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 *AMICUS CURIAE* AT&T MOBILITY, LLC IN SUPPORT OF NEITHER PARTY

SUZANNE L. MONTGOMERY
ALTRESHA Q. BURCHETT-WILLIAMS
AT&T SERVICES, INC.
208 S. Akard St., Suite 500
Dallas, Texas 75202
Telephone: (214) 757-3389
Facsimile: (214) 446-6408

PETER D. KEISLER
RICHARD KLINGLER
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: (202) 736-8000
Facsimile: (202) 736-8711

Counsel for Amicus Curiae AT&T Mobility, LLC

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

United States v. Quartavious Davis
No. 12-12928

Amicus Curiae files this Certificate of Interested Persons and Corporate Disclosure Statement, as required by 11th Cir. R. 26.1.1, 28-1(b), and 29-2.

Agarwal, Amit, Assistant United States Attorney

Altman, Roy, Assistant United States Attorney

American Civil Liberties Union Foundation, *Amicus Curiae*

AT&T Mobility, LLC, *Amicus Curiae*

AT&T Inc. (T), Parent Corporation of AT&T Mobility, LLC

Bankston, Kevin, Counsel for Center for Democracy & Technology

Brown, Hon. Stephen T., United States Magistrate Judge

Burchett-Williams, Altresha Q., Counsel for AT&T Mobility, LLC

Caruso, Michael, Interim Federal Public Defender

Center for Democracy & Technology, *Amicus Curiae*

Colan, Jonathan, Assistant United States Attorney

Crump, Catherine, Counsel for *Amici Curiae* ACLU Foundation, et al.

Davis, Quartavious, Defendant/Appellant

Dube, Hon. Robert L., United States Magistrate Judge

Electronic Frontier Foundation, *Amicus Curiae*

United States v. Quartavious Davis
No. 12-12928

Fakhoury, Hanni, Counsel for Electronic Frontier Foundation

Ferrer, Wifredo A., United States Attorney

Fisher, Sylvester, Co-Defendant

Garber, Hon. Barry L., United States Magistrate Judge

Gold, Hon. Alan S., United States District Judge

Golembe, Stephen J., Co-Defendant Counsel

Kayanan, Maria, Counsel for *Amici Curiae* ACLU Foundation, et al.

Keisler, Peter, Counsel for AT&T Mobility, LLC

Klinger, Richard, Counsel for AT&T Mobility, LLC

Korchin, Paul M., Assistant Federal Public Defender

Lenard, Hon. Joan A., United States District Judge

Malone, Omar, Co-Defendant Counsel

Markus, David Oscar, Counsel for Nat'l Ass'n of Criminal Defense Lawyers

Martin, Michael, Co-Defendant

Martin, Jahmal A., Co-Defendant

McAliley, Hon. Chris M., United States Magistrate Judge

Michaels, Alexander J., Co-Defendant Counsel

Montgomery, Suzanne L., Counsel for AT&T Mobility, LLC

Moss, Jr., Reginald A., Co-Defendant Counsel

United States v. Quartavious Davis
No. 12-12928

National Association of Criminal Defense Lawyers, *Amicus Curiae*

Nojeim, Greg, Counsel for Center for Democracy & Technology

O'Sullivan, Hon. John J., United States Magistrate Judge

Palermo, Hon. Peter R., United States Magistrate Judge

Perwin, Amanda, Assistant United States Attorney

Quencer, Kevin S., Assistant United States Attorney

Reid, Jamarquis T., Co-Defendant

Salyer, Kathleen M., Chief, Appellate Division

Schultz, Anne R., Assistant United States Attorney

Shapiro, Jacqueline E., Appellate Counsel

Sibila, Jorge A., Co-Defendant Counsel

Smith, Willie, Co-Defendant

Torres, Hon. Edwin G., United States Magistrate Judge

Turnoff, Hon. William C., United States Magistrate Judge

Ungaro, Hon. Ursula, United States District Judge

Wessler, Nathan Freed, Counsel for *Amici Curiae* ACLU Foundation, et al.

White, Hon. Patrick A., United States Magistrate Judge

Wizner, Ben, Counsel for *Amici Curiae* ACLU Foundation, et al.

Williams, Hon. Kathleen M., United States District Judge

United States v. Quartavious Davis
No. 12-12928

Zelman, Michael, Trial Counsel

Corporate Disclosure Statement

Amicus Curiae AT&T Mobility, LLC is a wholly owned subsidiary of AT&T Inc., a publicly traded company. No publicly held corporation owns 10% or more of AT&T Inc. stock.

DATE: November 17, 2014

/s/ Peter D. Keisler
PETER D. KEISLER

TABLE OF CONTENTS

TABLE OF CITATIONS

Page(s)

CASES

STATUTES, REGULATION, AND RULE

OTHER AUTHORITIES

STATEMENT OF THE ISSUES

1) Whether the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B), (d), is unconstitutional under the Fourth Amendment insofar as it authorizes the government to acquire records showing historical cell site location information from a telephone service provider?

