones*, the Supreme Court ruled that a warrant based on probable cause is required to support the retrieval of location data obtained by the placement of a GPS device under an individual's automobile. While the decision was premised on a trespass theory, at least five justices recognized that an individual has a reasonable expectation of privacy with respect to long term monitoring of his or her movements, including via a GPS device. As the panel decision in this case

recognized, a car owner can reasonably expect that his individual movements may be observed, but that

> there will not be a 'tiny constable' hiding in his vehicle to maintain a log of his movements. 132 S.Ct. at 958 n. 3 (Alito, J., concurring). In contrast, even on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way. One's cell phone, unlike an automobile, can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one. When one's whereabouts are not public, then one may have a reasonable expectation of privacy in those whereabouts. Therefore, while it maybe the case that even in light of the *Jones* opinion, GPS location information on an automobile would be protected only in the case of aggregated data, even one point of cell site location data can be within a reasonable expectation of privacy. In that sense, cell site data is more like communications data than it is like GPS information. That is, it is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private.

Davis, 754 F.3d at 1216.

Further, the comparative degree of precision of CSLI and GPS data does not impinge on an individual's legitimate expectation of privacy, where CSLI is sought for the express purpose of establishing an individual's location at a specific date and

time. As the panel decision in this case recognized, "There 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. ... That information obtained by an invasion of privacy may not be entirely precise does not change the calculus as to whether obtaining it was in fact an invasion of privacy." *Davis*, 754 F.3d at 1216.

An individual does not surrender his reasonable expectation of privacy in CSLI by placing or receiving a call. The contention that a cell phone subscriber lacks a protectible Fourth Amendment interest in CSLI because he or she "voluntarily conveys" such information to his cell phone company is a fiction not grounded in the realities of modern cell phone usage. *See In re Application of the U.S. for an Order Authorizing the Release of Historical Cell–Site Info.*, 809 F.Supp.2d at 127 ("The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected.").

Instead, such a contention relies on case law involving pen registers and business records of banks and similar entities that is inapposite to CSLI and the seizure of such electronic information under the SCA. No one at MetroPCS witnessed Davis's movements, let alone any criminal activity. The government required MetroPCS to provide a record of his movements, using MetroPCS as the custodian.

The technology itself needs only ephemeral and anonymous detection of location. Using this artefact of the technology as a retrospective homing beacon does not transform MetroPCS into a witness. Without the government's action, no person would have been exposed to Davis's every move, through review of a huge number and varied locations of calls, for two months. Human eyes would never have reviewed his location data, but for the application and order.

In *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577 (1979), invoked by the government, the Supreme Court upheld the use of a pen register installed at the offices of a phone company to obtain the numbers dialed by a customer on the basis that a telephone customer does not have a reasonable expectation of privacy in the phone numbers dialed on telephone company switching equipment. The ruling in *Smith* is limited to phone company records of the numbers that the customer affirmatively dials from his or her phone. *Id.* at 744, 99 S.Ct. at 2582 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

The *location* of the cell phone customer at the time calls were made or received—*unlike* the numerical information affirmatively disclosed by the customer

when using his phone—is information that was *not* voluntarily conveyed by any action on his part. Nor does *Smith* purport to address records as to a subscriber's location at the time of calls. *Smith* involved landline telephones and did not address the far different context of mobile cell phone usage and cell tower location data. *See Smith,* U.S. at 743, 99 S.Ct. at 2582 ("*Regardless of his location*, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call.")(emphasis added).

The Court in *Smith* found that "all subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, *for they see a list of their long-distance (toll) calls on their monthly bills*." 442 U.S. at 742, 99 S.Ct. at 2580 (emphasis added). No such comparable information is given to cell phone users on their monthly bills with respect to their *locations* at the time of making or receiving calls.

The government has cited *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619 (1976), for its ruling that bank customers lack a reasonable expectation of privacy in information voluntarily conveyed to banks, including checks, deposit slips, and financial statements. The Court in *Smith v. Maryland* relied on *Miller* to support its analysis that telephone subscribers voluntarily convey to their phone company the numbers dialed on their phones.

Miller likewise is wholly distinguishable from the instant context. Bank customers personally provide their banks with checks and deposit slips and receive monthly bank statements setting forth customer financial records. No cell phone customer personally provides his or her cell phone company with information concerning his whereabouts at the times calls are made or received nor does the company advise the customer of such information in its phone bill statements.

Moreover, as the Court in *Miller* recognized, "checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." 425 U.S. at 442, 96 S.Ct. at 1623. CSLI, which is not tangible or visible to a cell phone user, is not a propriety business record within a company's complete, unfettered control, such as an expense report. An individual's location and movements are not analogous to financial business data used in commercial transactions between people and entities, nor does an individual phone user affirmatively disclose to phone company employees his or her whereabouts when making and receiving calls.

