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 REPLY 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

TABLE OF CONTENTS

TABLE OF CITATIONS

CASES:

STATUTORY AND OTHER AUTHORITY:

REPLY ARGUMENT

The government extrapolates from relatively minor, long-accepted intrusions on privacy expectations a tenuous thesis for tracking virtually everyone in this country based on a prosecutor's assertions of evidentiary need. The government's inapt analogies offer little more than a slippery slope for erosion of privacy rights. Thus, the "*obsta principiis*" motto of the Supreme Court in *Boyd v. United States*, 116 U.S. 616, 635, 6 S.Ct. 524, 535 (1886)—urging courts to stop new privacy intrusions in their tracks—remains as valid today as ever: "It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon. Their motto should be *obsta principiis*."

1. The third-party doctrine did not remove MetroPCS's production of records to the government from the category of a search under the Fourth Amendment.

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 the government's rationale to use a relatively permissive standard to compel production of historical cell site location information (CSLI). The "third party records" doctrine, as applied in *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577 (1979); *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619 (1976), 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, 96 S.Ct. at 1623. 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, 96 S.Ct. at 1624. 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, 99 S.Ct. at 2581. 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, 99 S.Ct. at 2581.

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, 96 S.Ct. at 1623 ("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, 99 S.Ct. at 2581 (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. And these media have significant political importance and have been cited as means to break through walls of control created by authoritarian governments.

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 or how that information is generated. *See 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-sitelocation 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.

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). The ongoing, multi-channel, multiparty, 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* do not provide the guidance needed to excuse the government from the warrant requirement for *ex parte* seizure of personal location information in this context.

In *Riley v. California*, the Supreme Court "reject[ed]" the government's suggestion that the *Smith* third-party doctrine justified the search of cell phone data.

134 S.Ct. 2473, 2014 (2014). The analytical themes advanced by the Supreme Court in *Riley* counsel that this Court should likewise reject the government's suggestion that *Smith* eliminates Fourth Amendment protection in this case. In *Riley*, the Supreme Court seized the opportunity to explain that the pen register in *Smith* bore little relationship to the phone data mined by the government. Regarding an old-fashioned flip phone, the Court noted that a cell phone's call log (and thus its metadata) "contained more than just phone numbers" and included substantial personal identifiers, rendering a case about pen registers of little utility in deciding the Fourth Amendment question. *Id.* at 2493. *Riley* essentially limited *Smith* to its facts and distinguished those facts from cell phone data. *See also Ontario v. Quon*, 560 U.S. 746, 760, 130 S.Ct. 2619, 2630 (2010) (assuming a privacy interest in text messages sent on a government owned phone); *Kyllo v. United States*, 533 U.S. 27, 120 S.Ct. 2038 (2001) (finding a privacy interest in location-related data, although partially observable to the public), *Ferguson v. City of Charleston*, 532 U.S. 67, 121 S.Ct. 1281 (2001) (finding a privacy interest in the result of medical information, despite the fact that the individuals disclosed the information to hospital personnel); *Bond v. United States*, 529 U.S. 334, 336, 120 S.Ct. 1462, 1464 (2000) (exposing a bag to the public does not eliminate an expectation of privacy). *See also U.S. Dept. of Justice v. Reporters Committee For Freedom of Press,* 489 U.S. 749, 763-64 n.14,

109 S.Ct. 1468, 1476-147 n.14 (1989)(since almost every highly personal fact is known to someone other than the person who enjoys the privacy interest, "'meaningful discussion of privacy, therefore, requires the recognition that ordinarily we deal not with an interest in total nondisclosure but with an interest in selective disclosure.'")(quoting Karst, "The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data, 31 Law & Contemp. Prob. 342, 343-344 (1966)).