2) On the facts of this case, whether the government acquisition, pursuant to an order authorized by the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B), (d), of cellular telephone records showing historical cell site location information from a telephone service provider constitutes an unreasonable search or seizure in violation of Davis's constitutional rights under the Fourth Amendment?

INTEREST OF *AMICUS CURIAE*[1]

Amicus Curiae AT&T Mobility LLC (together with its affiliates, "AT&T") operates one of the world's most extensive and advanced wireless communications networks, providing state of the art data and voice services to more than 116 million users of mobile devices in the United States alone. AT&T's wireless networks provide customers with access to the Internet and a range of video, voice, data, and other services. As mobile services have become increasingly central to individuals' work and personal lives, providing mobile communications services has become an increasingly important focus of AT&T's business.

As is the case with many other technology companies in different sectors of the economy, AT&T receives and responds to an enormous volume of official demands to provide information to federal, state, and local law enforcement agencies in the United States. These demands may be made through search warrants, court orders issued on demonstrations of probable cause, court orders based on showings of less than probable cause, and subpoenas. Government officials seek a range of information, including the type of personal location information at issue here. In response, AT&T complies with applicable laws, including the Stored Communications Act provisions at issue in this case, and has

[1] Pursuant to Fed. R. App. P. 29(5), counsel for *amicus curiae* states that no counsel for a party authored this brief in whole or in part and no person other than *amicus curiae*, its members, or its counsel made a monetary contribution to its preparation or submission.

established a National Subpoena and Court Order Compliance Center. That Compliance Center operates on a continuous basis and is responsible for responding to and implementing judicial orders and subpoenas, employing more than 100 full-time employees. For the first six months of 2014, AT&T processed nearly 116,000 demands for various types of information from the government and private parties related to civil and criminal matters throughout the United States.[2]

In addition to seeking to accommodate the legitimate needs of the law enforcement community, AT&T also seeks to protect its customers' privacy and safeguard their personal information. AT&T values privacy as an essential personal right and protects privacy as a crucial element of its services. Customers value the privacy of their personal information, and protection of personal privacy informs customers' selection of service providers and their ongoing choice of whether to continue to do business with their service provider, whether that provider is AT&T or a competitor.

Considerable legal uncertainty currently surrounds the compelled production of location information. That uncertainty threatens to undermine both law enforcement and privacy interests and creates administrative difficulties and uncertainty for parties such as AT&T that are subject to orders to compel

[2] AT&T Transparency Report, *available at* http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html (last visited Nov. 13, 2014).

production of that information. The arguments that follow seek to assist the Court in creating clear and categorical legal rules that accord with the technology and consumer practices related to location information and that take into account both the privacy and the law enforcement interests implicated by such information.

SUMMARY OF ARGUMENT

This case concerns one of the many forms of personal location information generated in the digital economy. The government orders at issue – and tens of thousands like them annually – seek detailed records that can reveal the location and movements of the user of a particular mobile device, often over a relatively lengthy period. In many cases, the government can use that information to track the ongoing movements of particular targeted individuals, building a detailed understanding of the target's patterns of behavior and social and professional contacts and activities. Network, application, and other technological developments are making that location information ever more detailed and precise.

Considerable legal uncertainty surrounds the standards the government must satisfy to compel the production of location information, and achieving legal clarity is essential to protecting consumer privacy, defining the scope of legitimate law enforcement interests, and ensuring the efficient operation of companies operating in various sectors of the digital economy. On the one hand, courts increasingly recognize and protect privacy interests in personal location

information in contexts closely related to those presented here. In two recent decisions of the U.S. Supreme Court, members of that Court have described how personal location information, including information derived from mobile devices, implicates significant privacy interests. *See Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012). Those cases arose in contexts analogous in many respects to the practices at issue here, involving technology that determines the locations and movements of an individual, using data that may involve little or no action by the individual. On the other hand, the government asserts that the Stored Communications Act and older, "third party records" cases, *see Smith v. Maryland*, 442 U.S. 735, 741-42 (1979); *United States v. Miller*, 425 U.S. 435, 440 (1976), provide it with authority to require the production of location information under a standard of less than probable cause.

However the scope of the Fourth Amendment's protection is resolved, a clear and categorical rule will benefit all parties involved in the application of Section 2703(d), including the technology companies subject to orders to produce information. Whatever standard the Court ultimately determines the government must satisfy, the third party records cases may provide an unsatisfactory basis for resolving this case. *Smith* and *Miller* rested on the implications of a customer's knowing, affirmative provision of information to a third party and involved less extensive intrusions on personal privacy. Their rationales apply poorly to how

individuals interact with one another and with information using modern digital devices. In particular, nothing in those decisions contemplated, much less required, a legal regime that forces individuals to choose between maintaining their privacy and participating in the emerging social, political, and economic world facilitated by the use of today's mobile devices or other location based services.

