NO. 11-20884

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

IN RE: APPLICATIONS 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
Related Cases: 4:10-MJ-981, 4:10-MJ-990, 4:10-MJ-998

BRIEF OF AMICUS CURIAE SUSAN FREIWALD
IN SUPPORT OF AFFIRMANCE

Susan Freiwald
Professor of Law
University of San Francisco School of Law
2130 Fulton Street
San Francisco, CA 94117
(415) 422-6467
(415) 422-6433

STATEMENT REGARDING ORAL ARGUMENT

Amicus requests the opportunity to participate in oral argument, should this Court decide oral argument would be helpful.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST

Amicus is a law professor who teaches and writes scholarship in the areas of Cyberspace Law and Information Privacy Law. She has written several law review articles on how the Fourth Amendment and the federal surveillance statutes should apply to new communications technologies. She has also submitted amicus briefs in cases addressing the Fourth Amendment's application to newly emerging electronic surveillance techniques including in the Sixth Circuit regarding the Fourth Amendment protection of stored email. Amicus submitted amicus briefs in the Western District of Pennsylvania and the Third Circuit addressing the Fourth Amendment protection of location data as well as in the District Court below. Amicus has no stake in the outcome of this case, but is interested in ensuring that electronic privacy law develops with due regard for the vital role electronic communications play in our lives.

SUMMARY OF ARGUMENT

Government acquisition of historical cell-site records ("location data" or "location information") constitutes a search under the Fourth Amendment. Like the GPS tracking information the Supreme Court considered in *United States v. Jones*, 132 S. Ct. 945 (2012), location data reveals intimate information about users' personal lives and intrudes on reasonable expectations of privacy. As with wiretapping, acquisition of location data is hidden, continuous, indiscriminate, and

intrusive. As a result, such acquisition must be subject to the extensive judicial oversight that the warrant requirement provides. Contrary to the government's claim of a broad third-party rule, cell-phone providers' storage of location data does not detract from reasonable expectations of privacy. Acquisition of historical records intrudes on reasonable expectations of privacy as much as does real time monitoring; in fact, there may be no practical difference between the two. Because the government claims the ability to acquire location data without first procuring a warrant based on probable cause, this Court should affirm the District Court's order overruling the government's objections to Magistrate Judge Smith's denial of the government's applications. *In re Application of the United States of America for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010) (hereinafter "*Smith Opinion*").

ARGUMENT

I. GOVERNMENT ACQUISITION OF LOCATION INFORMATION IS A SEARCH UNDER THE FOURTH AMENDMENT

When the "government violates a subjective expectation of privacy that society recognizes as reasonable," it conducts a Fourth Amendment search. *Jones*, 132 S. Ct. at 954-55 (Sotomayor, J., concurring); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Because government agents intrude upon a cell phone user's reasonable expectation of privacy when they acquire his

location data, they must either obtain a warrant based on probable cause or establish an exception to the warrant requirement. The Supreme Court made clear in *Jones* that users have a subjective expectation of privacy in location data, notwithstanding that the data reveals activities in public. Applicable precedents, including *Jones*, also support an objective expectation. Because law enforcement agents acquire location data in a manner that is hidden, continuous, indiscriminate and intrusive, it is a practice, like wiretapping, that requires extensive judicial supervision to protect Fourth Amendment rights.

A. The Nature of Location Data

Before a court can assess reasonable expectations of privacy in location data, it must understand what location data is. In the present case, the government has argued that location data does not implicate constitutional privacy rights, *see* Brief for the United States 35-41 (2/15/2012) (hereinafter "Gov. Brief"), but it has not provided a clear statement on what the location data it seeks would reveal, and how the government can be sure that its acquisition will not intrude on privacy interests, particularly in light of the *Jones* decision. The government does not explain how the location data it seeks would be useful in its investigations but not intrusive enough to implicate the Fourth Amendment. The government suggests that a remand may be necessary if this Court has concerns about the nature of location

data.[1] Gov. Brief at 35.