Despite using an intermediary to place a phone call, cell phone customers take no affirmative steps to disclose their location to the public. CSLI is generated

automatically and conveyed without any choice or overt action explicitly exposing location. The user does not knowingly and voluntarily disclose the information under her own control. Unlike dialed telephone numbers or bank deposit slips, CSLI is not subject to general understanding any more than the operation of a satellite television signal. Indeed, interpreting this cell site data requires an understanding of radio frequency engineering. *Cf. Katz*, 389 U.S. at 351-52, 88 S.Ct. at 510-11 (holding that information that a person *knowingly* exposes to the *public* is not protected). Instead, it is transmitted independently of any input, control, or knowledge on the part of the cell phone user. To the extent that an unknowing, involuntary transmission of data that is automatically collected constitutes disclosure to a third party at all, a cell phone user's conduct is materially different from the active, deliberate choices made to disclose information that the Court discussed in *Smith* and *Miller*. The simple act of using, or even just carrying, a cell phone, which has the by-product of generating location data, does not indicate a disinterest in maintaining privacy.

Ultimately, the government's arguments are akin to the now discredited reasoning of *Olmstead v. United States*, which imbued the mechanics and the pseudo-public character of telephone signals with Fourth Amendment significance. 277 U. S. 438, 466, 48 S.Ct. 564, 568 (1928) ("[O]ne who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite

outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment.").

The nature of CSLI distinguishes this case from other cases involving the third party doctrine. As the Supreme Court has recognized, the nature of the record is critical to determining whether a person maintains a privacy interest. *Smith*, 442 U.S. at 741, 99 S.Ct. at 2580-81. Pen registers, for example, provide the government with very limited information. *Id.* CSLI, on the other hand, is more analogous to content, in which people maintain a privacy interest, although intermediaries have access to the information, because of detail it provides the government. *In re Application*, 809 F.Supp.2d at 124-25; *see also Davis*, 754 F.3d at 1216 (cell site data likened to communications data).

CSLI has attributes of content because of the highly personal nature of the data and the amount of information that it reveals about a person. Because cumulative CSLI, recording a person's movements over a prolonged period, "implicates sufficiently serious protected privacy concerns" it should be treated as "content, to prohibit undue governmental intrusion." *Id.* at 126. "There is no meaningful distinction between content and other forms of information, the disclosure of which to the government would be equally intrusive and reveal information society values as private. " *Id.* at 125 (relying on *Smith*, 442 U.S. at 741 n.5, 99 S.Ct. at 2580 n.5).

And the content of communications is not available to the government without a warrant, even if a third party stores and has access to it.

A cell phone customer's communication to the service provider intended to advance the commercial relationship is the telephone number dialed, *not* location information, and certainly *not* a series of location points over the course of months. A service provider might compel a cell phone customer to disclose location information to route calls, but compulsion is not choosing to disclose, and does not release a reasonable expectation of privacy in the totality of movements over a prolonged period. A person might grant a third party access because it is essential to the customer's interest, but the actual transmission of information that the customer intends is to a different party altogether—the recipient of the email in that case.

Unlike other records that a business might generate, Congress has directed cellular service providers to protect the confidentiality of CSLI. The Wireless Communication and Public Safety Act obliges cellular service providers to protect information that they acquire solely by virtue of the fact that they provide a telecommunications service to the customer. *See id.* at 841–42 (referring to 47 U.S.C. § 222(f)). Although this statute does not prevent law enforcement from accessing the information, the Congressionally-mandated limit on using the information that affects the provider's "proprietary interest . . . is undeniably relevant to the legitimate

expectation of privacy inquiry." *Id.* at 842. In contrast, relating to the records at issue in *Miller*, Congress had specifically legislated that customers should not expect to maintain privacy in information conveyed to banks. *See Miller*, 425 U.S. at 441, 96 S.Ct. at 1623 (relying on 12 U.S.C. § 1829(a)(1)).

Cell phone users maintain a subjective expectation of privacy in CSLI that society recognizes as reasonable. Not only does the third party doctrine fail to eliminate a subjective expectation of privacy, no other aspect of the technology or consumer relationship impinges on the subjective expectation of privacy.

