NO. 11-20884

IN THE

UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR HISTORICAL CELL SITE DATA

On Appeal from the United States District Court
for the Southern District of Texas
Houston Division, Civil No. 4:11-MC-00223

Brief of the American Civil Liberties Union Foundation, the ACLU Foundation of Texas, the Electronic Frontier Foundation, the Center for Democracy and Technology, and the National Association of Criminal Defense Lawyers as Amici Curiae in Support of Affirmance

Hanni Fakhoury
Matthew Zimmerman
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

Cynthia E. Orr
GOLDSTEIN, GOLDSTEIN & HILLEY
310 S. St. Mary's St.
29th Floor Tower Life Bldg.
San Antonio, Texas 78205
(210) 226-1463

Catherine Crump
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

Lisa Graybill
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF TEXAS
P.O. Box 12905
Austin, TX 78711
(512) 478-7300 ext. 116

CERTIFICATE OF INTERESTED PERSONS

Amici curiae American Civil Liberties Union Foundation, ACLU Foundation of Texas, Electronic Frontier Foundation, Center for Democracy and Technology, and National Association of Criminal Defense Lawyers certify that they are not-for-profit corporations, with no parent corporations or publicly-traded stock.

Undersigned counsel of record certify that no persons and entities as described in the fourth sentence of Rule 28.1 have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate possible disqualification or recusal.

The only party to this case is the United States, which is represented by the U.S. Department of Justice.

Dated: March 16, 2012

/s/ Catherine Crump
American Civil Liberties Union Foundation

/s/ Hanni Fakhoury
Hanni Fakhoury
Matthew Zimmerman
Electronic Frontier Foundation

/s/ Cynthia E. Orr
Cynthia E. Orr
Goldstein, Goldstein & Hilley

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

STATEMENT OF AMICI CURIAE

The American Civil Liberties Union Foundation ("ACLU") is a nationwide, non-profit, non-partisan public interest organization of more than 500,000 members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU Foundation of Texas, the organization's affiliate in Texas, was founded in 1938 to protect and advance civil rights and civil liberties in the state of Texas and currently has over 12,000 members. The protection of privacy as guaranteed by the Fourth Amendment is of special concern to both organizations. The ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy.

The Electronic Frontier Foundation ("EFF") is a non-profit, member supported civil liberties organization, based in San Francisco, California, working to protect privacy rights in a world of sophisticated technology. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy, and has served as counsel or amicus curiae in cases addressing privacy rights, as well as the Fourth Amendment's application to new technologies.

The Center for Democracy & Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated technologies. CDT

represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The National Association of Criminal Defense Lawyers ("NACDL") is a non-profit professional bar association that represents the nation's criminal defense attorneys. Its mission is to promote the proper and fair administration of criminal justice and to ensure justice and due process for those accused of crime or misconduct. Founded in 1958, NACDL has a membership of approximately 10,000 direct members and an additional 35,000 affiliate members in all 50 states and 30 nations. NACDL has frequently appeared as amicus curiae before federal and state courts, and regularly appears as amicus curiae in cases involving the Fourth Amendment, and its state analogues.

This Court granted amici ACLU, ACLU of Texas and EFF leave to file an amicus brief not to exceed 14,000 words. No party's counsel authored this brief in whole or in part, or contributed money intended to fund preparing or submitting the brief. No other person contributed money that was intended to fund preparing or submitting the brief.

STATEMENT REGARDING ORAL ARGUMENT

Amici request oral argument, as it may be helpful to the Court in addressing the novel issues presented by this appeal.

INTRODUCTION

This case raises the important question of whether courts may require the government to obtain a warrant based upon probable cause before accessing 60 days' worth of cell phone location data. This question is of great significance to the hundreds of millions of Americans who carry cell phones, because "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

This Court should join the Third Circuit in concluding that the Stored Communications Act ("SCA") grants courts the discretion to require the government to obtain a warrant based upon probable cause before accessing historical cell phone location data. *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 315-17 (3d Cir. 2010). The plain language of the SCA compels this conclusion. Moreover, the doctrine of constitutional avoidance supports this interpretation. After the Supreme Court's recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012), it is even clearer that the government violates the Fourth

Amendment when it obtains 60 days' worth of cell phone location data without first securing a warrant based upon probable cause. This Court can avoid ruling on the constitutionality of the SCA, however, by holding that the act allows courts to require a warrant based upon probable cause, as occurred here.

If this Court does reach the constitutional question, then it should conclude that the Fourth Amendment requires the government to first obtain a warrant based upon probable cause to access 60 days' worth of cell phone location data. If tracking a vehicle over 28 days violates a reasonable expectation of privacy, *see United States v. Jones*, 132 S. Ct. 945 (2012), then tracking a cell phone for more than twice that period surely violates such an expectation as well. Moreover, the warrant and probable cause requirements are essential to ensuring that these invasive searches do not take place without adequate justification.

Finally, the magistrate judge's findings of fact cannot serve as the basis for reversal. These findings are not before this Court. Rather, it is the decision of the district court, not the magistrate, that is on review. But even if the findings of the magistrate judge were before this Court, the appropriate standard of review is the "clearly erroneous" standard, which they easily meet.

The decision below should be affirmed.

ARGUMENT

I. THE STORED COMMUNICATIONS ACT GIVES JUDGES DISCRETION TO REQUIRE THE GOVERNMENT TO APPLY FOR A SEARCH WARRANT IN ORDER TO OBTAIN CELL PHONE LOCATION DATA.

The Supreme Court has cautioned that the "judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010). The issue of whether cell phone location data held by cell phone providers is protected by the Fourth Amendment presents such a risk, particularly in light of the Supreme Court's recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012), in which five justices agreed that long-term monitoring of location information violated a reasonable expectation of privacy and therefore constituted a "search" under the Fourth Amendment.

Yet this Court need not address the difficult constitutional issue of whether the rationales of the *Jones* concurrences apply to cell phone location data. The plain language of the SCA[1] makes clear that courts have the discretion to require the government to proffer probable cause and apply for a search warrant in order to obtain cell phone location data. That discretion is important, because it obliges this Court to avoid the constitutional issue here: whether the Fourth Amendment

[1] 18 U.S.C. §§ 2701-12. All further statutory references are to Title 18 unless noted otherwise.

requires the government to obtain a warrant based upon probable cause to access cell phone location data.

A. Statutory Background

"Statutory interpretation begins with the statute's plain language." *Carder v. Continental Airlines, Inc.*, 636 F.3d 172, 175 (5th Cir. 2011). A court's "inquiry must cease if the statutory language is unambiguous and the statutory scheme is coherent and consistent." *Robinson v. Shell Oil Co.*, 519 U.S. 337, 340 (1997) (internal quotation marks omitted).

Cell phone location data stored by a cell phone provider is protected against government access by the SCA, which is part of the Electronic Communications Privacy Act.[2] The SCA comprehensively regulates the disclosure of communications content, records, and other information stored by electronic communication service providers. Specifically, cell phone location data is protected under § 2703(c)(1), which states, in pertinent part:

> A governmental entity may require a provider of electronic communication service…to disclose *a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)* only when the governmental entity—
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
> (B) obtains a court order for such disclosure under subsection (d) of

[2] *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986).

> this section;
> [or]
> (E) seeks information under paragraph (2).

18 U.S.C. § 2703(c)(1) (emphasis added). In short, the government has only three ways of compelling a service provider to disclose non-content information pertaining to a customer: (1) obtain a search warrant under Rule 41 of the Federal Rules of Criminal Procedure; (2) obtain an order pursuant to § 2703(d); or (3) with respect to "subscriber information" – name, address, and credit card information – irrelevant here, obtain a subpoena. *See* 18 U.S.C. § 2703(c)(2).

In this case, the government did not obtain a Rule 41 search warrant, nor was it attempting to collect "subscriber information." At issue, then, is § 2703(d), which, as will be shown below, permits a court to demand a probable cause search warrant before authorizing the government to seize cell phone location data.

B. The Stored Communications Act Permits A Court To Require A Probable Cause Search Warrant Rather Than An Order Under The § 2703(d) Standard Before Authorizing The Seizure Of Cell Phone Location Data.