Riley's discussion of the privacy interest encompassed by data kept on a business's server, not just data maintained on the device itself, demonstrates that the government cannot evade the warrant requirement based on a claim that CSLI is a business record. When a trusted agent—the cell phone company—obtains personal data as part of its provision of essential service, and is then required by law to maintain the data, such data does not fall within the third-party exception to privacy rights. Cell phone users retain a reasonable expectation of privacy in data housed on a business's servers. Cell phone users do not necessarily know what data resides on the device and what data is stored in the cloud "and it generally makes no difference" to the privacy interest. *Id.* at 2491. Even if data is actually located on a business's server, individuals retain a privacy interest; it is still the individual's "effects" despite being stored remotely on a computer owned by a business. *Id.*

Cell phone users do not grant service providers the right to rummage through their personal data. Access to it does not transform the data into a business record instead of an individual's personal papers and effects. *See Warshak*, 631 F.3d at 286-88; *see also Stoner v. California*, 376 U.S. 483, 488-89, 84 S.Ct. 889, 892-93 (1969) (explaining that limited access to property does not include blanket authority to consent to search). The government also cannot claim that CSLI is a business record because the business has an independent interest in retaining historic CSLI. The excessive entanglement of law enforcement with telecommunications providers establishes that obtaining this information is a search. *See Ferguson*, 532 U.S. at 82-84, 121 S.Ct. 1290-91; *Klayman v. Obama*, 957 F. Supp. 2d 1, 33 (D. D.C. 2013). Because CSLI is essentially communications content stored like a bailment, the government can obtain CSLI from service providers only with a warrant. *See Warshak*, 631 F.3d at 286-87. A bailment is not transformed into a business record simply because of the storage location. *See Marvin v. United States*, 732 F.2d 669, 675–76 (8th Cir. 1984).

If this Court were to hold that cell phone tracking falls outside of the ambit of the Fourth Amendment, the Supreme Court's decision in *Jones,* 132 S.Ct. 945 (2012), would have little practical effect in safeguarding Americans from the pervasive

monitoring of their movements that so troubled a majority of the Justices. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J.); *id.* at 963-64 (Alito, J.).

2. Davis lost no privacy rights by using a nickname in purchasing phone service, rather than revealing his full legal name; a subjective expectation of privacy is not lost by an exercise in maintaining privacy, nor does an attempt to maintain privacy connote a teenager's understanding of CSLI laws or technological processes.

The government relies insistently on the particular facts of record in *United States v. Madison*, 2012 WL 3095357, at *8 (S.D. Fla. 2012), involving a defendant's manifestation of knowledge that communications companies regularly collect and maintain non-content information regarding cell-phone communications, including cell-site tower data. But there was no such evidence in this case. The government offers no surveys of public understanding of anything about how cell phones operate. A teenager's use of a nickname—particularly a fan-based nickname like "Lil Wayne"—is of no import to the momentous decision facing this Court. *See United States v. Finley*, 477 F.3d 250, 258-59 (5th Cir. 2007) (defendant had expectation of privacy to challenge search of cell phone where even though employer issued cell phone to defendant, defendant maintained a property interest in the phone, had a right to exclude others from using it and exhibited a subjective expectation of privacy in it, and took normal precautions to maintain his privacy in the phone). As in *Finley*,

this case does not involve the distinct issue of fraud on the phone service provider or any other forfeiture of the rights of a cell phone user.

3. Trial prosecutor's closing argument that Davis did not know of tracking.

The government seeks to retract an evidentiary inference that it relied on to convict the defendant. No one likes to be hoisted by their own petard. But facts are stubborn things. And this case—unlike *Madison*—lacks, by the government's own admission at trial, any case-based theory of waiver of privacy rights.

4. Even if though the data caused by his cell phone possession was not in his hands, Davis had a privacy interest through his use of the cell phone services.

Whatever standard the Court ultimately determines the government must satisfy, the third party records cases 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. "If times have

changed, ... the changes have made the values served by the Fourth Amendment more, not less, important." *Coolidge v. New Hampshire*, 403 U.S. 443, 455, 91 S.Ct. 2022, 2032 (1971); *see also United States v. Jones*, 132 S. Ct. 945 (2012). The government's argument that tracking people through untold thousands of location points implicates no privacy interest simply reprises the ways it defended warrantless wiretaps and thermal imaging in bygone eras. Indeed, its arguments are identical 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), and analogized (in the same overextensive manner as the government in the CSLI context) the defendant's using "a telephone instrument with connecting wires" to shouting in public, because the telephone signal went "beyond his house" and thus beyond "the protection of the Fourth Amendment."