An assumption that cell phone users understand the location tracking that occurs and that users voluntarily choose to convey location information is unsupported. A privacy policy does not impact on a cell phone customer's expectation of privacy.[2]

---

[2] Academics who study privacy have found that technology users rarely read or understand privacy policies. *See, e.g.*, Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 Info. Sys. Research 254, 256 (2011); Carlos Jensen, et al., *Privacy Practices of Internet Users: Self Reports Versus Observed Behavior*, 63 Int'l J. Human-Computer Studies 203, 223 (2005). Similarly, senior government officials responsible for consumer protection publically acknowledge that privacy policies do not impact consumer choices or beliefs. The Chairman of the Federal Trade Commission stated at the FTC Privacy Roundtable in 2009, "We all agree that consumers don't read privacy policies." *Id.* at 6; Statement of Thomas J. Sugrue, Chief, Wireless Telecommunications Bureau, FCC, Subcommittee on Telecommunications Trade, and Consumer Protections, House of Representatives Commerce Committee Hearing, June 14, 2001 (http://transition.fcc.gov/Speeches/misc/statements/sugrue061401.pdf). The Director of the FTC's Bureau of Consumer Protection told the New York Times that "I don't believe that most consumers either read [privacy policies] or, if they read

(continued...)

Nor is there any evidence in the instant case of the existence of such a privacy policy with respect to Davis's cell phone company, MetroPCS.

If society is "prepared to recognize as reasonable" a person's subjective expectation of privacy, then the Fourth Amendment applies. *Smith*, 442 U.S. at 740, 99 S.Ct. at 1580. Society continues to recognize location data as private, even if a third party generates and has access to it. *Cf. Katz*, 389 U.S. at 351, 88 S.Ct. at 511 ("what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

For example, when the American public learned that Apple iPhones stored ten months of location data in an unencrypted format, consumer complaints prompted Apple to revise its entire iPhone operating system within a week to prevent the potential for access to what customers considered private. Press Release, Apple, Inc., *Apple Q&A on Location Data* (April 27, 2011) (available at https://www.apple.com/pr/library/2011/04/27Apple-Q-A-on-Location-Data.html);

---

[2](...continued)
them, really understand it." Charlie Savage, U.S. Tries To Make It Easier To Wiretap The Internet, New York Times, Sept. 27, 2010 (http://www.nytimes.com/2010/09/27/ us/27wiretap.html?pagewanted=all&_r=0). Notably, the Chief Justice of the United States, John Roberts, has admitted that he generally does not read privacy policies or terms of service. *See* Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, A.B.A. Journal (Oct. 20, 2010).

Nick Bilton, *Tracking File Found in iPhones*, N.Y. Times, April 20, 2011. "Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which the consumers provide the data." White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* 15 (2012). In fact, in the press release, Apple informed customers that it will only collect and share location data anonymously, leading customers to believe that their location information remained private, although Apple still collects and uses it.

No analogous deliberate relinquishment of privacy occurred here regarding CSLI. The service provider's automatic generation of location data is entirely unlike selecting a screen name, providing a home address, and uploading photos. No conduct on the part of a cell phone user gives rise to an inference that the user no longer maintained a subjective expectation of privacy.

Even if it were applicable, the third party doctrine bears reconsideration. The third party doctrine first noted in *Katz* "has often been criticized as circular, and hence subjective and unpredictable." *Kyllo*, 533 U.S. at 34, 121 S.Ct. at 2043 (internal quotation and citation omitted). It "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." *Jones*, 132 S.Ct. at 957 (Sotomayor, J., concurring).

"Unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept risk of surveillance." *Smith*, 442 U.S. at 750, 99 S.Ct. at 2585 (Marshall, J., dissenting). And "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Id.* The Fourth Amendment should not "treat secrecy as a prerequisite for privacy." *Jones*, 132 S.Ct. at 957.

The SCA is unconstitutional not only in permitting the disclosure of records tracking a cell phone user's movements within constitutionally protected spaces, but also in allowing the seizure of records tracing a person's whereabouts over an extended period, thus revealing an intimate portrait of personal, social, religious, medical, and other activities and interactions. Five Supreme Court Justices, speaking through concurring opinions, and multiple lower courts, recognize a subjective and objectively reasonable expectation of privacy in location, albeit in public places, when the government tracks people over a prolonged period. *See, e.g., Jones*, 132 S.Ct. at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring); *United States v. Maynard*, 615 F.3d 544, 562–63 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S.Ct. 945; *People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009).

When electronic location tracking achieves nothing more than what traditional visual surveillance would reveal, like straightforward movements from one location

to another on public streets, then the tracking may not necessarily infringe upon a Fourth Amendment privacy interest. *See Knotts*, 460 U.S. at 281, 103 S.Ct. at 1085 ("The governmental surveillance . . . amounted principally to the following of an automobile on public streets and alleyways.") This conclusion, however, fails to address "dragnet type law enforcement practices" like the government's observing a suspect's movements constantly for 24 hours. *Id.* at 283-84, 103 S.Ct. at 1086. Different constitutional principles apply to that type of surveillance. *Id.* No conceivable interpretation of the quantity of location data allowed by the SCA could equate it with straightforward visual surveillance of public movements. *See Jones*, 132 S.Ct. at 964 (Alito, J., concurring) (using technology to secretly monitor every movement for four weeks is subject to a warrant, although physically following a suspect for a short time is not).