This Court does not need to remand, because it may and should determine, as a matter of law, that acquisition of location data is a search under the Fourth Amendment. This Court has enough information to determine that a warrant is required when law enforcement agents acquire location data. The comprehensive opinions below,[2] other cases involving location data, and the government's applications in this litigation all mandate that holding.

In a recently published law review article on cell site location data, I described the myriad factors that make the acquisition of location data intrude on private activities. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 702-16 (2011) (hereinafter "Freiwald, *Location Data*"). Specifically, as more location data points are collected in the same time frame, they paint an increasingly rich and complete picture of where a target has been. Location data richness has increased dramatically as, in addition to location data at the start and end of calls, location

[1] In the only other federal appellate case to consider Fourth Amendment protection for location data, the court remanded to develop the factual record. *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, 319 (3d Cir. 2010), *pet. for reh'g en banc denied* (3d Cir. Dec. 15, 2010) (hereinafter "*Third Circuit Opinion*"). Before a new hearing was conducted, the government abandoned its application. *See* Order, No 07-524m (filed on 08/09/11) (noting the government's withdrawal of its application for cell site location records and denying the government's request to seal that document.)

[2] I will not repeat the excellent arguments made by amici in support of the *Smith Opinion*. *See* Brief of American Civil Liberties Union, the ACLU Foundation of Texas, the Electronic Frontier Foundation, and the Center for Democracy and Technology, Part III (filed March 16, 2010).

data is collected during a call (duration data) and when phones periodically register with nearby cell sites (registration data). *See* Freiwald, *Location Data*, at 704-08. The Government has requested registration and duration data in several recent cases. *See*, *e.g*., *Third Circuit Opinion*, 620 F.3d at 308 (quoting application as seeking "without limitation . . . call handoffs, registrations and connection records"); *United States v*. *Benford*, No. 2:09 CR 86, 2010 WL 1266507, *1 (N.D. Ind. Mar. 26, 2010) (describing the information sought as data "identifying which cell tower communicated with the cell phone while it was turned on"); *In the Matter of the Application of the United States For And [sic] Order: (1) Authorizing Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services*, 727 F. Supp. 2d 571, 579 (W.D. Tex. 2010) (hereinafter "*Austin Opinion*") (describing government's application as seeking "*the exact location of the Target Devices* (differentiated from the first or last cell-site used to make or receive a call, which simply identifies the location of the third party Provider's infrastructure)").

The government's applications in this case requested both registration data and duration data. They sought registration information, or "continuous location data to track the target phone over a two month period, whether the phone was in active use or not." *Smith Opinion* at 829; *see also id*. at 841 ("Clearly, these

requests seek the phone's location not only at the beginning and end of calls, but also 'registration' information as the phone moves about the network.") In addition, the government requested duration information, or "cell site information, [to be] provided to the United States on a continuous basis for (a) the origination of a call …, (b) the termination of the call and (c) if reasonably available, during the progress of the call. . . ." *See, e.g.*, Application at 3, 4:10-mj-00998 (filed on 10/12/10) (unsealed per order of Feb. 12, 2012).[3]

The government relies on MetroPCS's affidavit to support its claim that the provider stores only call initiation and termination data. *See* Gov. Brief at 11. That affidavit, however, specifically states that it "does not address information produced by MetroPCS in response to a prospective court order, such as a pen/trap order, prospective warrant, or wiretap order." Affidavit of Jarret Guill on Behalf of MetroPCS Texas, at ¶3, 4:10-mj-00998 (filed on 12/3/10). As just described, the government's application requested a court order compelling MetroPCS to create records on a continuous basis. MetroPCS, like T-Mobile, was to receive and store the location records as they were generated and then deliver them to the government.[4] *See* 990 Application at 3 n.5 ("'After receipt and storage' is intended

[3] The other two applications contain similar language. *See* Application at 2, 4:10-mj-00981 (filed on 10/05/10) (unsealed per order of Feb. 10, 2012); Application at 3, 4:10-mj-00990 (filed on 10/06/10) (unsealed per order of Feb. 9, 2012) (hereinafter "990 Application").