5. Fourth Amendment would, of course, shield Davis from incriminating information in records MetroPCS turned if the records were deemed to derive from Davis's phone use.

Couch v. United States, 409 U.S. 322, 324, 335-36, 93 S.Ct. 611, 614, 619 (1973), holding that a person could not reasonably claim a Fourth Amendment expectation of privacy in records to which she "retained title" after she "surrendered possession of the records" to her accountant, is not an apt analogy. Davis did not

give his cell phone company any physical items; he was tracked by technology beyond his (and the undersigned's) understanding. Davis did not text the cell phone company to give them his location. In relation to the CSLI data, he was more like a *couch potato* than an active conveyor of physical items like the petitioner in *Couch*.

While "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed," *Miller*, 425 U.S. at 443, 96 S.Ct. at 1624, this rule does not apply to CSLI technological advances in constant tracking of everyone. There is nothing in the record that shows Davis voluntarily disclosed his location data to the company. At most, the record shows he did not even wish to share his actual name with the company, let alone where he was when he received or made calls. When a cell phone user makes or receives a call, there is no indication that making or receiving the call will also create a record of the caller's location. The user does not input her location information into the phone, and the phone does not notify the user that her location has been logged. Moreover, unlike the dialed phone numbers at issue in *Smith*, location information does not appear on a typical user's monthly bill. Further, many smartphones include a location privacy setting that, when enabled, prevents applications from accessing the phone's location.

However, this setting has no impact at all on carriers' ability to learn the cell tower in use, thus potentially misleading phone users. Cell-tower location information is automatically determined by the wireless provider, but is not actively, intentionally, or affirmatively disclosed by the caller. *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 at 318-19.

Moreover, any posited awareness by a cell phone user – unsupported by anything in the facts of record in this case – that his cell phone emits signals enabling his service provider "to detect its location for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes." *Tracey v. State*, __ So.3d __, 2014 WL 5285929, at *16 (Fla. Oct. 16, 2014). The Florida Supreme Court in *Tracey*, ruling that "cell phones are 'effects' as that term is used in the Fourth Amendment," further recognized that "requiring a cell phone user to turn off the cell phone just to assure privacy from governmental intrusion that can reveal a detailed and intimate picture of the user's life "places an unreasonable burden on the user to forego necessary use of his cell phone, a device now considered essential by much of the populace." *Id.* at ** 16, 18.

The government's suggestion that the MetroPCS privacy policy converts automatic, involuntary retention of location information into voluntary conveyance of such data is misplaced. There is nothing in the record as to the version of the privacy policy in effect when the government requested Davis's location records. Nor, in its current version as set forth by the government, does the policy explain what location information was collected or how long it was retained. Further, the government made no showing that Davis was actually aware that MetroPCS's privacy policy existed.

The record is devoid of any evidence that Davis, a teenager at the time who suffered from lifelong learning disabilities, knew anything about cell phone towers and how cell phones work, let alone that MetroPCS was recording his location whenever he made or received phone calls. Nor is it plausible to infer his understanding of cell phone company policies regarding location data, where the Chief Justice of the United States has acknowledged not reading 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). The government concedes that "the service contract and privacy policy governing Davis's phone are not part of the record in this case." Gov't En Banc Answer Br. at 28 n.4.

6. The cell tower records are not like security surveillance tapes.

Citing *Donaldson v. United States*, 400 U.S. 517, 91 S.Ct. 534 (1971), in which a taxpayer was not permitted to intervene in a summons proceeding as to records in an employer's possession and owned by employer, the government would treat a cell phone company as an independent entity having no duty of confidentiality regarding its customers. The government's analogy is both inapt and proves too much. A taxpayer would clearly have standing to raise a claim of violation of his constitutional rights if a third party were ordered to produce records belonging to the taxpayer. *See United States v. Kordel*, 397 U.S. 1, 7, 90 S.Ct. 763, 766-767 (1970)("Without question" corporate officer had right to invoke his personal constitutional privilege against self-incrimination with respect to discovery request served by government agency on corporation); *Reisman v. Caplin*, 375 U.S. 440, 445, 84 S.Ct. 508, 511-14 (1964) (tax document summons may be challenged, on constitutional or other grounds, by any affected party, including taxpayer); *see also Jones*, 132 S. Ct. at 952 n.6 (contrasting other location tracking from the "dragnet-type law enforcement practices" that GPS tracking makes possible).