Although this Court has never addressed the specific issue here, the Third Circuit has held that the SCA provides magistrates the discretion to deny applications for cell phone location data even when the government has made the factual showing required under § 2703(d). *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't,*

620 F.3d 304, 315-17 (3d Cir. 2010) (hereinafter "*Third Circuit Opinion*"), *pet. for reh'g en banc denied* (3d Cir. Dec. 15, 2010) . For the reasons stated in the Third Circuit's persuasive opinion, this Court should follow suit.

The relevant text of § 2703(d) states:

> 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 governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d) (emphasis added). As the Third Circuit explained, the SCA's use of the phrase "only if" in § 2703(d), indicates that the "specific and articulable facts" showing required by that section is a necessary, but not sufficient condition for the issuance of a § 2703(d) order.

This interpretation of the text of § 2703(d) is consistent with how the phrase "only if" has been interpreted by this and other courts. *See United States v. Silva*, 957 F.2d 157, 159 (5th Cir. 1992) (quoting *California v. Hodari D.*, 499 U.S. 621, 628 (1991) to explain that "only if" signifies "a *necessary*, but not a *sufficient*, condition"); *see also Twp. of Tinicum v. U.S. Dep't of Transp.*, 582 F.3d 482, 488 (3d Cir. 2009); *Alden Mgmt. Servs., Inc. v. Chao*, 532 F.3d 578, 581 (7th Cir. 2008).

As the Third Circuit noted, "[i]f Congress wished that courts 'shall,' rather

than 'may,' issue § 2703(d) orders whenever the intermediate standard is met, Congress could easily have said so. At the very least, the use of 'may issue' strongly implies court discretion, an implication bolstered by the subsequent use of the phrase 'only if' in the same sentence." *Third Circuit Opinion*, 620 F.3d at 315. This Court has also explained that when Congress uses terms that have established meaning, a court must infer that "Congress means to incorporate the established meaning of these terms." *United States v. Southland Mgmt. Corp.,* 288 F.3d 665, 677 n.13 (5th Cir. 2002).

In sharp contrast to § 2703(d)'s permissive language, Congress has elsewhere provided for *mandatory* issuance of court orders based on a specific legal showing. In particular, the statute governing the installation of "pen register" and "trap and trace devices" that capture non-content communication routing information in real time, sets forth a mandatory standard under which courts must grant government applications for orders authorizing such surveillance:

> Upon an application made under section 3122 (a)(1), the court *shall* enter an *ex parte* order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, *if* the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

18 U.S.C. § 3123(a)(1) (emphasis added). The pen register statute's "shall…if" requirement stands in sharp contrast to the permissive "shall…*only* if" language

found in § 2703(d). If possible, the Court must "give effect . . . to every clause and word of a statute." *See Duncan v. Walker*, 533 U.S. 167, 174 (2001). For the "only" in § 2703(d) to have meaning, it must be construed to allow the Court the discretion to deny an application for an order under § 2703(d) even if a "specific and articulable facts" showing has been made. *See Third Circuit Opinion*, 620 F.3d at 319.

The practical effect of such a denial is that pursuant to § 2703(c)(1)(A), the government must instead proceed by obtaining a search warrant based on probable cause, issued under Rule 41 of the Federal Rules of Criminal Procedure. *See Third Circuit Opinion*, 620 F.3d at 316. Therefore, "the statute as presently written gives the [magistrate judge] the option to require a warrant showing probable cause." *Id.* at 319.

Recognizing a court's discretion to impose additional requirements before issuing an order under § 2703(d) is also consistent with Congress' recognition that electronic content providers are storing more (and more invasive) types of records and other information, with uncertain protection under the Fourth Amendment. As the Senate Judiciary Committee's report on the statute explained:

> With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information *may* be subject to no

constitutional privacy protection.

S. Rep. No. 99-541 at 3 (1986) (emphasis added); *see also, e.g.*, S. Hrg. 98-1266 at 17 (1984) ("In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether a participant to an electronic communication can claim a reasonable expectation of privacy] are not always clear or obvious.").

Similarly, in 1994, Congress amended the SCA in the Communications Assistance for Law Enforcement Act ("CALEA") to provide additional protections for non-content records held by electronic content storage providers that in the past could be obtained with a mere subpoena. *See* Pub. L. No. 103-414, Title II, § 207(a), 108 Stat. 4292 (Oct. 25, 1994). CALEA brought greater protection to customers by specifically enumerating the limited subscriber information that could be obtained with only a subpoena under 18 U.S.C. § 2703(c)(2). It also created a new intermediate category of transactional information that could only be obtained using a warrant or an order under § 2703(d). Congress did so because it recognized that "in the face of increasingly powerful and personally revealing technologies," H.R. Rep. No. 103-827 at 13 (1994), the requirement of a mere subpoena was not sufficient to protect the privacy of the increasing quantity and quality of more invasive types of records threatening to reveal a "person's entire on-line profile." H.R. Rep. No. 103-827 at 17 (1994).

Allowing disinterested magistrates the flexibility to require a greater showing from the government for the disclosure of particularly sensitive or novel types of private information ensures that the SCA's protections are not made obsolete by emerging technologies, consistent with Congress' broad protective purpose. Moreover, in the context of uncertainty regarding the scope of Fourth Amendment protection in emerging technologies—uncertainty that was starkly highlighted by the Supreme Court's recent decision in *Jones*, discussed in more detail below—it makes sense that Congress would provide a constitutional safety-valve by allowing a judge to deny an application under § 2703(d) and instead require the government to seek a Rule 41 search warrant under § 2703(c)(1)(a).

C. None Of Professor Kerr's Jurisdictional Arguments Alter The Conclusion That § 2703(d) Gives Magistrate Judges Discretion To Require A Search Warrant.

In his amicus brief, Professor Orin S. Kerr writes that Congress did not grant magistrate judges the discretion to rule on the constitutionality of § 2703(d) orders, but this argument hinges on impermissibly reading "only . . . if" out of the statute. *See* Amicus Curiae Br. of Professor Orin S. Kerr ("Kerr Amicus") at 12-16.

Professor Kerr recognizes that magistrate judges are empowered to either grant or deny § 2703(d) requests, but he argues that the use of the words "shall issue" means the matter is "non-discretionary." *Id.* at 13, 16. Yet Congress' expression of its desire to give magistrate judges discretion is not based on the

phrase "shall issue," but rather, as the Third Circuit highlighted (and as explained earlier), by using the words "only if" in § 2703(d). "Only if" means that the "specific and articulable facts" standard is a necessary, but not necessarily a sufficient, condition for the issuance of a § 2703(d) order. Professor Kerr's brief does not deal with this crucial portion of the statute. *See* Kerr Amicus at 15-16.

Professor Kerr next argues that the lack of discretion is "inherent" in the SCA, Kerr Amicus at 13-16, an argument the Third Circuit has already dispensed with easily, as should this Court. Like the government before the Third Circuit, Professor Kerr argues that the purpose of allowing the government to obtain cell phone location data with a warrant is to permit the government to avoid having to use different types of processes for different records. But as the Third Circuit explained, this argument "trivializes the statutory options to read the § 2703(c)(1)(A) option as included so that the Government may proceed on one paper rather than two." *Third Circuit Opinion*, 620 F.3d at 316. The more persuasive argument is that presented above: allowing different forms of processes permits magistrate judges to safeguard constitutional rights in the face of rapidly changing technology.

Magistrate judges are routinely given discretion to make decisions based on constitutional concerns. Congress permitted district court judges to "designate a

magistrate judge to hear and determine *any* pretrial matter pending before the court," subject to a small number of exceptions irrelevant here. 28 U.S.C. § 636(b)(1)(A) (emphasis added). Even in matters otherwise excluded in 28 U.S.C. § 636(b)(1)(A), magistrate judges are nonetheless authorized to conduct evidentiary hearings and make findings and recommendations to the district court. 28 U.S.C. § 636(b)(1)(B). And naturally, many of these decisions bear directly on constitutional rights. When a magistrate judge makes a recommendation to a district court judge to suppress evidence or grant *habeas corpus* relief, for example, the magistrate makes a legal decision about the constitutionality of government conduct. And that decision is subject to review by the district court judge (and ultimately the court of appeals), just like the decision to approve or deny a § 2703(d) application.[3]

Professor Kerr worries, nonetheless, that because government applications for § 2703(d) orders are made *ex parte*, institutional difficulties arise in deciding the constitutionality of government applications, but his solution—allowing the issue to be resolved only after the fact—creates even bigger problems. For if a magistrate judge believes he is being asked to authorize an unconstitutional act,

[3] Professor Kerr also worries that magistrate judges do not have the authority under Article III of the Constitution to rule on the constitutionality of § 2703(d). *See* Kerr Amicus at 16-19. There is no Article III problem here because, as explained above, Congress explicitly authorized the magistrate's use of discretion in the text of § 2703(d).

preventing him from denying the application results in the expenditure of considerable government resources in pursuit of a course of action that may later be found illegal and unusable in court proceedings. And that in turn results in unnecessary privacy intrusions into the lives of innocent people, against whom a criminal case may never be brought, and who may never realize they were being surveilled by the government.