[4] *Cf. United States v. Warshak*, 631 F.3d 266, 335 (6th Cir. 2010) (Keith, J., concurring) (regarding prospective order for records as "no more than "back-door wiretapping").

to ensure that the information authorized under these paragraphs is information that is first captured and recorded by the provider before being sent to the Investigative Agency.")[5] Notwithstanding the affidavit, therefore, and assuming that MetroPCS views a court order requesting such forward-looking information to be a prospective court order, the government's applications could well have generated exceedingly detailed duration information compiled throughout the progress of a call.

In addition, carriers have been collecting data generated during use of newer technologies, such as texting. *See In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011) (hereinafter "*E.D.N.Y. Opinion*"). Because text messages are sent so much more frequently than calls are made, collecting location data for text messages dramatically increases the richness and intrusiveness of the data. Freiwald, *Location Data*, at 708-09. Although the applications do not request text message data in this case, they do ask for cell location data associated with two-way radio communications. *Smith Opinion,* 747 F. Supp. 2d at 829.

[5] The records are to be provided to the United States "on a continuous basis" "after receipt and storage" and are described in a separate section from the section describing the records that have already been generated and stored for the preceding 60 days. *See, e.g.,* 990 Application at 2-3.

Data precision also depends on the density of towers (which has been growing over time), on mathematical techniques (such as triangulation), and on the use of new cell technologies that increase accuracy. *See* Stephanie Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards For Law Enforcement Access to Location Data that Congress Could Enact*, BERK. TECH. L. J. *15 (forthcoming 2012), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1845644 (describing the recent rollout of hundreds of thousands new cell site technologies that increase the accuracy of single cell site location data significantly and in some cases make it even more accurate than GPS data). In the applications, below, the government requested cell sector data, *Smith Opinion*, 747 F. Supp. 2d at 829, which reduces the area in which a target may be found around a cell site from a circle emanating outward to a pie-slice. Use of sector information increases the precision of the location data and its ability to tie the target to the location of the cell tower.

In his opinion, Magistrate Judge Smith considered cell phone technology as it exists now and is developing. In doing so, he followed the instructions of the Supreme Court. *See United States v. Kyllo*, 533 U.S. 27, 36 (2001) ("While 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."); *see also id*. at 40 (rejecting the idea that the constitutionality of the

surveillance should be judged on the basis of what occurred in the case at bar, and instead requiring courts to "take the long view" and give "clear specification of those methods of surveillance that require a warrant"); *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (describing GPS tracking as a "tool . . . amenable to misuse.").

In sum, location data in general and in this litigation in particular is rich and precise enough to provide a complete and detailed portrait of a target's activities. *See, e.g., Austin Opinion*, 727 F. Supp. 2d at 582 ("[R]eceipt of [location data] will permit the government to 'follow' the phone user's movements 24 hours a day, 7 days a week, wherever they go, whatever they are doing."). Based on the subjective and objective expectations of privacy in location data, to which I next turn, this Court should agree with the District Court below that the acquisition of location data intrudes on reasonable expectations of privacy, constitutes a search under the Fourth Amendment and requires the protections of the warrant requirement.

B. Subjective Expectations of Privacy in Location Data

Most cell phone users would be unpleasantly surprised, if not outraged, to learn that a law enforcement agent could gain access to their location data without first obtaining a warrant based on a showing of probable cause. Location data, whether the product of GPS monitoring or cell site location data acquisition,

"generates a precise, comprehensive records of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); *Smith Opinion*, 747 F. Supp. 2d at 838 (describing location data sought by the government as providing "not a single snapshot at a point in time, but a continuous reality TV show, exposing two months' worth of a person's movements, activities and associations in relentless detail.") Knowledge that the government keeps track of such information could easily inhibit valuable and constitutionally protected activities. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (expressing concern about the chilling impact of government "watching" on "associational and expressive freedoms").