Also at issue is the scope of Section 2703(d) of the Stored Communications Act, which is likewise the source of considerable legal uncertainty. For example, a significant question exists whether Section 2703(d) even applies to the production of historical cell site location information ("CSLI"), and the provision even more clearly does not apply to orders seeking prospective, real-time CSLI. But in all events, the section need not present any issue of the statute's constitutionality. That is because, where Section 2703(d) applies, it does not necessarily authorize the government to secure information under the lower, "reasonable grounds" standard, but is instead flexible enough to require the government to meet the Warrant Clause's probable cause standard where that result is justified by the nature of the information at issue. Finally, regardless of whether the Court determines that a "reasonable grounds" standard or a probable cause standard applies in this case, it should set forth a categorical rule that can be applied in all cases where the government seeks to compel the production of historical CSLI.

ARGUMENT

I. CONSIDERABLE LEGAL UNCERTAINTY SURROUNDS THE STANDARDS APPLICABLE TO GOVERNMENT EFFORTS TO COMPEL THE PRODUCTION OF LOCATION INFORMATION.

A. The Government Seeks Different Types of Location Information, Including Historical CSLI, That Often Implicate Significant Privacy Interests.

While this case involves historical location records generated by a wireless network, it is important to understand the broader context of location-based services in a digital world. Health tracking devices, vehicle navigation systems, applications on tablets and smartphones, and any number of other services and devices have the capability to collect, transmit, and store location information. This location information may be stored by service providers ranging from small tech start-ups to large multi-service technology service providers like Google. Government requests for this information implicate privacy interests that vary depending on the scope of the information requested and the technology involved. For example, the historical CSLI at issue in this case is but one type of location information generated by wireless telecommunications networks and sought by the government, and any rule addressing that type of information needs to be carefully crafted to ensure that it does not inadvertently address different information presenting different law enforcement, privacy, and technological concerns.

Location information is generated by the normal operation of wireless telecommunication networks in a range of ways. Mobile devices, including but not limited to cell phones, communicate periodically with towers that serve a surrounding area, or "cell." Those towers, in turn, receive and send data and voice communications through the wireline telecommunications network, connecting the device user to other users, various data and information sources, and the Internet. The device usually – but not always – communicates with the nearest cell tower. As the user of the device moves from one area to another, the connection to the wireless network may be handed off from cell tower to cell tower. At the most basic level, the wireless network needs to determine the location of the mobile device in order to send and receive communications to and from that device.

Certain of the communications between mobile devices and the wireless network generate records of the user's location. CSLI for a given communication may identify the particular cell tower the device is using at that time, as well as the direction of the signal from the tower and other data concerning the transmission between the device and the tower. CSLI thus often indicates that the user is located within the particular cell served by a specified tower and, based on the direction and signal information, within a particular sector of the cell. CSLI may also reflect a user's movements over time by identifying each of the various towers

engaged as the user moves across multiple cells during and between communications.

CSLI is often generated based on voice and data communications initiated or received by the targeted device. This includes, for example, the periodic messages sent or received related to email or texting and other data transmissions, including those generated by the mobile device's operating system or applications on the mobile device. CSLI may reflect attempted but uncompleted calls from third parties, as well as completed voice calls initiated or received by the device user. Wireless network operators often use this information for a range of diagnostic functions and to improve the deployment, operation, and quality of their networks. For example, CSLI showing an unusually large number of call terminations and initiations in a specific location may indicate that a provider needs to address a dead spot or gap in coverage.

The precision of this location information varies according to the array of the towers and technology employed. As the density of the cell towers increases (decreasing the area covered by any particular tower), the precision of the CSLI increases correspondingly. Rural or sparsely populated areas generally have fewer cell towers, each serving a larger territory. In more densely populated areas, towers are much closer together and serve smaller areas, generating more specific location information. As customers demand more bandwidth to support

smartphones, video services, and other high-volume Internet access, service providers are increasing the density of cell towers, further shrinking the size of particular cells. Service providers are also increasingly boosting their network coverage through small cells known as "microcells" or "femtocells" that may cover an area as small as a single floor of a building or an individual house.