To this point, Professor Kerr's amicus brief questions whether this case is even ripe, suggesting that at the time the government applies for a § 2703(d) order, a judge is to either approve or deny the request without determining "the constitutionality of the future execution of the search" because "[a] court cannot apply the Fourth Amendment when no facts yet exist." Kerr Amicus at 2, 4, 8. This sweeping argument should be rejected as contrary to how the Supreme Court has applied the Fourth Amendment in the past. In *Chandler v. Miller*, 520 U.S. 305 (1997), the Supreme Court struck down a Georgia law mandating drug testing of certain candidates for elective office. The Supreme Court did not require the candidates to wait until after they were tested to pursue a challenge. Nor did the Supreme Court enjoin the statute only as to them, on the off-chance that a future candidate might be, for example, a parolee with a reduced expectation of privacy. *See* Kerr Amicus at 9. The Supreme Court struck the statute down in its entirety. *Chandler*, 520 U.S. at 323.

Similarly, where the government files an application requesting access to specific data—in this case, cell phone location data for whenever a phone is turned on—magistrate judges need not sit idly by while individuals' constitutional rights are violated. Indeed, absent extraordinary circumstances, the application stage is the *only* point at which the rights of innocent Americans to be free from warrantless location tracking may be vindicated, for without a subsequent criminal prosecution they are unlikely to even learn that they were targets.

Discussing search warrants, the Supreme Court long ago noted that since "the police acting on their own cannot be trusted . . . the Constitution requires a magistrate to pass on the desires of the police *before* they violate the privacy of the home." *McDonald v. United States*, 335 U.S. 451, 456 (1948) (emphasis added). As a result, judges are required to ensure that when it comes to "what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Stanford v. Texas*, 379 U.S. 476, 485-86 (1965).

The only way to ensure that nothing is left to an officer's discretion is for a judge to craft explicit limitations with an eye toward the future, anticipating potential constitutional problems and placing limits to prevent unconstitutional privacy intrusions. This observation applies directly to cell phone location data. If a magistrate judge believes a § 2703(d) application presents a potential constitutional problem, he or she has the discretion to require the government to

request a search warrant instead. Doing so *before* the government obtains the data is necessary to ensure that "nothing is left to the discretion" of the government.

Moreover, if a magistrate denies a § 2703(d) request, the government has recourse: it can either appeal to a district court judge (as it did here), or come back with an application for a search warrant supported by probable cause. And if a magistrate approves a § 2703(d) order, it can still be subject to meaningful review if a criminal defendant challenges it in the course of a criminal prosecution that follows the government's seizure of records.

In sum, Congress gave magistrate judges the discretion not only to make constitutional determinations, but also to require the government to apply for a search warrant. By requiring the government to request a search warrant, the magistrate judge saves § 2703(d) from being declared unconstitutional. And as is clear from the serious nature of the constitutional issues at play in this case, explained below, this Court can also avoid finding § 2703(d) unconstitutional.

D. The Doctrine Of Constitutional Avoidance Requires This Court To Construe § 2703(d) As Giving Judges Discretion To Require A Warrant.

The constitutional avoidance doctrine "rest[s] on the reasonable presumption that Congress did not intend" any meanings of a statute to "raise[] serious constitutional doubts," *Clark v. Martinez*, 543 U.S. 371, 381 (2005), and "[i]t is therefore incumbent upon [the Court] to read the statute to eliminate those doubts

so long as such a reading is not plainly contrary to the intent of Congress." *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 78 (1994) (internal citations omitted).

Section 2703(d) places no restrictions on the discretion it grants to magistrates, *see Third Circuit Opinion*, 620 F.3d at 319, but of course that discretion is not boundless: "[N]o judge in the federal courts has arbitrary discretion . . . ." *Id.* at 316. Rather, a magistrate's decision to require a warrant "must be supported by reasons" justifying a divergence from § 2703(d)'s specific and articulable facts standard. *Id.* at 316-17. In other words, courts, including magistrates, clearly may not abuse the discretion that has been granted to them.

In this case, there is a very clear and straightforward basis for the magistrate's exercise of discretion. Well-grounded constitutional concerns, reaffirmed by *Jones*, about the status of location information led the magistrate to conclude that a warrant was necessary. In light of the discretion granted to courts by Congress in § 2703(d), and particularly in light of the Supreme Court's recent admonition that courts should avoid unnecessary rulings on how the Fourth Amendment applies to new technologies, it is clear that when faced with a government application that raises a serious constitutional question, the appropriate course for a magistrate is to avoid that question by exercising its discretion and denying that application. *See Quon*, 130 S. Ct. at 2629. It is equally clear under

the doctrine of constitutional avoidance that this Court need not endeavor to definitively answer the serious Fourth Amendment question posed by the government's application in order to affirm the magistrate's denial, but instead need only recognize that it does raise a serious Fourth Amendment question.

As amply demonstrated by the magistrate judge's comprehensive opinion, and as fully explained below, the question of whether cell phone location data is protected by the Fourth Amendment is present in this case. However, to the extent this Court disagrees with the Third Circuit and finds no room for discretion in § 2703(d), the answer to this serious Fourth Amendment question is clear: cell phone users do have a reasonable expectation of privacy in their location, and the government must obtain a warrant before acquiring cell phone location data from a cell phone provider.

II. THE GOVERNMENT NEEDS A WARRANT BASED UPON PROBABLE CAUSE TO OBTAIN ACCESS TO 60 DAYS' WORTH OF HISTORICAL CELL PHONE LOCATION DATA.

The Supreme Court's decision in *Jones* makes it clear that obtaining 60 days' worth of cell phone location data is the sort of prolonged location tracking that constitutes a search under the Fourth Amendment. Location tracking, particularly over a long period of time, can reveal a great deal about a person. "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an

outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012).

In *Jones*, five justices of the Supreme Court concluded that an investigative subject's "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Jones*, 132 S. Ct. at 958, 964 (Alito, J. concurring); *id.* at 955 (Sotomayor, J. concurring) (expressing agreement with Justice Alito). If tracking a vehicle for 28 days is a search, then surely tracking a cell phone for 60 days is likewise a search, particularly because people constantly keep their cell phones with them in their purses and pockets as they traverse both public and private spaces. Moreover, the warrant and probable cause requirements are essential to ensuring that these invasive searches do not take place without adequate justification.

The government argues that *Jones* is inapplicable, but its argument rests on an unjustifiably narrow reading of *Jones* that fails to account for Americans' expectation that they will not be subject to long-term and constant monitoring of their movements. The government's reliance on the Court's jurisprudence regarding bank records and dialed telephone numbers is similarly misplaced, because cell phone location data is not voluntarily communicated to cell phone

providers in the same way that banking transactions and dialed numbers are disclosed to banks and telecommunication companies. Further, the government's fallback argument – that it should only have to demonstrate that its request is reasonable even if the Fourth Amendment applies – carries little weight, because the case law the government draws on, which addresses subpoenas, invariably involves the provision of prior notice, which is absent in this case.

A. Obtaining 60 Days' Worth Of Cell Phone Location Data Is A "Search" Under The Fourth Amendment Requiring A Warrant Based Upon Probable Cause.

The district court correctly concluded that "[w]hen the government requests records from cellular services, data disclosing the location of the telephone at the time of particular calls may be acquired only by a warrant issued on probable cause." (R. 43).[4] The *Jones* case and the *Karo* case before it make clear that when the government engages in prolonged location tracking, or when tracking reveals information about a private space that could not otherwise be observed, that tracking constitutes a search within the meaning of the Fourth Amendment. Cell phone tracking is a search for both of these reasons.