Citizens have a subjective expectation of privacy in their location data, and would not expect police to have access to it without first demonstrating a compelling justification to a reviewing court. Justice Alito's concurrence in *Jones*, joined by Justice Sotomayor, recognized as much in the related GPS context. 132 S. Ct. at 964 (Alito, J., concurring) ("[S]ociety'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."); *see also United States v. Karo*, 468 U.S. 705, 735 (1984) (Stevens, J., concurring in part and dissenting in part) ("As a general matter, the

private citizen is entitled to assume, and in fact does assume, that his possessions are not infected with concealed electronic devices.").

C. Objective Expectations of Privacy in Location Data

The objective prong of the reasonable expectation of privacy test ultimately requires this Court to make a normative finding about whether users should be entitled to view the object of the search as private. As Justice Harlan, author of the reasonable expectation of privacy test, explained: "The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens, the risks of the electronic listener or observer without at least the protection of a warrant requirement." *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). The critical question in this case is whether law enforcement agents may use cell phone technology as a means to conduct constant surveillance of our citizens without the procedural limits imposed by the Fourth Amendment. The answer must be "no."

In the *Warshak* case, the Sixth Circuit the court recognized that "[a]s some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise." *United States v. Warshak,* 631 F.3d 266, 286 (6th Cir. 2010). The court found that e-mail "plays an indispensable part in the Information Age," *id*., and that it "requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective

guardian of private communication, an essential purpose it has long been recognized to serve." *Id*. The *Warshak* court's recognition that "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish," *id*. at 285 (citing *Kyllo*, 533 U.S. 27, 34 (2001)), supports a finding of an objective expectation of privacy in location data. *See also E.D.N.Y. Opinion*, 809 F. Supp. 2d at 126 ("[E]stablished normative privacy considerations support the conclusion that the reasonable expectation of privacy is preserved here, despite the fact that cell-site-location records [are] disclosed to cell-phone service providers.").

By analogy, users have an objectively reasonable expectation of privacy in their location data. Just as the Supreme Court recognized that warrantless government eavesdropping violated the privacy on which the target "justifiably relied" while using the telephone booth, *Katz v. United States*, 389 U.S. 347, 353 (1967), so warrantless access to location data would violate the privacy on which cell phone users justifiably rely while using their cell phones. *Jones,* 132 S. Ct. at 964 (Alito, J., concurring) (finding that the GPS tracking in the case "involved a degree of intrusion that a reasonable person would not have anticipated.") When describing government acquisition of telephone conversations as a search under the Fourth Amendment, the Supreme Court in *Katz* reasoned that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has

come to play in private communication," 389 U.S. at 352. To deny Fourth Amendment protection to location data would similarly ignore the vital role that mobile telephony has come to play in the lives of the over 322 million wireless subscribers in the United States. *See* CTIA Consumer Info, 50 Wireless Quick Facts, http://www.ctia.org/consumer_info/index.cfm/AID/10323 *(*cited by *Jones,* 132 S. Ct. at 963 (Alito, J., concurring)).

D. Acquisition of Location Data Must be Subject to the Warrant Requirement Because it is Hidden, Continuous, Indiscriminate and Intrusive

Location data acquisition shares those features of other types of electronic surveillance that the Supreme Court and lower courts have found to require high procedural hurdles and extensive judicial oversight. In *Berger*, the Supreme Court explained that electronic eavesdropping techniques presented "inherent dangers" and therefore required more "judicial supervision" and "protective procedures" than even "conventional" searches. *See Berger v. New York*, 388 U.S. 41, 60 (1967); *see also id*. at 64 (noting that New York statute permitting eavesdropping with insufficient judicial oversight constituted a "general warrant" in violation of the Fourth Amendment).[6] When they determined that the Fourth Amendment required the same procedural hurdles for some uses of silent video surveillance,

[6] In fact, law enforcement agents seeking location data should perhaps satisfy the heightened procedural requirements imposed on government wiretappers. *See* Freiwald, *Location Data*, at 747-48.