Cellular communications technology may also generate other, more precise forms of location information. For example, some mobile devices, such as smartphones, are equipped with GPS technology which determines the device's exact location based on signals received by the phone from a network of satellites. In addition, because mobile devices are often in contact with more than one cell tower at a time, it is often possible to locate the device through triangulation – *i.e.*, determining the point of overlap among the areas covered by each of the multiple towers within range of a particular device.[3]

The government frequently seeks to compel the production of various types of location data for law enforcement purposes from a range of technology

[3] Other means to locate a mobile device exist in addition to – and to some extent overlapping with – CSLI, GPS, and triangulation data. For example, information about the cell tower and signal direction can be coupled with "timing advance" data (*i.e.*, information about how long it takes the signal from the mobile device to reach the cell tower) to calculate location more precisely. In addition, a method known as "Assisted GPS" involves sending to the mobile device a file of data that can help the device's GPS chip more quickly identify the most appropriate satellite to establish the device's location.

companies. Often, the government seeks information about the location of targeted devices to track the device user.[4] Orders sought by the government frequently take one of the following three forms.

1. Mobile Locate Orders. "Mobile locate" requests seek the most precise location information for a particular mobile device that is technically feasible at the time of the request. Often, that information is in the form of GPS coordinates (if the target device is enabled with GPS capability) or based on triangulating data from multiple cell towers. In some instances, however, the most precise location information for a particular phone at a particular time would be CSLI (and the responsive information would therefore take that form).

Privacy concerns are especially acute when the government obtains orders requiring the production of this detailed mobile location data. In AT&T's experience, the government, when seeking to secure mobile locate orders, always makes a probable cause showing and does not request Section 2703(d) orders based on the lower, "reasonable grounds" showing for this information.

2. Prospective CSLI. The government frequently seeks orders pursuant to Section 2703(d) to compel the production of "prospective CSLI" – location

[4] *See, e.g., In re Application of the U.S. for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers*, 416 F. Supp. 2d 390, 396 n.9 (D. Md. 2006) ("[T]he government only wants this information so it can track the suspect's movement via his cell phones.").

information that will only come into existence *following* the issuance of the order and thus is not "stored" at the time the demand is served. Government requests for prospective CSLI may cover days, weeks, or even months. The telecommunications service provider arranges to provide this information through an electronic delivery mechanism that provides nearly real-time location information to the government. Prospective CSLI thus may enable the government, over time, to construct the user's patterns of movement and behavior, to track the user contemporaneously, and even to anticipate where the user will soon be. For example, the government has used prospective CSLI to track down and apprehend specific targeted individuals.

Especially in conjunction with orders for prospective CSLI, the government often also seeks orders pursuant to the Pen Register Act to install pen register and trap and trace devices, which capture the numbers dialed by the targeted user and the numbers of devices used to place incoming calls to the target. In addition, these orders also provide the government with location information generated as the targeted mobile device repeatedly "checks in" or registers with the mobile network, providing further, general information about the user's location. That registration data is not always stored by the service provider (and thus is normally provided only with prospective CSLI, not with historical CSLI).

3. Historical CSLI. Finally, the government also seeks orders pursuant to Section 2703(d) for historical CSLI, the type of information at issue in this case. Although the government at times erroneously uses the term "historical" CSLI to include a range of records that may not come into existence until moments before the carrier transmits the location information to the government (*i.e.*, prospective CSLI), the term as used here describes only records already in existence when the government secures the Section 2703(d) order. That is, the demand is retrospective compared to demands seeking records prospectively.

These orders for historical CSLI typically require production of records reflecting the use of a particular mobile device, identified by its phone number, for days, weeks, or months (in this case, 67 days). The information includes the cell tower and tower face used by the device when it communicates with a cell tower, generating location information indicating the user's patterns of movement over a significant period of time. The records can reveal where a user was or is likely to be at a particular time of day or night. For example, the government has used such information to argue, as it did in this case, that an individual was at the scene of one or multiple crimes or travelled along a route known to have been used in committing a charged offense. Such records could be used to extrapolate the individual's location, including at home, work, church, or other private places.

B. Recent, Leading Cases Have Increasingly Recognized the Privacy Interests Affected by the Compelled Production of Long-Term Location Information.

Recent, leading cases have increasingly recognized that some types of location information, in certain circumstances, implicate significant privacy interests traditionally protected by the probable cause standard of the Fourth Amendment's Warrant Clause. At the same time, the government continues its practice of seeking orders compelling the production of such location and related personal information under a relatively low, "reasonable grounds" standard set out in Section 2703(d). Which standard applies to which categories of personal information is a source of increasing, and increasingly important, legal uncertainty that affects the operation of many technology companies that hold information sought by the government.

With respect to at least the "mobile locate" information described above, the government acknowledges the significance of the privacy interests at issue by consistently applying and satisfying the warrant standard when it secures orders to produce that information. The government does not normally do so for historical and prospective CSLI, even though those types of information are similar in important respects to the location information secured through "mobile locate" orders and based on GPS systems or triangulation. *See supra* pp. 8-13. The principal difference between mobile locate information and CSLI relates to the

precision of the revealed location, but that difference is narrowing as carriers accelerate their use of small-cell technologies and add towers to expand capacity.