And the mere fact that while on another person's property, one may be subject to the owner's recording of events on or near that property—or even subject to police monitoring of activities on a public street—does not mean private tracking of every

communication or passive use of a phone (including from one's home) is to be treated as a publicly-displayed activity. Far from it, such private use of computer-phone operations comes closer to the core of privacy under the Fourth Amendment's focus on books and papers, expressive content and means.

7. Technological advances may readily give rise to an expectation of privacy in information.

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 (as in this case) over a relatively lengthy period. The government's use of that information to track the movements of particular targeted individuals, building a detailed understanding of the target's patterns of behavior and social and professional contacts and activities, goes to the core of expectations of privacy. But for the technological development, there would have been no invasion of the privacy right. *See Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038 (2001); *Riley*, 134 S. Ct. at 2490; *Jones*, 132 S. Ct. at 950-51.

8. SCA provides for keeping track of people's movements, and it unlikely that Congress sought to allow the Fourth Amendment violation.

A significant question exists whether Section 2703(d) even applies to the production of 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.

The *en banc* questions posed by this Court, 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, raises an underlying issue of statutory construction. The distinction between historical and real-time uses can be blurred by the manner in which the government conducts an investigation. 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).

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 the Federal Rule of Criminal Procedure 41 tracking device warrant requirements. *See* Fed. R. Crim. P. 41(a)(2)(E) (adopting Section 3117 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) (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.

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, interpreting the

term as including unsworn argument by a prosecutor of the reasonableness of an investigative effort. But that view of "reasonable grounds" may be too narrow. And the statute could be interpreted to incorporate the same reasonableness concepts as the Fourth Amendment itself, such that where a warrant would normally be required, there would not be reasonable grounds for the statutory bypass.

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. 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). 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, 615–32 (5th Cir. 2013) (Dennis, J. dissenting). This issue of statutory construction is relevant to several aspects of the case, including application of the good faith exception. 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).

"Surveillance" and "monitoring" are just two of the factors that distinguish CSLI tracking, in a law-enforcement influenced environment, from an ordinary production of preexisting documentary evidence from such a witness. Thus, what the government refers to as the "thoughtful normative" arguments made by Davis and

amici—such as the difference between short and long term data collection, or between cell tower location and other location data—involve fundamental rights and affect the interpretation of Congress's "nuanced policy" determinations relating to privacy expectations in context of technological changes.

As the use of cell phones becomes ubiquitous and cell site location information becomes ever-more precise, it is crucial for courts to provide guidance to law enforcement and the public about the scope of the Fourth Amendment. Moreover, as the Supreme Court noted in *Clark v. Martinez,* 543 U.S. 371, 125 S.Ct. 716 (2005), "It is not at all unusual to give a statute's ambiguous language a limiting construction called for by one of the statute's applications." *Id.* at 380, 125 S.Ct. at 724; *see also Zadvydas v. Davis,* 533 U.S. 678, 689, 121 S.Ct. 2491, 2498 (2001) ("We have read significant limitations into [numerous] statutes in order to avoid their constitutional invalidation.").

Unlike the issue in *United States v. Steiger*, 318 F.3d 1039, 1045 (11th Cir. 2003), of whether an independent party using available technologies to make records as to its own property implicate the Fourth Amendment, there is unquestionably government action at issue here. The Supreme Court already rejected a similar government argument in *Riley*. *Riley* drew no meaningful distinction between locally stored data and cloud-based data. 132 S.Ct. at 2491, 2388. Cell service providers,

like other cloud-based technologies, incidentally accumulate massive quantities of information about users that, when aggregated, implicate significant privacy rights. *Riley* recognized a reasonable expectation of privacy in this data. *See id.* at 2489-90. Simply stated, nobody at MetroPCS witnessed appellant's movements, let alone any criminal activity. The government, using MetroPCS as custodian, required the cell service provider to furnish a record of Davis's movements. But the technology requires merely anonymous, transitory detection. Utilizing an article of technology as a means to track an individual's movements does not make MetroPCS a witness. Absent the conduct of the government, no one would have ever known or seen what the government argued was appellant's every move.