In *Jones*, five justices of the Supreme Court agreed that when the government engages in prolonged location tracking, it conducts a search under the

[4] Amici do not have access to the government's excerpts of record. Nonetheless, to the extent possible, this brief has attempted to cite to the record using the same citations the government used in its opening brief.

Fourth Amendment. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring) (expressing agreement with Justice Alito). The Metropolitan Police Department and FBI came to suspect that Antoine Jones was involved in trafficking narcotics. *Id.* at 947. Law enforcement agents installed on the car he drove a GPS tracking device that was used to gather information on his travels. *Id.* Although the law enforcement agents obtained a warrant to track Jones's car, they did not comply with its instructions when installing the GPS device. *Id.* The government conceded noncompliance with the warrant and argued only that a warrant was unnecessary. *Id.* at 947 n.1. The government tracked Jones's movements for 28 days, with the device registering the car's location, accurate within 50 to 100 feet, and transmitting that information to a government computer. *Id.*

Justice Scalia wrote for the majority, although his opinion is of limited relevance here. The majority held that because the government "physically occupied private property for the purpose of obtaining information," a search had taken place. *Id.* at 949. It explained that the "reasonable-expectation-of-privacy test" derived from *Katz v. United States*, 389 U.S. 347 (1967), "has been *added to*, not *substituted for*, the common-law trespassory test." *Id.* at 952. Acknowledging that its opinion only addressed surveillance that involves a trespass, the majority wrote that "[s]ituations involving merely the transmission of electronic signals

without trespass would *remain* subject to *Katz* analysis." *Id.* at 953. Thus, the majority left cell phone tracking for another day.

Five justices—including Justice Alito, who wrote for four justices concurring in the judgment, and Justice Sotomayor, who joined the majority opinion but concurred separately to note that she *also* agreed with the Alito opinion—did conduct a *Katz* analysis, and concluded that long-term location tracking violates reasonable expectations of privacy. *Id.* at 960, 964 (Alito, J., concurring in judgment); *id.* at 955 (Sotomayor, J., concurring). Justice Alito concluded that, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 964. He explained that, "[f]or such offenses, 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." *Id.*

Justice Alito's conclusion did not depend on the particular type of tracking technology at issue in *Jones*. He was well aware that the government can also track location by accessing cell phone company records, identifying the proliferation of mobile devices as "[p]erhaps most significant" of the emerging location tracking technologies. *Id.* at 963. In fact, he expressly faulted the majority's trespass-based rationale on the grounds that it "leads to incongruous

results" because it could result in Fourth Amendment protection against surveillance that involves a trespass but not functionally equivalent surveillance that does not. *Id.* at 961. For this reason, Justice Alito analyzed the issue in *Jones* by looking at the type of information the government sought to gather: location information. *Id.* at 958 (identifying the proper question as "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.")

Although Justice Sotomayor joined Justice Scalia's majority opinion, she wrote a separate concurrence in which she explained that she also agreed with Justice Alito's conclusion that, under the *Katz* reasonable expectation of privacy test, "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Id.* at 955 (quoting Alito concurrence in judgment, *id.* at 964). Justice Sotomayor spelled out the privacy-invasive nature of location tracking at length:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is 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 (internal quotation marks omitted).

In short, five justices agreed that at least long-term location tracking

constitutes a search under the Fourth Amendment because it violates individuals' reasonable expectations of privacy, and the other four justices expressly noted that they were not reaching the question of whether electronic location tracking that does not involve trespass violates a reasonable expectation of privacy.

Moreover, the Court has made clear that location tracking that reveals otherwise undiscoverable facts about protected spaces also implicates the Fourth Amendment. In *United States v. Karo*, 468 U.S. 705 (1984), the Court held that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. In *Karo*, the police placed a primitive tracking device—a beeper—inside a can of ether and used it to infer that the ether remained inside a private residence. *Id.* at 708-10. In considering a Fourth Amendment challenge to the use of the beeper, the Court held that using an electronic device to infer facts about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as searching the location without a warrant. *Id*. at 714-15. Such location tracking, the Court ruled, "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place, *id*. at 707, regardless of whether it reveals that information directly or

through inference. *See also Kyllo v. United States*, 533 U.S. 27, 36 (2001) (rejecting "the novel proposition that inference insulates a search," noting that it was "blatantly contrary" to the Court's holding in *Karo* "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home").

If following a car for 28 days violates an expectation of privacy that society is prepared to recognize as reasonable, then surely tracking a cell phone for 60 days does as well. Just as "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period," *Jones*, 132 S. Ct. at 964 (Alito, J., concurring), so, too, is it society's expectation that government agents would not track the location of a cell phone for 60 days. The expectation that a cell phone will not be tracked is even more acute than is the expectation that cars will not be tracked because individuals are only in their cars for discrete periods of time, but carry their cell phones with them wherever they go. Moreover, cars are visible on the public street, whereas individuals generally keep their cell phones in a concealed place. To be sure, *Jones* dealt with GPS tracking and this case deals with the government's collection of cell phone location data. However, the relevant question is not what type of technology is being used, but what information is being gathered. *Id.* at 958, 964 (Alito, J., concurring). Here, as in

Jones, the information being gathered is long-term information about movements. Because there is no practical distinction between the information the government seeks in this case and the information the government sought in *Jones*, the government must be deemed to be conducting a search in this case just as it was in *Jones*.

Moreover, cell phone location data implicates Fourth Amendment interests for a second reason: like the tracking in *Karo*, it reveals or enables the government to infer information about whether the cell phone is inside a protected location and whether it remains there. The cell phone travels through many such protected locations during the day where, under *Karo*, the government cannot warrantlessly intrude on individuals' reasonable expectations of privacy. *See, e.g. Kyllo*, 533 U.S. at 31 (home); *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486-88 (1964) (hotel room). This is true even if cell phone location data is as imprecise as the government claims,[5]

[5] The government argues that the MetroPCS affidavit establishes that "cell-site records cannot locate a cell phone with precision," Gov't Br. at 35, but the affidavit is inadequate to determine how closely individuals can be tracked, and suggests that the government could learn about the location of cell phones in protected spaces, which is all that is necessary for the tracking to constitute a search. The affidavit states that the radius of its towers ranges from 100 yards to five miles. (A. 110). But that does not indicate how precisely someone can be located. That depends not only on whether tower coverage is separated by sectors, but also on the density of towers, and the affidavit is silent on whether its towers are sufficiently close together that some service areas overlap. Cell phone network coverage is rapidly becoming more dense, with the number of active cellular

because even imprecise information, when combined with visual surveillance or a known address can enable law enforcement to infer the exact location of a phone. *Third Circuit Opinion*, 620 F.3d at 311. Indeed, that is exactly how the government's experts routinely use such data; as the *Third Circuit Opinion* notes, "the Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home."[6] *Id.* at 311-12.

The government argues that this Court cannot apply the location tracking cases without first remanding to the district court for fact-finding about the accuracy of the records the government seeks, Gov't Br. at 35, but a remand is unnecessary because the relevant facts are already in the record. It is undisputed

---

towers increasing by 11.5% each year. CTIA The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey* at 9 (2009), *available at* http://files.ctia.org/pdf/CTIA_Survey_Midyear_2009_Graphics.pdf. As a result, cell site technology is increasingly accurate. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 702-05 (2011). Furthermore, to the extent that the affidavit indicates that some of its towers have ranges of only 100 yards, this is certainly precise enough to pinpoint a phone's location within larger private properties not open to visual surveillance. *See* (A. 110).

[6] The government argues that there was no search of a constitutionally protected place under *Karo*, but this hinges on an excessively crabbed interpretation of that opinion. Gov't Br. at 37. In *Karo*, the Court held that monitoring a beeper in a private residence was a violation of the Fourth Amendment because "it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant." *Id.* at 715. In other words, the government did not need to know the particular location, *i.e.* whether the beeper was in the hallway closet or the downstairs bathroom.

that the government seeks cell phone location data for a prolonged period of time, a full 60 days. It is also undisputed that the only reason the government seeks the records is their utility in locating investigative subjects.