Historical CSLI and prospective CSLI are thus increasingly implicating privacy concerns similar to those addressed in somewhat different contexts in two recent Supreme Court cases. In *Riley v. California*, concerns surrounding mobile device location information formed a principal basis for the Supreme Court's conclusion that the government must meet the warrant standard before it may search a mobile device incident to an arrest. The Court emphasized that "[d]ata on a cell phone can also reveal where a person has been" and cautioned that "[h]istoric location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." 134 S. Ct. at 2490.

United States v. Jones addressed the implications of long-term location monitoring, which is often at issue in government orders seeking historical CSLI or prospective CSLI. The decision rested directly on a trespass theory in concluding that officials must secure a warrant before installing and monitoring a GPS tracking device on a person's automobile, 132 S. Ct. at 950-51, but five Justices concurred to indicate that prolonged location tracking itself implicates such significant privacy interests that it amounts to a search under the Fourth Amendment that requires a warrant, *id.* at 964 (Alito, J., concurring); *id.* at 955

(Sotomayor, J., concurring). Writing for himself and three other Justices, Justice Alito concluded that "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" and that a criminal suspect's "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id.* at 958, 964. Justice Alito identified the proliferation of mobile devices as "[p]erhaps [the] most significant" of the emerging location tracking technologies. *Id.* at 963; *see also id.* (noting the prevalence of "cell phones and other wireless devices" that "permit wireless carriers to track and record the location of users"). Justice Sotomayor separately observed that "GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" *Id.* at 956. All five Justices agreed that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Id.* at 955 (quoting Justice Alito's concurrence, *id.* at 964).

Although greater precision is associated with GPS location information, similar observations may apply to the long-term location monitoring enabled by

historical and prospective CSLI. CSLI at times may provide more sensitive and extensive personal information than the car tracking information at issue in *Jones*. Users typically keep their mobile devices with them during the entire day, potentially providing a much more extensive and continuous record of an individual's movements and living patterns than that provided by tracking a vehicle; CSLI, therefore, is not limited to the largely public road system or to when the device user is in a vehicle. That difference, in turn, may enable officials to use historical and prospective CSLI to construct a more detailed and intimate portrayal of the targeted person's daily habits and work and leisure routines – including activities related to the home. *Cf. Kyllo v. United States*, 533 U.S. 27 (2001) (warrant required for thermal imaging of home conducted from public space); *Payton v. New York*, 445 U.S. 573, 586 (1980) ("It is a 'basic principle of Fourth Amendment law' that searches and seizures inside a home without a warrant are presumptively unreasonable.").

C. The Supreme Court's "Third Party Records" Cases May Not Provide an Appropriate Basis for Resolving the Current Legal Uncertainty in This Context.

Even as recent decisions heighten the legal uncertainty surrounding the standard for compelling production of personal location information, the increasing importance and changing uses of mobile devices undermine an important rationale

for the government's efforts to use a relatively permissive standard to compel the production of historical and prospective CSLI.

In support of the government's efforts to compel the production of CSLI upon a showing of less than probable cause, the government has traditionally invoked cases establishing the "third party records" doctrine. *See Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976). However, important factors that led the Supreme Court not to apply the warrant standard in those cases are absent in this context. Although *Jones* and *Riley* did not overrule *Smith* and *Miller*, their identification of privacy interests related to location information point to why those older cases may not be controlling here.

Smith and *Miller* focused on the Fourth Amendment implications of a person's knowing, affirmative acts necessary to undertake discrete commercial transactions that create particular records held by third parties and later sought by the government. In *Miller*, the Supreme Court concluded that an individual had no reasonable expectation of privacy in banking records such as checks, deposit slips, and monthly statements because these documents were "the business records of the banks," which were "'parties to the [negotiable] instruments with a substantial stake in their continued availability and acceptance.'" 425 U.S. at 440. In that context, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id*. at 443. In

Smith, the Supreme Court held that an individual has no reasonable expectation of privacy in dialed phone numbers captured by a pen register. The Court emphasized the "limited capabilities" of pen registers, which "do not acquire the *contents* of communications" and do not disclose "the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed." 442 U.S. at 741-42. Telephone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." *Id.* at 743.

The privacy and related social interests implicated by the use of modern mobile devices and by CSLI are fundamentally different and more significant than those evaluated in *Miller* and *Smith*. *Miller*, 425 U.S. at 443 ("We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents"); *Smith*, 442 U.S. at 741-42 (emphasizing the "limited capabilities" of pen registers). Use of mobile devices, as well as other devices or location based services, has become integral to most individuals' participation in the new digital economy: those devices are a nearly ever-present feature of their most basic social, political, economic, and personal relationships. In recent years, this has become especially

true of the data communications – from email and texting to video to social media connections – that occur on a nearly continuous basis whenever mobile devices are turned on.