The government's involvement in not merely authorizing and encouraging cellular service providers to collect and store CSLI, but enforcing laws and regulations requiring this CSLI activity distinguishes any attempt to treat the data searches as private party action. Service providers entered into a joint protocol with the government to develop and deploy hardware and software that would satisfy law enforcement's desire to track customers.[1] Although the service providers might now

---

[1] The existence of a business purpose for cell site location records does not vitiate the fact that the government drove the collection of the data and creation of the record. Importantly, wireless service providers have no independent business purpose in recording and storing over long periods the details of a particular (continued...)

use that equipment for business purposes as well, when it stores and delivers the data to the government to track a specific person, it is not turning over a business record. *See Ferguson*, 532 U.S. at 88 (Kennedy, J., concurring) ("As a systemic matter, law enforcement was a part of the implementation of the search policy in each of its applications.").

9. Location tracking that is independent of a person's affirmative, public manifestations of location distinguishes CSLI from transactional records.

Cell phones "hold for many Americans the privacies of life." *Riley*, 134 S. Ct. at 2495(citation and internal quotation marks omitted). In *Riley*, the Supreme Court

---

[1](...continued)
individual's movement. Thus, when routing a call, service providers monitor and manage cell site use, but they do not store and track specific individuals for their own ends, but rather to satisfy law enforcement. The "extensive entanglement of law enforcement cannot be justified by reference to legitimate needs." *Ferguson*, 532 U.S. at 83 n.20, 121 S.Ct. at 1292 n.20.

The current law enforcement practice of retroactively tracking defendants with historical CSLI grew out of the surveillance partnership that Congress created with the Communications Assistance to Law Enforcement Act (CALEA), 47 U.S.C. § 1001 *et seq*., which was designed to allow law enforcement to continue its surveillance activities in the face of new digital technologies and services. *See* 47 U.S.C. § 1001(2)(requiring wireless communications carriers to store and make available to law enforcement "call-identifying data" that allows law enforcement to determine cell phone location). The regulatory atmosphere in place while location tracking technology developed establishes that the government is not simply obtaining a business record that the cell service provider recorded and stored on its own initiative. Legislation demanded that businesses develop a means to give the government that record, independent of any business purpose. In *Miller*, the bank's keeping of account records was the essence of its business.

focused on individuals' strong privacy interest in the information that their cell phones reveal about them—concerns that are not limited to the warrant exception at issue, searches incident to arrest. The Supreme Court declared without qualification that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Id.* at 2488 (emphasis added). The Supreme Court described just how intimate and detailed location data is: "Data on a cell phone can also reveal where a person has been. Historic location information... can reconstruct someone's specific movements down to the minute, not only around town, but within a particular building." *Id.* at 2490. *Riley* recognized that analyzing CSLI allows the government to retroactively track a person into a home or other protected space. *Id.* Generating and monitoring "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" infringes upon an individual's reasonable expectation of a privacy that is protected by the Fourth Amendment. *Riley*, 134 S. Ct. at 2490.

Riley also adopted the mosaic theory of privacy explained in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), and approved by Justices Sotomayor and Alito in their *Jones* concurrences. 134 S. Ct. at 2489. 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.

As customers demand more bandwidth to support smartphones, video services, and other high-volume Internet access, service providers increase the density of cell towers, further shrinking the size of particular cells.

10. Comparing an *ex parte* CSLI order to a judicial subpoena directing third-party production, does not change the Fourth Amendment analysis in this case.

Warrants and subpoenas *are* subject to different standards of constitutional reasonableness. *See Miller*, 425 U.S. at 446, 96 S.Ct. at 1625 (reaffirming the "traditional distinction between a search warrant and a subpoena"). But they are also subject to different opportunities for adversarial litigation. The sealed order to produce CSLI in this case, while arguably subject to a mandamus challenge by the cell phone company, is many steps removed from an ordinary discovery device such as a subpoena. The subpoena process remains available to the government in any

case in which it seizes evidence. That does not eliminate the Fourth Amendment's application to unilateral law enforcement violations of privacy rights. The ability to issue subpoenas says nothing about complying with the warrant requirement when the Fourth Amendment so directs. *Riley*, in step with recent CSLI decisions and statutes, indicates that, if it wants to use seize CSLI in an investigation, the government needs to get a warrant.