Prolonged surveillance of a person's movements reveals intimate details of a person's life. *Maynard*, 615 F.3d at 562. One may not have a privacy interest in a single trip on a public road, because it reveals little about a person and the public may easily observe it. But a person retains a privacy interest in "the whole of one's movements" over the course of at least a month because "prolonged 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." *Id.* For

example, "repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month." *Id.* If the government knows all of a person's movements, it "can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups." *Id.* In his concurrence in *Jones*, Justice Alito remarked that the government crossed the Fourth Amendment line before four weeks of constant tracking. 132 S.Ct. at 964.

The fact that *Jones*/*Maynard* addressed GPS rather than CSLI does not impair its relevance to this case. The particular technology is not what establishes the Fourth Amendment privacy interest; the type of information and intrusion raises the constitutional concerns. *See Kyllo*, 533 U.S. at 35-36, 121 S.Ct. at 2044. And as discussed above, there is little practical difference between GPS tracking and tracking via CSLI. As Justice Alito pointed out in his concurrence in *Jones*, cell phones and other wireless devices "permit wireless carriers to track and record the location of users." *Jones*, 132 S.Ct. at 963.

Historic CSLI "captures enough of the user's location information for a long enough time period . . . to depict a sufficiently detailed and intimate picture of [the user's] movements to trigger the same constitutional concerns as the GPS data in

Maynard." *In re Application*, 809 F.Supp.2d at 119. Indeed, CSLI presents "even greater constitutional concerns than the tracking at issue in *Maynard*," because it entitles the government to conduct "'mass' or 'wholesale' electronic surveillance." *Id.* It depicts substantially more details about a person's movements than the GPS data in *Maynard* because it is not dependent upon a person driving to a place. If a person walks, uses public transportation, refrains from moving, or is a passenger in another person's car, the government can still track his or her whereabouts with CSLI.

The government collected "a precise, comprehensive record" of the defendant's "public movements that reflect a wealth of detail." *Jones*, 132 S.Ct. at 955. Providing the government with this private information, absent a showing of probable cause, allows for "arbitrary exercises of police power" and "'a too permeating police surveillance.'" *Id.* (quoting *United States v. Di Re*, 332 U.S. 581, 595, 68 S.Ct. 222, 229 (1948)).

The SCA, in permitting the government's warrantless acquisition of CSLI, including for prolonged, continuous time periods, intrudes on a subjective expectation of privacy that society recognizes as reasonable and is unconstitutional.

II. EVEN IF THE WARRANTLESS SEIZURE OF CELL TOWER SITE DATA WERE PERMITTED IN LIMITED CIRCUMSTANCES, THE SEIZURE IN THE PRESENT CASE, INVOLVING 67 CONSECUTIVE DAYS OF CELL TOWER SITE DATA, WHERE THE GOVERNMENT, IN SEEKING AN ORDER TO COMPEL DISCLOSURE, ASSERTED THAT ONLY SEVEN DAYS OF CELL SITE DATA MET THE RELEVANCE AND MATERIALITY TEST, WAS UNREASONABLE AND VIOLATED THE FOURTH AMENDMENT.

The seizure of CSLI for a period exceeding two months intruded on Davis's reasonable expectation of privacy. The Fourth Amendment protects against location tracking of an individual such as Davis over a prolonged period. Davis did not knowingly or voluntarily share such extensive information concerning his location. The government offered no evidence that Davis's cell phone company informed him of a policy regarding the disclosure of CSLI nor that Davis ever consented to such disclosure. The government argued, in fact, that Davis and his codefendants lacked knowledge of CSLI.

The long-term tracking of Davis's cell phone over a period of 67 days was a unconstitutionally invasive search. Efforts "to bring the guilty to punishment, praiseworthy as they are, are not to be aided by the sacrifice of those great principles established by years of endeavor and suffering which have resulted in their

embodiment in the fundamental law of the land." *Weeks v. United States*, 232 U.S. 383, 393, 34 S.Ct. 341 (1914).