The ongoing digital recording and storage of location information that can reveal the pattern of the user's movement amount to much more than a record reflecting discrete transactions, equivalent to the deposit slip or dialed digits records at issue in *Miller* and *Smith*. *Miller* and especially *Smith* rested on the absence of any true sacrifice of privacy interests, and none beyond the affirmative, discrete commercial transactions at issue – but that hardly describes either the privacy interests implicated by location information, *see supra* pp. 14-17, or how that information is generated, *see supra* pp. 8-10. *Cf. United States v. Warshak*, 631 F.3d 266, 287-88 (6th Cir. 2010) (distinguishing *Miller* and holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of 'emails that are stored with, or sent or received through, a commercial ISP'"); *see also In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 120-26 (E.D.N.Y. 2011) ("[C]umulative cell-site-location records implicate sufficiently serious protected privacy concerns that an exception to the third-party-disclosure doctrine should apply to them, as it does to content…."). Nothing in *Smith* or *Miller* requires that individuals must choose

between participating in the new digital world through use of their mobile devices and retaining the Fourth Amendment's protections.

Nor does *Miller* or *Smith* address how individuals interact with one another and with different data and media using mobile devices in this digital age. Location enabled services of all types provide a range of information to their users. At the same time, mobile applications, vehicle navigation systems, mobile devices, or wireless services for mobile devices often collect and use data in the background. A mobile application may send or receive an update in the background, triggering a location data point stored in the device or sent to the application provider or the mobile service provider. When placing a call, a cell phone user affirmatively dials the digits of the phone number to be called, but does not affirmatively enter the device's location coordinates. That location is nonetheless captured by the service provider. *See also supra* p. 9. Even for voice communications, the device location may be recorded when the mobile device receives a call, even an uncompleted call, but the user's role is wholly passive. *See In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 317-18 (3d Cir. 2010) ("[W]hen a cell phone user receives a call, he hasn't voluntarily exposed anything

at all.") (internal quotation marks omitted).[5] The ongoing, multi-channel, multi-party, two-way data and voice communications that are the hallmarks of individuals' participation in the digital social and economic world bear little resemblance to the discrete, affirmative acts at issue in *Miller* and *Smith*.

For all these reasons, *Miller* and *Smith* may not provide the guidance needed or relevant to resolving the legal uncertainty surrounding the compelled production of personal location information in this context.

II. TO THE EXTENT SECTION 2703(d) EXTENDS TO HISTORICAL CSLI, IT DOES NOT REQUIRE THAT SUCH ORDERS BE ISSUED UPON A LOWER, "REASONABLE GROUNDS" SHOWING AND SHOULD BE APPLIED ON A CATEGORICAL BASIS.

The questions posed by the Court in its scheduling order, relating to whether Section 2703(d) is "unconstitutional … insofar as it authorizes the government to acquire records showing historical [CSLI] …" and whether the order at issue here was lawful, raise three underlying issues of statutory construction. First, does Section 2703(d) even authorize the compelled production of CSLI? Second, even if the statute provides that authority, does Section 2703(d) always permit the government to secure whatever information it seeks using a "reasonable grounds" standard or does it in some circumstances require the government to make a

[5] Indeed, the government will sometimes initiate a call to a target and then disconnect before the call is answered, simply to generate such location information. *See, e.g., United States v. Forest*, 355 F.3d 942, 947 (6th Cir. 2004), judgment vacated, 543 U.S. 1100 (2005).

probable cause showing sufficient to support a warrant? And, third, should the showing required of the government by Section 2703(d) to obtain historical CSLI be applied on a case-by-case basis or categorically? The following discussion describes why the statute does not clearly provide for the production of historical CSLI (and does not provide for the production of prospective CSLI), why the statute is flexible enough to require a probable cause showing where the information at issue justifies that standard, and why, whatever standard the Court determines applies to historical CSLI, a categorical rather than case-by-case application of that standard under Section 2703(d) is appropriate.

A. Whether Section 2703(d) Even Supports The Government's Efforts to Require Production of Historical CSLI Presents a Significant Question.