The government attempts to limit the impact of *Jones* by arguing that because the Court "looked to the original scope" of the Fourth Amendment in that opinion, and because the original scope allowed for compulsory process, *Jones* supports allowing the government to obtain cell phone location data under a reasonableness standard. Gov't Br. at 38. The majority stated no such thing. The majority held that the Fourth Amendment must protect "at a minimum" what it protected at the time the Fourth Amendment was adopted. *Jones*, 132 S. Ct. at 953. It adopted a floor, not a ceiling as the government suggests. Moreover, the majority expressly stated that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* The majority left open the possibility that cell phone location data would require a warrant based upon probable cause under *Katz*. Further, the government's argument ignores the fact that, as described above, five justices in *Jones* held that long-term tracking violates a reasonable expectation of privacy. Finally, as explained in greater detail below, the compulsory process cases are inapposite because they uniformly involve situations where the government provided notice prior to obtaining information, something the government has not done here. *See*

Part II.C, *infra*.

The government next tries to distinguish this case from *Jones* by pointing out that *Jones* involved real-time tracking and this case involves historical tracking, Gov't Br. at 39, but that is not a meaningful distinction. In both cases the government obtains long-term information about a person's travels. People have just as strong a privacy interest in a record of their movements stretching back 60 days as they have in their real-time movements. A contrary ruling would wholly eviscerate *Jones* because police officers would be free to use GPS devices to record vehicles' travels so long as they waited some minutes before accessing those records, thereby rendering them "historical."

The government also points out that cell phone location data are less precise than GPS tracking records, Gov't Br. at 39-40, but cell phone location data do not have to be exactly as precise as GPS records in order to track movements. The purpose of obtaining information about a person's location over 60 days is an interest in tracking that person's movements, and five justices have made clear that they consider that to be within an individual's reasonable expectation of privacy. *Jones*, 132 S. Ct. at 954, 957. Finally, while Justice Alito did state that the ideal solution to new privacy concerns may be legislative, *id.* at 964 (Alito, J., concurring), the SCA already allows magistrate judges the discretion to require a warrant, *see* Part I.B *supra*, and it is the judiciary, not Congress, that bears ultimate

responsibility for determining whether the laws of the land conform to the Constitution. *See Powell v. McCormack*, 395 U.S. 486, 549 (1969).

If it reaches the constitutional question, this Court should hold that the Supreme Court's location tracking cases dictate that the government conducts a search when it obtains historical cell phone location data. Prolonged location tracking, whether of a car or a cell phone, violates Americans' reasonable expectations of privacy. Moreover, it should hold that these searches require the government to obtain a warrant based upon probable cause. "A search conducted without a warrant is unreasonable *per se* and therefore unconstitutional under the Fourth Amendment, unless it is conducted pursuant to consent or under exigent circumstances." *United States v. Gonzales*, 121 F.3d 928, 938 (5th Cir. 1997), *overruled on other grounds by United States v. O'Brien*, 130 S. Ct. 2169 (2010). The warrant requirement is essential to the protections guaranteed by the Fourth Amendment. The purpose of the probable cause requirement is "to safeguard citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime." *Brinegar v. United States*, 338 U.S. 160, 176 (1949). Other than its reliance on the compulsory process cases to argue that the appropriate Fourth Amendment standard is "reasonableness," an argument amici rebut at length *infra* at II.C, the government makes no argument that any exception to the warrant requirement applies.

Even if this Court is not prepared to conclude on the present record that it would constitute a search for the government to use a court order to compel cell phone providers to disclose 60 days' worth of cell phone location data, there is at least enough information in the present record for this Court to conclude that the lower court did not abuse its discretion in requiring the government to obtain a warrant based upon probable cause in this case. The Fourth Amendment status of cell phone location data at the very least poses a serious constitutional question warranting a discretionary denial of the government's application.

B. Cell Phone Providers' Ability To Access Customers' Location Data Does Not Eliminate Cell Phone Users' Reasonable Expectation Of Privacy In That Data.

The government contends that the location tracking cases are distinguishable from this case because they do not concern business records held by a third party, Gov't Br. at 15, but the Court's business record cases are not so sweeping. Moreover, the Third Circuit reached a conclusion that directly contradicts the government's claim. It held that cell phone users may maintain a reasonable expectation in their location records even though these records are held by a third party business. *Third Circuit Opinion*, 620 F.3d at 317-18. In addition to being correct and persuasive authority, the *Third Circuit Opinion* also demonstrates the existence of a serious constitutional question on this score, justifying exercise of the discretion granted under § 2703(d) to avoid the issue by requiring a warrant.

The government relies principally on two Supreme Court cases, but neither is as broad as it claims. Gov't Br. at 16-23. In *United States v. Miller*, 425 U.S. 435 (1976), the Supreme Court held that a bank depositor had no expectation of privacy in records about his transactions that were held by the bank. The government asserts that this case stands for the proposition that a customer can never have an expectation of privacy in a third party business's records because a customer "can assert neither ownership nor possession" over them, Gov't Br. at 16 (quoting *Miller*, 425 U.S. at 440), but that statement by the Court was not the end of the analysis. The Court proceeded to consider whether Miller nevertheless could maintain a reasonable expectation of privacy in the bank's records, noting that "[w]e 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." *Miller*, 425 U.S. at 442 (internal citation omitted). The conclusion of that analysis—that Miller had no such expectation—turned not on the fact that the records were owned or possessed by the banks, but on the fact that Miller "voluntarily conveyed" their contents to the bank. *Id.* (internal quotation marks and citation omitted).

The government also leans heavily on *Smith v. Maryland*, 442 U.S. 735 (1979), but that case, too, does not extend as far as the government claims. Gov't Br. at 18. In *Smith*, the Court held that the use of a pen register to capture the

telephone numbers an individual dials was not a search under the Fourth Amendment. 442 U.S. at 739, 742. Key to its decision was a determination that individuals voluntarily convey telephone numbers to the phone company. *Id.* at 744. Moreover, in *Smith*, as in *Miller*, the question of voluntary exposure was not solely dispositive, or else *Smith* would have overruled the Court's previous holding that telephone callers maintain a reasonable expectation of privacy in their phone calls:

> A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service. The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world."

Id. at 746-47 (Stewart, J., dissenting) (quoting *Katz v. United States*, 389 U.S. 347, 352 (1967)). Considering *Katz*, *Smith* also had to consider the *invasiveness* of the surveillance at issue, and relied on the conclusion that surveillance of dialed numbers was not meaningfully invasive of privacy:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed-a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

Id. at 741 (quoting *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977)).

Contrary to the government's claim, Gov't Br. at 16, there is no *per se* rule that a business's customer may never have an expectation of privacy in the contents of the business's records; rather, the question of expectation of privacy turns on whether the contents of those records were voluntarily conveyed to the business, and what if any privacy interest a user retains in the records.

This Court should follow the Third Circuit and reject the government's argument that *Miller* and *Smith* govern here. As the *Third Circuit Opinion* explicitly recognizes, "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." 620 F.3d at 317. The court considered it significant that "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information." *Id.*

Moreover, there are good reasons that *Miller* and *Smith* should not be expanded to new contexts. The Supreme Court has recognized that "[s]ituations can be imagined, of course, in which *Katz'* two-pronged inquiry would provide an inadequate index of Fourth Amendment protection." *Smith*, 442 U.S. at 741 n.5; s*ee also Jones*, 132 S. Ct. at 950 (applying trespass theory of the Fourth Amendment, not *Katz*, to preserve constitutional minimum of privacy protection from location tracking). If this Court accepts the government's unjustifiably broad interpretation of *Miller* and *Smith*, this will be one of them. As Justice Sotomayor

pointed out in her *Jones* concurrence, the idea that people have no reasonable expectation of privacy in information they divulge to third parties is obsolete in today's digital world:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . . I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Jones, 132 S. Ct. at 957.

New technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34; *see also United States v. Warshak*, 631 F.3d 266, 285 ("the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish"). Just as the Sixth Circuit has concluded that email must be afforded the same constitutional protection as postal mail, even though it is stored with a third party, so, too, should this Court find that the constitution protects individuals from warrantless cell phone tracking. The Sixth Circuit protected email because "otherwise, the Fourth

Amendment would prove an ineffective guardian of private communication." *Warshak*, 631 F.3d at 286. If this Court holds that cell phone tracking falls outside of the ambit of the Fourth Amendment, the Supreme Court's decision in *Jones* will 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., concurring) and 963-964 (Alito, J., concurring in the judgment).