The government created and exploited a surveillance environment, in which cellular service providers have acquiesced, rendering the ensuing data law enforcement, not business, records. Even if a business has some non-law enforcement purpose in collecting data, when there is an agreement to share data with the government and when the data is collected "to generate evidence *for law enforcement purposes*," then collecting the data and sharing it with the government is a Fourth Amendment search, not a business-related event. *Ferguson v. City of Charleston*, 532 U.S. 67, 83, 121 S.Ct. 1281, 1291 (2001) (emphasis in original). When the government removes legal barriers to a common carrier collecting data, makes plain its "strong preference" for collecting and storing the data, and communicates "its desire to share in the fruits of such intrusions," then the common carrier has conducted a search on behalf of the government. *Skinner v. Railway Labor Executives' Assoc.*, 489 U.S. 602, 615, 109 S.Ct. 1402, 1412 (1989). To turn a business's data collection efforts into a search that violates the Fourth Amendment, the government must take some steps authorizing and offering affirmative encouragement for the collection. *United States v. Jarrett*, 338 F.3d 339, 344, 346 (4th Cir. 2003).

"The justifications for the good-faith exception do not extend to situations in which police officers have interpreted ambiguous precedent, or relied on their own extrapolations from existing caselaw." *United States v. Davis*, 598 F.3d 1259, 1267 (11th Cir. 2010) (internal quotation marks and citations omitted). That type of "legal analysis [is] better reserved to judicial officers, whose detached scrutiny . . . is a more reliable safeguard against improper searches." *Id.* "When law enforcement officers rely on precedent to resolve legal questions as to which '[r]easonable minds . . . may differ,' *Leon*, 468 U.S. at 914, 104 S.Ct. at 3416, the exclusionary rule is well-tailored to hold them accountable for their mistakes." *Davis*, 598 F.3d at 1267. The good faith exception thus does not insulate the government from making incorrect legal decisions based on ambiguous or contradictory authority regarding the constitutionality of a search. *Id.* Acting in good faith when the law is unsettled means erring on the side of caution and the Constitution. *See United States v. Johnson*, 457 U.S. 537, 561, 102 S.Ct. 2579, 2593 (1982) (holding that, when constitutional questions are unsettled, objectively reasonable officers err on the side of strictly complying with the Fourth Amendment rather than engaging in the constitutionally risky search behavior).

The Supreme Court's opinion in *United States v. Jones*, 132 S.Ct. 945 (2012), addressed a Fourth Amendment challenge to the seizure of location evidence obtained over a 28-day period after a law enforcement officer attached a GPS tracking device

to an individual's automobile. *Id.* at 947. A five-member majority held the Fourth Amendment was violated; the Court applied a physical trespass rationale. *Id.* at 949-54. Two concurring opinions endorsed by a total of five justices embraced an alternative rationale for finding a Fourth Amendment violation: The defendant's reasonable expectation of privacy rendered the GPS tracking unconstitutional. *Id.* at 955 (Sotomayor, J., concurring) (quoting *Katz v. United States*, 389 U.S. 347, 353 (1967)); *id*. at 958 (Alito, J., concurring). Five Supreme Court justices agreed in *Jones* that (1) the government conducts a Fourth Amendment search when it engages in prolonged location tracking, and (2) prolonged location tracking violates reasonable expectations of privacy. *See* 132 S. Ct. at 964 (Alito, J., concurring in the judgment); id. at 955 (Sotomayor, J., concurring). While the majority opinion in *Jones* relied on a trespass analysis in concluding a search had occurred, it specified that "[s]ituations involving merely the transmission of electronic signals without trespass" are subject to analysis to determine whether reasonable expectations of privacy have been violated. *Jones*, 132 S. Ct. at 953.

In this case, the government obtained, without a warrant, more than two months worth of historical data that it used to learn of Davis's movements. D.E. 266-1:2. Davis did not expect to be subjected to such an egregious, long-term intrusion on his privacy, and his expectation of privacy was reasonable. Indeed, the prosecutor told the

jury that Davis "could not have known … his cell phone was tracking his every moment [sic]." D.E. 287:4-5. The application did not purport to justify seizing months of data, offering a rationale only for seven days of calls; and the application and order notably failed to relate the application to any potentially applicable federal criminal statute. The facial defects in the application and order, in combination with its excessive scope and the absence of any evidence of consent or knowledge of a privacy waiver by Davis, render the search violative of the Fourth Amendment even if the SCA itself were not found unconstitutional in all applications to cell tower site data.