As Justice Alito's concurrence in *Jones* observed, a mobile device functions as the ultimate tracking device, 132 S. Ct. at 963, and the government seeks to compel production of CSLI for just that reason. But Congress, through a statutory regime separate from Section 2703(d), has already provided for how the government may secure such tracking location information – and that requires a probable cause showing. Congress defined "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117. The government's use of CSLI for tracking purposes turns a mobile device into just such a tracking device. That, in turn, subjects

government requests for such tracking information to Federal Rule of Criminal Procedure 41's tracking device warrant requirements. *See* Fed. R. Crim. P. 41(a)(2)(E) (adopting Section 3117's definition of "tracking device"); *id.* 41(d), (e)(2)(C), (f)(2) (addressing tracking device warrants); *see also, e.g.*, *In re Application of the U.S. for an Order Authorizing Prospective & Continuous Release of Cell Site Location* Records, No. H:13-1198M, 2014 WL 3513120 (S.D. Tex. July 15, 2014) ("*S.D. Tex. 2014 opinion*") (applying tracking device definition to CSLI and rejecting court decisions that have found that mobile devices are not tracking devices); *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info.*, 396 F. Supp. 2d 294, 321-22 (E.D.N.Y. 2005).

Section 2703(d)'s inapplicability to CSLI is especially clear for prospective CSLI – and the Court should carefully distinguish between historical CSLI and prospective CSLI for this and other purposes. In the context of prospective CSLI, the mobile device even more clearly functions as a tracking device (permitting the government to follow the target's movements nearly as they occur), and Section 2703(d) of the *Stored* Communications Act, by contrast, is designed to permit the government to secure pre-existing records rather than "records" that have not yet even come into existence. Section 2703 governs disclosure of "a record or other

information pertaining to a subscriber to or customer of" a relevant service. 18 U.S.C. § 2703(c). The word "record" addresses information that has already been created or "record[ed]." Moreover, the provision authorizes the government to require a provider "to *disclose* a record or other information," not to create a record or obtain information, and one cannot normally disclose something that one does not yet possess.[6]

Furthermore, Section 2703 bears none of the hallmarks that characterize the processes Congress has established for ongoing collection of prospective communications information. *See, e.g., S.D. Tex. 2014 opinion*, 2014 WL 3513120. Congress limited such ongoing information collection by setting time limits on collection, requiring renewal of the order to extend the time limits, mandating annual reporting to Congress, requiring efforts to minimize the amount of non-targeted communications intercepted, and directing that collection orders be sealed. *See* 18 U.S.C. §§ 2518(5), 2519, 3123(c), 3123(d), 3126. Similarly, Federal Rule of Criminal Procedure 41 sets time limits on warrants for use of a tracking device, as defined in 18 U.S.C. § 3117. Fed. R. Crim. P. 41(e)(2)(C). The

[6] Likewise, subsection 2703(b) addresses disclosure of the contents of a communication "held or maintained," similarly indicating that the communication has already been made at the time of the order. 18 U.S.C. § 2703(b). In addition, subsection 2703(a) addresses disclosure of the contents of communications "in electronic storage" and applies different standards for disclosure of communications that have been in storage for 180 days or less. *Id*. § 2703(a).

omission of these types of safeguards from Section 2703(d) confirms that Congress did not intend that provision to authorize the ongoing, real-time collection and production of CSLI.

B. The Statute Is Best Construed to Require the Government to Satisfy the Probable Cause Standard When Merited by the Privacy Interests At Issue.

Whether this Court concludes that a probable cause standard or a "reasonable grounds" standard applies in this particular case, another issue of statutory construction is whether Section 2703(d) permits the higher standard to be applied to information within its scope. The better view is that it does.

Section 2703(d) provides that a "court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if" the government provides "reasonable grounds" linking the records to a criminal investigation. The government has argued that it may always secure an order under Section 2703(d) upon a "reasonable grounds" showing, but that position has been rejected by the Third Circuit, a dissenting Fifth Circuit judge, and numerous magistrate judges. Appropriately, they construe Section 2703(d) as setting a minimum standard the government must always satisfy and requiring that the government satisfy the Warrant Clause's probable cause standard before issuing an order requiring production of information implicating significant privacy interests. *See* 18 U.S.C. § 2703(c)(1)(A). As discussed below, *infra* pp.

27-28, this more flexible approach could be applied by magistrate judges on a case-by-case basis or, more aptly, used categorically to require a specific standard (whether probable cause or something else) for all requests for historical CSLI. *See infra* pp. 28-30.

As the Third Circuit emphasized, the statutory phrase "may issue" is "the language of permission, rather than mandate" and "strongly implies court discretion, an implication bolstered by the subsequent use of the phrase 'only if' in the same sentence." *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 315; *id*. at 315-16 (summarizing cases adopting this reasoning). In addition, the government's construction would render the word "only" superfluous. *Id*. at 316. For those reasons, the Third Circuit accepted the argument that "the requirements of Section 2703(d) merely provide a floor" and held that "the statute … gives the [magistrate judge] the option to require a warrant showing probable cause" where the government's request for information implicates significant privacy interests. *Id.* at 315, 319. For similar reasons, Judge Dennis disagreed with his Fifth Circuit colleagues who concluded that Section 2703(d) was less flexible. *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 615-632 (5th Cir. 2013) (Dennis, J. dissenting).