This Court should reject the government's invitation to apply *Miller* and *Smith* to this case because the exposure of cell phone location data to a cell phone provider is nothing like the direct conveyance of phone numbers to an operator or bank documents to a teller. In both *Miller* and *Smith*, the relevant documents and dialed numbers were directly and voluntarily conveyed to bank tellers and telephone operators, or their automated equivalents. *See, e.g.*, *Smith*, 442 U.S. at 744. Put simply, the phone customer knew what numbers he was exposing to the phone company; the bank customer knew what documents he was exposing to the bank. When a cell phone user makes or receives a call, there is no indication to the user that making or receiving that call will also locate the caller.[7] Nor does this

[7] Contrary to the government's assertion, Gov't Br. at 22, the Court in *Smith* did not assume that telephone subscribers understood the technical design of telephone networks. Instead, it analyzed whether a typical telephone user realized that using a telephone involved conveying phone numbers to the telephone company. *Smith*,

location information appear in the typical cell user's bill, a critical fact in *Smith*. *Id.* at 742 ("All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").

Moreover, not only do cell phone owners not know that their location is being communicated to the cell phone companies, they do not communicate their location to the cell phone company of their own volition. Unlike the customer in *Smith*, who made the choice to communicate the telephone numbers he called to his phone company by dialing them on his telephone, or the customer in *Miller*, who chose to give copies of checks to his bank, cell phone customers never affirmatively communicate their location to cell phone companies.

Finally, like the email at issue in *Warshak* and as the Third Circuit found when it addressed historical cell phone location data, individuals retain a privacy interest in their location data. *Warshak*, 631 F.3d at 266 ("*Miller* involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue here."); *Third Circuit Opinion*, 620 F.3d at 318-19 (recognizing that individuals can have a reasonable expectation of privacy in cell phone location data). This case, too, does not involve simple business records. The government has asked for a transcript of an individual's movements for 60

---

442 U.S. at 742 ("[W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial.").

days. Given the Supreme Court's ruling in *Jones* that individuals have a reasonable expectation of privacy in their long-term movements in public places, *see supra* at II.A, this Court should not apply *Miller* and *Smith* to cell phone location data.

The government attempts to forestall this conclusion by relying on T-Mobile's and MetroPCS's terms of service, Gov't Br. at 20-21, but even if T-Mobile and MetroPCS customers actually read and understand these companies' privacy policies, Gov't Br. at 19-20, they may—and, in amici's view, do—still maintain an expectation of privacy in the location of their phones. Email users may understand that their email provider stores copies of their email content, and may be subject to terms of service or privacy policies making clear that the provider may access that content in the ordinary course of business. Yet in *Warshak*, the Sixth Circuit had no difficulty concluding that email users maintain an expectation of privacy in their emails, even though the email provider's contract with the user made clear both the provider's ability and right to access those emails in certain circumstances.[8] *Warshak*, 631 F.3d at 286-88 (holding that the

[8] In a footnote, Gov't Br. at 23 n.5, the government argues that it is improper for this Court to conduct an inquiry into whether individuals voluntarily convey location data to cell phone companies, but the reasoning of the cases the government cites concerning third party subpoenas do not support its argument. In *Miller*, it was only *after* concluding that defendant Miller had no privacy expectation in the bank records at issue that the Court concluded that the traditional subpoena rules would apply. *Miller*, 425 U.S. at 442-46; *see also id.* at 444

government needed to obtain a warrant and demonstrate probable cause to access email, despite terms of service that permitted the provider to access emails in some circumstances); *United States v. Paige*, 136 F.3d 1012, 1020 n.11 (5th Cir. 1998) ("[A] homeowner's legitimate and significant privacy expectation . . . cannot be entirely frustrated simply because, *ipso facto*, a private party (e.g., an exterminator, a carpet cleaner, or a roofer) views some of these possessions."); *United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997) (individuals have a reasonable expectation of privacy in their hotel rooms even though management has a right to enter); *United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009) (tenants have reasonable expectation of privacy in their apartments even though landlords have a right to enter).

The government then cites to a number of cases in which courts have applied

---

("*Since no Fourth Amendment interests of the depositor are implicated here*, this case is governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant[.]") (emphasis added). In the government's second case, *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984), targets of an SEC investigation sought injunctive relief to require prior notice of SEC subpoenas to third parties, so they could assert their Fourth Amendment rights. *O'Brien*, 467 U.S. at 739. Only after concluding that the targets lacked a reasonable expectation of privacy in bank records subpoenaed by the SEC did the Supreme Court conclude that the targets were "disable[d] . . . from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers." *Id.* at 743. The necessary implication of this ruling is that such an argument does exist and was not rejected by the Supreme Court. Otherwise, an analysis of whether the targets possessed reasonable expectations of privacy in the records would have been unnecessary. The Supreme Court did not rule on that argument, and therefore did not rule it out.

the third party doctrine, but these cases either involve factual circumstances that bear little resemblance to obtaining cell phone location data or are district court decisions that this Court need not and should not follow. Gov't Br. at 24-26. Moreover, none of these cases are as persuasive as the *Third Circuit Opinion*, which, as discussed above, held that the third party doctrine does not apply to requests for historical cell phone location data. 620 F.3d at 317.

In *Hoffa v. United States*, the Supreme Court held that an individual's statements to a confidential informer were not protected from disclosure under the Fourth Amendment, but that was because the statements were made knowingly and voluntarily to the informer. 385 U.S. 293, 302 (1966). As the Third Circuit has described, there is nothing knowing and voluntary about the conveyance of cell phone location data to cell phone companies. *Third Circuit Opinion*, 620 F.3d at 317. For the same reason, the Tenth Circuit's decision regarding subscriber information (*i.e.*, name, address) is of no relevance here. *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008).

The government also cites *Donaldson v. United States*, 400 U.S. 517 (1971), but that case does not even involve a Fourth Amendment claim, *id.* at 522, and in any event, both it and another of the government's cases, *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984), involve access to financial records that, as in *Miller*, trigger no privacy expectation. Both *Reporters Committee for Freedom of the*

Press v. AT&T, 593 F.2d 1030 (D.C. Cir. 1978), and *Newfield v. Ryan*, 91 F.2d 700 (5th Cir. 1937) are based on outdated understandings of the Fourth Amendment. *Reporters Committee* addressed the Fourth Amendment interest in dialed telephone numbers before the Supreme Court issued its decision on this exact topic in *Smith*. 442 U.S 735. *Newfield* addressed the privacy of telegrams, 91 F.2d at 704, but it was decided before the Supreme Court established the *Katz* "reasonable expectation of privacy" test in 1967, a case in which the Supreme Court also held that the Fourth Amendment protects the privacy of telephone conversations. *Katz*, 389 U.S. at 350-54.

Moreover, while the Ninth Circuit did hold that to/from email and Internet Protocol ("IP") addresses are not protected by the Fourth Amendment, it reached this conclusion on the grounds that these bits of information "constitute addressing information," and expressly cautioned that its opinion "does not imply that more intrusive techniques or techniques that reveal more content information are also constitutionally identical to the use of a pen register." *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008). As amici explained above, cell phone tracking is exactly such a technique. Finally, the government cites a number of district court opinions that have adopted its argument but as it points out other district court opinions have held that a warrant is required. Gov't Br. at 25-26.

The government argues that the business record cases override the location

privacy cases, but the authority it cites for this proposition does not sweep so broadly. In *Smith*, the Court held that individuals have no Fourth Amendment protection against the use of a pen register, which can reveal that a telephone number was dialed inside a home. Gov't Br. at 27-28 (comparing *Smith* with *Karo*). But pen registers present the unique circumstance of revealing only a piece of information in which individuals have no privacy interest. In this respect, use of a pen register is like a dog sniff, which the Court has held presents a special case because it "discloses only the presence or absence of narcotics, a contraband item" in which individuals can have no expectation of privacy.[9] *United States v. Place*, 462 U.S. 696, 707 (1983). Cell phone location data does not fall into this narrow exception, because they indicate far more than unlawful activity, and instead implicate strong privacy interests.