Significantly, the prosecutor stressed Davis's ignorance of the location tracking data as a fact demonstrating guilt. D.E. 287:14. Even absent the prosecutor's arguments to the jury, there would be no reason to assume Davis knew he was conveying location evidence to his service provider each time he used his phone. By engaging in the physical act of dialing a phone number, a phone user reasonably could deduce that he was sharing the dialed number with his service provider. The collection of location information, however, occurs covertly. Also, while some cell phone bills may document phone numbers called, or from whom calls are received, cell tower location information is not routinely provided to customers. The involuntary conveyance of location data does not eliminate an individual's expectation of privacy, as explained by the Third Circuit. *In re Application of the U.S.*, 620 F.3d at 317-18

(ruling that cell phone customers neither voluntarily nor knowingly share location information with their cell phone providers; only information shared is the number dialed, which does not indicate to the caller that placing the call will also identify the caller's location; further, in receiving a call, the cell phone user does not voluntarily expose anything).

While the Fifth Circuit has reached the opposite conclusion, *see In re Application of the U.S. For Historical Cell Site Data*, 724 F.3d 600, 612 (5th Cir. 2013) (agreeing with the government that cell phone users "know that they convey information about their location to their service providers when they make a call and that they voluntarily continue to make such calls"), the Fifth Circuit's reasoning is dependent on facts not proven in this case. The Fifth Circuit's findings that cell phone customers knowingly convey location information to cell phone service providers and that customers know this information is collected were based largely on evidence that some service providers provide this information to their customers. 724 F.3d at 613. The government points to no such evidence in this case. Moreover, even if such information is available from Davis's service provider, there is no evidence that a reasonable person in Davis's position would be aware of it. The Fifth Circuit's findings also rely on the assumption that cell phone users have a detailed understanding of how calls are transmitted. *Id.* In this case, there is no evidence that

Davis understood how or why the dialing of a phone number caused the transmission of communications between two cell phones.

For these reasons, the assumptions supporting the Fifth Circuit's findings that cell phone users knowingly acquiesce in the creation and collection of location information have no application in this case. Instead, the government should be bound by the prosecutor's position at trial that Davis did not know his cell phone use was revealing his location.

The district court did not explain its reasons for denying the motion to suppress the cell tower site data. *See* D.E. 276; D.E. 277:45. The record reflects no finding that the prosecutor acted in good faith in seeking the cell tower site data without obtaining a warrant. Absent a finding of good faith, the admission of the cell tower site data cannot be affirmed on that basis. *See United States v. Accardo*, 749 F.2d 1477, 1481 (11th Cir. 1985) (remanding to permit the district court to decide the good faith issue in the first instance). Moreover, while evidence obtained by law enforcement officers in reliance on a statute later found to be unconstitutional may be admissible under the good faith doctrine, *see Illinois v. Krull*, 480 U.S. 340, 355, 107 S.Ct. 1160, 1170 (1987), this case presents materially different circumstances. The cell tower site data was obtained by a prosecutor, whose legal training and experience rendered

unreasonable any reliance on a statute that authorized a warrantless intrusion on a person's reasonable expectation of privacy.

The panel relied exclusively on *United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405 (1984), in analyzing whether the good faith exception to the exclusionary rule excuses the government's Fourth Amendment violation. The panel mistakenly focused on the actions of unidentified "officers," and it attributed the constitutional error to the magistrate judge. The panel stated that the officers in this case "acted in good faith reliance on an order" issued by a magistrate judge and "had a sworn duty to carry out the provisions of the order;" the panel also referred to "the 'magistrate's' error." *Davis*, 754 F.3d at 1217–18 (quoting *Leon*, 468 U.S. at 920 n.21, 104 S.Ct. at 3419). The record reflects no relevant action on the part of any law enforcement officer. At the prosecutor's request, the magistrate judge directed the cell phone provider to turn CSLI over to a federal agent. D.E. 266-1, 268-1. The agent, at most, served as a conduit in providing the records to the prosecutor. The prosecutor later told the district court he obtained the requested information and forwarded it to another police department for analysis. D.E. 364:167. In addition, constitutional error should not be attributed to the magistrate judge; instead, responsibility for the errors in this case rested primarily or exclusively with the prosecutor. The prosecutor's actions when he sought and obtained constitutionally-protected information without

meeting even the statutory standards, failing to identify a federal offense that was violated, and seeking an excessive amount of data, fell outside the bounds of objective good faith.

Leon establishes that any reliance the investigative team places on a decision made by a judicial officer must be objectively reasonable. 468 U.S. at 922, 104 S.Ct. at 3420. The task facing the magistrate in *Leon* was the well-established duty to determine whether the information presented by a police office sufficed to establish probable cause. The magistrate in *Leon* made that determination, albeit erroneously.