This issue of statutory construction is important for how the Court answers the first question posed in its scheduling order. Under the broader construction of Section 2703(d), this case presents no issue of Section 2703(d)'s constitutionality: Section 2703 is flexible enough to require the government to meet the Warrant Clause's probable clause standard when required by the Fourth Amendment or otherwise, and provides a lesser standard when the government's request does not implicate that higher degree of privacy interests. In that view, Congress did not categorically dictate the constitutional protections appropriate for the different types of information the government might seek and instead assumed that the courts would apply the Fourth Amendment as appropriate. Only if the Court adopts the Fifth Circuit's inflexible approach is there any potential constitutional clash between the branches. The benefit of avoiding this constitutional conflict, and the implausibility of the view that Congress purported to determine categorically what information the Fourth Amendment would protect, further support adopting the more flexible construction of Section 2703(d).

C. If Section 2703(d) is Found to Extend to Historical CSLI, the Relevant Standard Should Apply Categorically to Historical CSLI.

If the Court concludes that Section 2703(d) supports orders compelling the production of historical CSLI and authorizes magistrate judges to apply the legal standard appropriate to whatever type of information is requested, a further issue is

whether magistrate judges are to apply one applicable standard to government requests for historical CSLI on a categorical basis or are to determine the applicable standard on a case-by-case basis. This issue arises whether the Court concludes that the government need only have established "reasonable grounds" to secure the order at issue in this case or concludes that a probable cause showing was necessary – either as a matter of the Fourth Amendment directly or based on the doctrine of constitutional avoidance. *See, e.g.*, *Clark v. Martinez*, 543 U.S. 371, 381 (2005); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 632 (Dennis, J., dissenting) (doctrine of constitutional avoidance requires a probable cause showing for orders to compel production of historical CSLI).

Privacy, law enforcement, and administrative interests would be better furthered by a categorical rule rather than a case-by-case approach. Given the overwhelming volume of governmental requests for long-term CSLI, a case-by-case approach would be unworkable and administratively difficult for service providers, law enforcement officials, and magistrate judges. As described above, *supra* p. 11, the government already consistently obtains warrants under a probable cause standard for orders seeking mobile locate information. Requiring a consistent standard for an additional category of location information (long-term historical CSLI) would avoid the significant uncertainty inherent in assessing individual cases because it cannot be known in advance exactly what CSLI will

reveal. When the order to produce long-term CSLI is entered, it will be unknown whether the mobile device user's location will be identified with the high level of precision available through small cells or dense cell tower coverage, or with less revealing, sparsely distributed towers. Whether the records will, in each instance, track home residence use or reveal other personal behaviors will also be unknown. Requiring a particular level of showing by the government for all orders seeking this entire category of information would provide clear rules for law enforcement officials, magistrate judges, and the service providers that seek to ensure that their actions satisfy both legitimate privacy concerns and legitimate law enforcement interests.

CONCLUSION

For the foregoing reasons, this Court should distinguish carefully among the different type of information that the government may seek pursuant to a Section 2703(d) order (especially between historical CSLI and prospective CSLI), consider whether Section 2703(d) even applies to the historical CSLI at issue in this case, avoid construing Section 2703(d) as always requiring the government to make only a "reasonable grounds" showing to secure information within the provision's scope, and use a categorical approach to resolve the uncertainty regarding the showing required of the government to secure an order compelling the production of historical CSLI.

Respectfully submitted,

Dated: November 17, 2014

/s/ Peter D. Keisler

SUZANNE L. MONTGOMERY
ALTRESHA Q. BURCHETT-WILLIAMS
AT&T SERVICES, INC.
208 S. Akard St., Suite 500
Dallas, Texas 75202
Telephone: (214) 757-3389
Facsimile: (214) 446-6408

PETER D. KEISLER
RICHARD KLINGLER
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: (202) 736-8000
Facsimile: (202) 736-8711

Counsel for Amicus Curiae AT&T Mobility, LLC

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitations of Federal Rule of Appellate Procedure 32(a)(7)(B) and the Rules of this Court, because it contains 6,811 words as determined by the Microsoft 2007 word-processing system used to prepare the brief, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using the Microsoft Word 2007 word-processing system in 14-point Times New Roman font.

/s/ Peter D. Keisler
PETER D. KEISLER

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of November, 2014, I electronically filed the foregoing through the Court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system. I further certify that the original and 19 copies of the foregoing were delivered to the Court by courier and that I caused the foregoing to be transmitted via electronic mail to the individuals listed below.

/s/ Peter D. Keisler
PETER D. KEISLER

Amit Agarwal
Assistant United States Attorney
99 N.E. 4th Street
Miami, Florida 33132-2111

Jacqueline E. Shapiro
Attorney for Appellant
40 N.W. 3rd Street, PH 1
Miami, Florida 33128