Particularly considering the recent *Third Circuit Opinion* and the decision in *Warshak*, the district court was correct to conclude that cell phone users maintain a

[9] The government faults the magistrate judge for relying in part on the Wireless Communication and Public Safety Act of 1999 to find a reasonable expectation of privacy, but it is wrong to suggest that statutory law is irrelevant to an analysis of whether individuals possess a reasonable expectation of privacy in certain information. Gov't Br. at 28-29. While the existence of a statute *without more* is not sufficient to show that a particular type of information it safeguards is protected under the Fourth Amendment, *Quon*, 130 S. Ct. at 2634, it nonetheless helps support a conclusion that an individual's expectation of privacy in that information is reasonable. *See, e.g.*, *Doe v. Broderick*, 225 F.3d 440, 450-51 (4th Cir. 2000) (criminal statute prohibiting release of medical records is "relevant to the determination of whether there is a 'societal understanding' that [a patient] has a legitimate expectation of privacy in his treatment records.").

reasonable expectation of privacy in their cell phone location data regardless of the purported third-party rule of *Smith* and *Miller*. To the extent this Court disagrees, however, the appropriate course would be to uphold the denial of the government's application based on the discretion granted under § 2703(d) in order to avoid unnecessarily addressing this undeniably serious constitutional question.

C. The Compulsory Process Cases Do Not Change The Result.

Considering cell phone users' reasonable expectation of privacy in cell phone location data, the district court was correct to conclude that the government must obtain a search warrant based on probable cause before obtaining such private information. The government takes issue with this conclusion, analogizing § 2703(d) orders to subpoenas and arguing that regardless of a cell phone user's expectation of privacy, it need only satisfy a reasonableness standard to compel production of cell phone location data from a cell phone provider. Gov't Br. at 30-34. The government's analogy to traditional subpoenas is inapt because here, the person with a constitutional privacy interest in the records that the government seeks to obtain—the cell phone user—will not be notified of the compulsory process at issue, and therefore will have no opportunity to contest the order's reasonableness prior to the disclosure.

Courts have consistently recognized that a warrant requires probable cause, though a subpoena does not, because a search and seizure conducted pursuant to a

warrant is immediate and provides no opportunity for judicial review in advance, while a subpoena can be contested in court prior to enforcement. *See, e.g.*, *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) (holding that while a subpoena can issue without a warrant, the subpoenaed party is protected because it can "question the reasonableness of the subpoena, before suffering any penalties for refusing to comply with it, by raising objections in an action in district court" (internal citations omitted)); *Zurcher v. Stanford Daily*, 436 U.S. 547, 561 (1978) (assuming that "the subpoena *duces tecum*, offer[s] . . . the opportunity to litigate its validity" before compliance); *See*, 387 U.S. at 544-45; *Okla. Press Publ'g Co. v. Walling*, 327 U.S. 186, 195, 217 (1946).

Where—as here—the government secretly seeks to compel the disclosure of information through a third party, and the target possesses a Fourth Amendment-protected reasonable expectation of privacy, the government prevents the target from contesting the reasonableness of the government's demand. As one district court has noted, "[t]he very existence of a right to challenge [a compelled disclosure] presupposes an opportunity to make it. That opportunity [will be] circumvented, frustrated and effectively foreclosed by the methods employed here." *In re Nwamu*, 421 F. Supp. 1361, 1365 (S.D.N.Y. 1976). Such an invasion of an expectation of privacy, without any opportunity for the holder of that expectation to challenge the invasion, is indistinguishable from—indeed, is—a

search requiring a probable cause warrant.

Here, the cell phone user has a Fourth Amendment-protected reasonable expectation of privacy in the cell phone location data that is sought by the government. The *Third Circuit Opinion* assumed that the Fourth Amendment would require probable cause to the extent that cell phone location data sought with a § 2703(d) order would implicate a constitutionally-protected privacy interest. *Third Circuit Opinion*, 620 F.3d at 312-313; *see also id.* at 320 (Tashima, J., concurring). Even more recently, the Sixth Circuit in the *Warshak* case had no difficulty in holding that a §2703(d) order to an email provider requesting emails in which the customer maintained a reasonable expectation of privacy would violate the Fourth Amendment, despite the government's pressing the same "reasonableness" argument that it does here. Supplemental Resp. of the United States to Section II of Defs.' Omnibus Pretrial Mots. at 4-9, *United States v. Warshak*, 631 F.3d 266. After deciding that email users possess a reasonable expectation of privacy in the emails they store with third party email providers, the *Warshak* court concluded that "it is manifest that agents of the government cannot compel a commercial ISP ("Internet Service Provider") to turn over the contents of an email without triggering the Fourth Amendment," and "[i]t only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment

search, which necessitates compliance with the warrant requirement absent some exception." 631 F.3d at 286.

Particularly considering such precedent, the compelled disclosure of third party materials in which a target maintains a reasonable expectation of privacy, without the target receiving any notice or opportunity to challenge the government's demand, is a Fourth Amendment search requiring probable cause. Indeed, because the Supreme Court has yet to directly address this argument, there remains a serious constitutional question justifying the exercise of a court's discretion under § 2703(d) to deny the government's application and thereby avoid the issue.

III. THE MAGISTRATE JUDGE'S FACTUAL FINDINGS ARE NOT BEFORE THIS COURT, AND EVEN IF THEY WERE, NEITHER LOWER COURT COMITTED REVERSIBLE ERROR.

The government asks this Court to reverse the district court on the basis of factual findings the magistrate judge—not the district court judge—made in the course of issuing an opinion, *see* Gov't Br. at 41-46. Those factual findings are nowhere cited, let alone relied upon, by the district court judge.

Even if this Court reviews the magistrate judge's "findings of facts," there is no reversible error. The government's argument that the magistrate judge did not satisfy Federal Rule of Evidence 201 is a red herring because, as the government itself almost concedes, *see* Gov't Br. at 41 n.11, the Federal Rules of Evidence

("FRE") are not applicable to courts' consideration of government applications for cell phone location data. And in turn, there can be no error by the magistrate judge for failing to meet the "reasonable dispute" standard in FRE 201. Likewise, because FRE 201 does not apply, the judicial notice standard does not place any limits on the magistrate judge's fact finding. As a result, this Court must review the magistrate's "findings of facts" for clear error. Because there is none, the "findings of facts" cannot be a basis for reversal.

A. The Magistrate's Findings Of Facts Are Not Before This Court.

At the outset, it should be clear that the "findings of facts" the government complains about were made by the magistrate judge, not the district court, whose order is uniquely under review by this Court. *See Magistrate Judge Opinion*, 747 F. Supp. 2d at 831. The district court did rely on certain facts, specifically that the records at issue "would show the date, time, called number, and location of the telephone when the call was made." (R. 43). But these facts are undisputed. In fact, they were put into evidence by the government itself. *See* (A. 49). The government cannot disown them now. Thus, any complaint by the government about these facts is not before this Court.

B. Since, As The Government Has Essentially Conceded, The Federal Rules Of Evidence Do Not Apply To § 2703(d) Proceedings, The Magistrate Judge's "Findings of Facts" Did Not Violate FRE 201's "Reasonable Dispute" Requirement.

Even if this Court were to find that the district court judge accepted the magistrate judge's "findings of facts" as his own, there is no FRE violation. In its brief, the government comes close to conceding that the Federal Rules of Evidence do not apply in this case at all. *See* Gov't Br. at 41 n.11 ("Although Rule 201 may not apply to an application for a 2703(d) order…"). It should have gone all the way. Since the FRE do not apply to § 2703(d) orders, the government's claim that the magistrate judge's "findings of facts" fail FRE 201(b)'s "reasonable dispute" requirement is clearly wrong.

Federal Rule of Evidence 1101(d) addresses when the FRE do not apply:

> The rules (other than with respect to privileges) do not apply in the following situations:
>
> (1) Preliminary questions of fact. The determination of questions of fact preliminary to admissibility of evidence when the issue is to be determined by the court under rule 104.
>
> (2) Grand jury. Proceedings before grand juries.
>
> (3) Miscellaneous proceedings. Proceedings for extradition or rendition; preliminary examinations in criminal cases; sentencing, or granting or revoking probation; issuance of warrants for arrest, criminal summonses, and *search warrants*; and proceedings with respect to release on bail or otherwise.

Fed. R. Evid. 1101(d) (emphasis added). While the list does not include applications for § 2703(d) orders, that does not mean the rules apply to these applications. A number of courts have concluded that the list is illustrative rather

than exclusive. *See United States v. Frazier*, 26 F.3d 110, 113 (11th Cir. 1994); *United States v. Singer*, 345 F. Supp. 2d 230, 234 (D. Conn. 2004); *United States v. Weed*, 184 F. Supp. 2d 1166, 1173 (N.D. Okla. 2002).