In contrast, the essential question underlying the constitutionality of the search and seizure in this case, i.e., whether CSLI could constitutionally be obtained by court order, was never presented to the magistrate judge. Further, when the prosecutor made an *ex parte* request for a court order, he could not reasonably have expected that the magistrate judge would *sua sponte* undertake an assessment of whether the prosecutor's request complied with the Fourth Amendment. Because the prosecutor did not raise the issue, the magistrate judge made no ruling touching on the constitutional question, possibly assuming that the prosecutor was pursuing a legitimate investigation under 18 U.S.C. § 2113, an offense that had nothing to do with the case. Thus, to the degree the government claims it relied on a decision made by the magistrate judge, that reliance was objectively unreasonable. Finally, the

analysis in *Leon* recognized that officers may rely in good faith on a judicial officer's issuance of a search warrant. Thus, *Leon* should not properly be applied to excuse, as here, the government's failure to seek a search warrant.

The government urged the panel to apply the good faith exception to the exclusionary rule based on the government's reliance on provisions of the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B) and (d). *See* Appellee's Initial Br. at 45 (citing *Illinois v. Krull*, 480 U.S. 340, 348-49, 107 S.Ct. 1160 (1987)). In *Krull*, the Supreme Court held that "a good-faith exception to the Fourth Amendment exclusionary rule applies when an officer's reliance on the constitutionality of a statute is objectively reasonable, but the statute is subsequently declared unconstitutional." 480 U.S. at 346, 107 S.Ct. at 1165 (emphasis added). The Court further held an officer cannot "be said to have acted in good-faith reliance upon a statute if its provisions are such that a reasonable officer should have known that the statute was unconstitutional." *Krull*, 480 U.S. at 355, 107 S.Ct. at 1170. The panel did not address *Krull* in its good faith analysis. Nor does *Krull* support a good faith finding in this case, because the government could not reasonably have relied on 18 U.S.C. § 2703(c)(1)(B) and (d) to authorize a warrantless search and seizure of CSLI. Section 2703 allows the government to obtain cell phone subscriber records by several routes, one being by a warrant obtained upon a showing of probable cause (§ 2703(c)(1)(A))

and another being by court order without probable cause (§ 2703(c)(1)(B), (d)). To obtain an order, the government need only offer "specific and articulable facts showing that there are reasonable grounds to believe that [the records] are relevant and material to an ongoing criminal investigation." § 2703(d). The government would not reasonably have believed Congress considered the application of § 2703 to the seizure of CSLI at the time it enacted the statute in 1986. The possibility that Congress contemplated the government's later use of the statute to obtain information that could track a cell phone user's movements in relation to suspected criminal activity is extremely remote. Federal case law documenting the use of CSLI to prove the whereabouts of criminal suspects first appears in the mid-1990's. *See, e.g., United States v. Thompson*, 454 F.3d 459 (5th Cir. 1996). Further, Congress could not have contemplated that Miami would be blanketed by a profusion of cell towers in 2011, the time of the charged offenses, resulting in the availability of effective tracking via CSLI. Thus, the government used § 2703(c)(1)(B) in a context not contemplated by Congress. When the issue is unsettled, courts "reject the government's invitation to allow police officers to rely on a diffuse notion of the weight of authority around the country." *United States v. Martin*, 712 F.3d 1080, 1082 (7th Cir. 2013). Given that neither the Supreme Court nor this Court had explicitly approved the particular police practice, the government may not, "for purposes of the exclusionary rule, . . . parse and

weigh the decisions of our sister circuits in an attempt to predict what this Court (or even the Supreme Court) would say if faced with a similar case." *United States v. Katzin*, 732 F.3d 187, 209 (3d Cir. 2013).

Krull's expansion of the good faith exception to encompass good faith reliance on statutes rests on the reasoning that "an officer cannot be expected to question the judgment of the legislature that passed the law." *Krull*, 480 U.S. at 349-50, 107 S.Ct. at 1167. In enacting § 2703, Congress made no judgment about whether prosecutors should be allowed to obtain CSLI by requesting a court order, rather than by establishing probable cause and obtaining a warrant. Thus, when the prosecutor chose to seek constitutionally protected CSLI without obtaining a warrant, he necessarily relied on his own judgment, as informed by his supervisors at the U.S. Attorney's Office and the policies of the U.S. Department of Justice. The prosecutor's judgment, rather than that of Congress, yielded the conclusion that CSLI could be obtained under the authority of the statute, without a warrant. *Krull*'s reasoning therefore does not establish objective good faith on the part of the government. Moreover, by crafting a statute that provided the prosecution with a warrant option and a non-warrant option, Congress manifested an expectation that the government would make a reasonable effort to determine whether the information it sought was protected by the Fourth Amendment. By providing a warrant option, Congress afforded prosecutors a safety

valve to use when seeking private information newly available due to advancing technology. When presented with a statute that provided those options, the prosecutor had a duty to pause and consider the constitutional implications of his request for CSLI. It is unreasonable to believe that Congress intended the warrant and non-warrant provisions to be used interchangeably, subject only to the preference of the prosecutor.