11. The participation of a magistrate judge in issuance of the sealed order does not diminish the Fourth Amendment violation.

The mere involvement of a magistrate judge, in *ex parte* review of an unsworn presentation by a prosecutor, does not approximate the testing and rigor of independent probable cause analysis for issuance of warrants. *See 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. Nor do the statute's remedies for abuses cure the Fourth Amendment problem. The appropriate remedy remains exclusion of the evidence, not monetary damages.

12. That the government admits it asked for and obtained much more CSLI than it even wanted for its investigation does little to inspire confidence that a new exception to the warrant requirement will offer protection from abuse.

The government concedes the sloppiness and excess of its application and the order it drafted, and argues that its failure to use even more of the improperly obtained evidence proves that the SCA processes the government abused are adequate in instances of belated government restraint or lack of curiosity about the data it improperly obtained. There is simply no precedent for using evidence of the lack of rigor of a seizure process to justify watering down Fourth Amendment protections.

13. The government's resort to emergency, murder, or terrorism scenarios is misplaced where it has made no showing that having a prosecutor make a proffer to a magistrate takes less time than having the actual agent witness make a sworn statement in a warrant application.

Important goals are served by law enforcement. But absent special circumstances clearly inapplicable here, such goals do not trump constitutional rights that preserve the foundation for a democratic society. The statute is not limited to emergencies or special circumstances in any event, and a general resort to arguments based on fear of crime have always been rejected by courts protecting fundamental Fourth Amendment rights. *Riley* already considered and rejected the government's argument. "We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime." 134 S. Ct. at 2493. "Police efficiency," the Supreme Court explained, does not trump the Fourth Amendment, particularly where

(like here) law enforcement seeks to rummage through private data, unrestrained, with "reviled general warrants" like those that inspired the Fourth Amendment in the first place. *See id.* at 2493-94.

14. The government's claim for application of the good faith exception fails in light of the facial defects of the application and order, its overbroad nature, the text of the statute, and the deliberate choice made by the government to take the non-warrant route.

Application of the exclusionary rule in this case—a remedy that the government contends would not destroy its ability to prosecute the defendant and thus would permit a meaningful retrial—is critical to enforcement of the fundamental Fourth Amendment interest at stake. There simply was no reliance on a magistrate judge determination in this case. In essence, a prosecutor made a closing argument in the form of an application for a sealed order that unconstitutionally violated the defendant's property rights. The magistrate judge had no basis to say the prosecutor's assertions were unreasonable and hence the magistrate judge relied *on the prosecutor*. The circularity of the reliance equation is self-evident. Application of a good faith exception here would simply encourage prosecutorial actions in violation of the constitution, not reliance on a rigorous application of constitutional law. 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 government concedes that the district court did not make a good faith finding in Davis's case, requiring at the least a remand for that determination. In the district court, the government would have the opportunity to show whether the totality of the circumstances establishes that relying on general theories and an internally contradictory statute was objectively unreasonable. Neither the statute, general third-party doctrine cases, nor the "weight" of cases interpreting § 2703(d) support applying the good faith exception.

The inapplicability of the good faith exception does not mean that the government acted in subjective bad faith. *See United States v. Leon*, 468 U.S. 897, 919 n.20 (1984). But it did not act with particular care either. The government characterizes failure to identify the crime being investigated and for which the cell phone data was sought as a mere "scrivener's error." But such facial defects—such as misidentifying a house to be searched—render warrants facially invalid and should have no less effect here. *See Groh v. Ramirez*, 540 U.S. 551, 557-58, 564, 124 S.Ct. 1284, 1289-90, 1294 (2004) (warrant that failed to describe the persons or things to be seized was invalid on its face, and no reasonable officer would have relied on it,

notwithstanding that requisite particularized description was provided in search warrant application).

CONCLUSION

Wherefore, 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 6,998 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 filed electronically and forwarded to the Court by Fedex services for delivery on the 31st day of December 2014.

s/Jacqueline E. Shapiro
Jacqueline E. Shapiro