Amici can find no cases squarely addressing whether the Federal Rules of Evidence apply when courts consider § 2703(d) orders. However, there are good reasons to conclude that the evidence rules are inapplicable. Search warrants are expressly exempt from Federal Rule of Evidence 1101(d)(3) because, as the advisory committee explained, the "nature of the proceedings makes application of the formal rules of evidence inappropriate and impracticable." Fed. R. Evid. 1101, Advisory Committee's Note to Subdivision (d). The same holds true for § 2703(d) applications. These applications are often time-sensitive, and it would neither be practical nor in some cases even possible for the government to comply with the evidence rules.

For example, the prohibition on hearsay would mean that agents would not be able to recite in affidavits the information provided to them by confidential informants. Rather, the informants themselves would have to provide testimony, which would itself be limited by the hearsay rule. Applying the evidence rules to applications for cell phone location data would invalidate the government's longstanding practice, previously unquestioned by courts, of relying on hearsay-laden affidavits of law enforcement agents as a basis for applications to obtain cell

phone location data. *See, e.g., In re Application of U.S. for an Order: (1) Authorizing Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Info.; and (3) Authorizing Disclosure of Location-Based Servs.*, 727 F. Supp. 2d 571 (W.D. Tex. 2010) (affidavit accompanied cell site application).

In *Frazier*, the Eleventh Circuit held that even though hearings on supervised release were not specifically mentioned in Federal Rule of Evidence 1101(d), they are sufficiently similar to probation and parole hearings which Rule 1101(d) exempts that it was appropriate to exempt supervised release hearings as well. *Frazier*, 26 F.3d at 113. In a similar vein, this Court should analogize between search warrants and § 2703(d) applications and conclude that the evidence rules do not apply to adjudications of either one.

The government's primary complaint about the "findings of facts" is that they are subject to "reasonable dispute," and thus inappropriate for judicial notice under Federal Rule of Evidence 201(b). *See* Gov't Br. at 41. But since, as demonstrated above, the FRE do not apply, the "findings of facts" could not have violated FRE 201's reasonable dispute requirement.

C. Even If This Court Decides To Review The "Findings of Facts," The Magistrate Judge Did Not Commit Clear Error.

The government confuses the standard of review to apply to this issue, but reviewing under the correct "clear error" standard, the magistrate judge's "findings of facts" survive.

1. The Correct Standard Of Review Is "Clear Error," Not Abuse Of Discretion.

Clinging to the incorrect notion that the FRE applies, the government claims the proper standard of review for the magistrate judge's factual findings is "abuse of discretion." *See* Gov't Br. at 3 (citing *Taylor v. Charter Med. Corp.*, 162 F.3d 827, 829 (5th Cir. 1998)). Yet, in another portion of its brief, the government analogizes § 2703(d) orders to suppression hearings. *See* Gov't Br. at 41 n.11.

Factual findings in a suppression hearing are reviewed under the "clear error" standard, not an "abuse of discretion" standard. *United States v. Howard*, 106 F.3d 70, 73 (5th Cir. 1997). A "factual finding is clearly erroneous 'when although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed.'" *Id.* (quoting *Anderson v. City of Bessemer City*, 470 U.S. 564, 573 (1985)).

Applying the correct standard, this Court cannot be left with "the definite and firm conviction" that the magistrate judge made an error, or that the district court was wrong to accept his findings of facts.

2. The Magistrate Judge's Factual Determinations Were Proper.

The magistrate judge based its "most significant findings" on expert testimony given to Congress by University of Pennsylvania professor Matt Blaze. *Magistrate Judge Opinion*, 747 F. Supp. 2d at 830.[10] But that was not the only source the magistrate judge referenced; it also cited the DOJ's own Electronic Surveillance Manual, and surveys from The Wireless Association ("CTIA"), the leading cellular phone trade group. *Id.* at 831-35. And the government cannot point to anything in these "findings of facts" that leaves this Court with a "the definite and firm conviction" that the magistrate committed a mistake.[11]

[10] Professor Blaze has a Ph.D. in Computer Science from Princeton University, 12 years of industry experience, and his academic focus is "the properties and capabilities of surveillance technology." *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 1-2 (2010) (statement of Professor Matt Blaze), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf.

[11] The government claims that the "findings of facts" were contradicted by the sworn affidavit of MetroPCS, *see* Gov't Br. at 44-45, but it is wrong. For example, the magistrate judge found "[s]ome carriers also store frequently updated, highly precise, location information not just when calls are made or received, but as the device moves around the network." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 833-34. The government argues this contradicts MetroPCS's affidavit which states it "'do[es] not currently create and store cell-site information unless a call is made,' that MetroPCS stores only a record of the tower the phone was connected to at the beginning and end of the call, and that MetroPCS does not store cell-site records when a phone is idle." Gov't Br. at 44-45 (quoting (A. 110-12)). But there is no contradiction because the "findings of fact" are qualified: it states "some carriers" – not all – store more precise information.

More importantly, however, the government misconstrues the ultimate conclusion in the "findings of fact." The majority of the government's complaint centers on the precision of cell phone location data. *See* Gov't Br. at 44-45. It argues that the "findings of facts" are inconsistent with a 2007 case and a 2000 FCC opinion about the accuracy of cell phone towers. *See* Gov't Br. at 45-46. But the magistrate's decision was not based on the specific precision of MetroPCS or T-Mobile technologies. Instead, the magistrate judge looked to the future and the inevitable technological advances to come, noting "[e]ven if an exact latitude and longitude is not yet ascertainable or recorded for every single mobile call, network technology is inevitably headed there." *Magistrate Judge Opinion*, 747 F. Supp. 2d at 837.

In other words, the magistrate's "findings of facts" amounted to a conclusion that the precision of cell site towers is improving, getting more accurate and leading to a greater ability of law enforcement to identify an individual's location over an extended period of time. This forward-looking approach makes sense because the 2000 and 2007 opinions cited by the government are ancient history given the rapid change of technology. *See Jones*, 132 S.Ct. at 963 (Alito, J., concurring in the judgment) ("For older phones, the accuracy of the location information depends on the density of the tower network, but new 'smart phones,' which are equipped with a GPS device, permit more precise tracking."). And the

Supreme Court has cautioned, "[w]hile the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36.

The only "definite and firm conviction" to take from the magistrate judge's "findings of facts" is that he was not mistaken about the rapid changes in technology that make it easier than ever before for the government to obtain precise cell phone location data. This factual determination does not merit reversal.

CONCLUSION

Justice Sotomayor has warned about the dangers of location tracking information, "a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent 'a too permeating police surveillance.'" *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). The lower courts elevated privacy at a minimal cost to effective law enforcement by simply requiring the government to obtain a search warrant in order to obtain the specific location tracking information – cell phone location data – that it wanted. This Court should protect privacy and reinforce the Fourth Amendment in a time of rapid technological change. The lower courts should be affirmed.

/s/ *Catherine Crump*
Catherine Crump
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500

/s/ *Hanni Fakhoury*
Hanni Fakhoury
Matthew Zimmerman
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

/s/ *Lisa Graybill*
Lisa Graybill
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF TEXAS
P.O. Box 12905
Austin, TX 78711
(512) 478-7300 ext. 116

/s/ *Cynthia E. Orr*
Cynthia E. Orr
Bar No. 15313350
GOLDSTEIN, GOLDSTEIN & HILLEY
310 S. St. Mary's St.
29th Floor Tower Life Bldg.
San Antonio, Texas 78205
(210) 226-1463

March 16, 2012

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 13,867 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Microsoft Office Word 2010 in 14-point Times New Roman font.

3. All required privacy redactions have been made.

4. The ECF submission is an exact copy of the hard copy submissions, and

5. The digital submission has been scanned for viruses with the most recent version of Symantec Endpoint Protection, version 12.1.1, updated March 16, 2012, and according to that program, is free of viruses.

/s/ *Catherine Crump*
Catherine Crump
American Civil Liberties Union

Dated: March 16, 2012

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fifth Circuit by using the appellate CM/ECF system in No. 11-20884 on March 16, 2012.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ *Catherine Crump*
Catherine Crump
American Civil Liberties Union

Dated: March 16, 2012