A statute enacted in 1998, after the government began using CSLI for prosecutorial purposes, should have put the government on notice that Congress viewed CSLI as more deserving of constitutional protection than other types of cell phone subscriber information. In 47 U.S.C. § 1002(a)(2)(B), Congress specifically forbade the government from using pen registers and trap and trace devices, which are issued on a relevance standard, 18 U.S.C. § 3123(a)(1), to gain access to "information that may disclose the physical location of the subscriber." The statute limiting the use of these investigative tools surely put the government on notice that Congress considered location information to warrant more protection than other information routinely obtained through phone records. An objectively reasonable prosecutor would have considered this statutory limitation in assessing whether § 2703(c)(1)(B), which embodies a similar standard, authorized a warrantless seizure of CSLI. At best, the prosecutor could have concluded that the law regarding the application of §

2703(c)(1)(B) to the modern technology used to harvest CSLI was unsettled. Acting in good faith when the law is unsettled requires erring on the side of caution and the Constitution. *United States v. Johnson*, 457 U.S. 537, 561, 102 S.Ct. 2579, 2593 (1982) (when constitutional questions are unsettled, objectively reasonable officers err on the side of strictly complying with the Fourth Amendment rather than engaging in constitutionally risky behavior). Instead, the prosecutor made a deliberate, strategic choice not to seek a warrant and, instead, to follow the easier, more expedient path of simply seeking a court order under § 2703(c)(1)(B). This decision is inconsistent with a finding of good faith.

The likelihood that the prosecutor subjectively believed that using the statute to obtain CSLI was constitutional is immaterial. The good faith exception must be applied using an objective reasonableness standard. *United States v. Herring*, 555 U.S. 135, 145, 129 S.Ct. 695, 703 (2009).

The government is an interested party that has a stake in all federal criminal prosecutions. It cannot be expected to view its options objectively when faced with the need to apply constitutional principles in circumstances that were not contemplated when long-standing doctrines were being developed. From the government's perspective, the interest of expediency in conducting criminal investigations may weigh in favor of using traditional investigative tools and methods aggressively to

obtain evidence made possible by recent technology, despite uncertainty about whether constitutional violations may result. If the government can be secure in the knowledge that the courts will apply the good faith exception to insulate from reversal convictions obtained through such evidence, the government has no reason to exercise caution in recognizing and protecting the Fourth Amendment rights of suspects.

The panel implicitly concluded that application of the exclusionary rule to the improperly-obtained CSLI would not have a deterrent effect in future investigations. However, the explosion of technological advances in recent years has created innumerable situations where prosecutors must assess whether traditional doctrines apply when accessing electronic data that did not exist or was not readily available at the time the doctrines were developed. The use of CSLI in criminal prosecutions is but one example of the manner in which modern technology creates uncertainty in how to apply traditional constitutional principles. For example, in *Riley v. California*, 134 S.Ct. 2473 (2014), the Supreme Court addressed whether police officers could conduct warrantless searches of digital information on cell phones in reliance on the well-established warrant exception for searches incident to arrest. The Court rejected various analogies advanced by the government in support of approving the warrantless searches and held that the time-honored search-incident-to-arrest exception to the warrant requirement could not justify the warrantless search of cell phone data. *See*

also Kyllo v. United States, 533 U.S. at 33, 121 S.Ct. at 2043 (noting that prior Fourth Amendment holdings should not be unduly extended in light of technological advances).

Exclusion of the CSLI obtained in violation of Davis's Fourth Amendment rights is necessary to deter future constitutional violations.

CONCLUSION

Based upon the foregoing argument and citations of authority, the Court should vacate Davis's convictions.

Respectfully submitted,

s/ Jacqueline E. Shapiro
JACQUELINE E. SHAPIRO, ESQ.
Attorney for Appellant
40 N.W. 3rd Street, PH 1
Miami, Florida 33128
Tel. (305) 403-8207
Fax: (305) 403-8209

CERTIFICATE OF COMPLIANCE

I CERTIFY that this brief complies with the type-volume limitation of FED. R. APP. P. 32(a)(7). According to the WordPerfect program on which it is written, the numbered pages of this brief contain 12,657 words.

s/ Jacqueline E. Shapiro
Jacqueline Shapiro

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a true and correct copy of the foregoing brief was forwarded by Fedex next-day service on November 15, 2014, for hand delivery on the 17th day of November 2014 to Assistant United States Attorney Amit Agarwal, 99 N.E. 4th Street, Miami, Florida 33132-2111.

s/ Jacqueline E. Shapiro
Jacqueline E. Shapiro