several federal Courts of Appeal elaborated on which features necessitated heightened judicial oversight. Judge Posner, in a decision for the Seventh Circuit whose reasoning was widely followed, explained that the *hidden*, *continuous*, *indiscriminate*, and *intrusive* nature of electronic surveillance raises the likelihood and ramifications of law enforcement abuse. *See United States v. Torres*, 751 F.2d 875, 882-84 (7th Cir. 1984); *see id*. at 882 ("[I]t is inarguable that television surveillance is exceedingly intrusive … and inherently indiscriminate, and that it could be grossly abused – to eliminate personal privacy as understood in modern western nations.").

When government agents acquire location data they use a technique that is similarly hidden, continuous, indiscriminate and intrusive. Unlike the search of a home, which is usually subject to view either by the occupant of the home or his neighbors, government acquisition of location data is *hidden*. Just as a telephone user does not know when a law enforcement agent wiretaps his call, a cell phone user does not know when a law enforcement agent acquires his location information. That significantly raises the risk that agents will exceed the scope of a proper investigation with impunity. Justice Sotomayor raised the same concern with GPS monitoring in *Jones*. *See* 132 S. Ct. at 956 (Sotomayor, J., concurring) ("And because GPS monitoring … by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited

police resources and community hostility.'") (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004)).

In addition, location data reveals information over a *continuous* period, as do telephone conversations and video surveillance footage. The longer the period an investigation spans, the greater the likelihood that the government will conduct surveillance without sufficient justification. To address that risk, the Supreme Court required that electronic surveillance orders issue for a limited period of time and cease as soon as the constitutional justification ceases. To apply for a renewal, agents must satisfy the same requirements as those imposed on initial requests. *See Berger*, 388 U.S. at 59. When location data spans a period of time, such as the 60 day period the government requested in its applications, its acquisition should also be subject to constitutional limits.

Besides being hidden and continuous, acquisition of location data is inherently *indiscriminate* in that much of the information obtained will not be incriminating. Just as the wiretapping of traditional telephone calls acquires non-incriminating conversations and video surveillance footage includes numerous innocent scenes, location data may reveal many movements and activities that are entirely unrelated to criminal actions.

For example, in one of its applications below, the government requested location data for a subscriber whose phone was apparently *used by* the target of a

criminal investigation. *See* 990 Application at 2, 4; *see also In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 534 F. Supp. 2d 585, 588 & n.11 (W.D. Pa. 2008), *vacated and remanded*, 620 F.3d 304 (3d Cir. 2010) (describing the subscriber whose location data agents sought as having a cell phone apparently "used by" the target of the criminal investigation, but noting "no specific information connecting these two individuals."). The government appears to seek information about apparently innocent parties regularly. According to an industry lawyer, "With respect to location information of specific users, many orders now require disclosure of the location of all of the associates who called or made calls to a target." *See* Al Gidari, Jr., *Symposium: Companies Caught in the Middle, Keynote Address*, 41 U.S.F. L. Rev. 535, 557 (2007). The risk of acquiring information about non-incriminating activities mandates substantial judicial oversight to reduce unwarranted invasions of privacy and to ensure that searches not become government fishing expeditions. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("[T]he government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.")

As already discussed, law enforcement acquisition of location data has the potential to be extremely *intrusive* in that it may disclose a detailed record of a target's movements. The government's ability to draw inferences about a target's

activities from his movements enhances the intrusive nature of location data. As discussed above, uninvited and virtually constant government observation of one's movements implicates constitutional privacy rights, the right to travel, and First Amendment rights of association and expression. Though location information differs from telephone conversations and videotaped footage, its acquisition shares the intrusive character of wiretapping and video surveillance. Because of that, it must be subject to heightened requirements, and at least a warrant, so that the government does not needlessly intrude on valuable privacy rights. *See Jones*,132 S. Ct. at 956 (Sotomayor, J., concurring) (cautioning against the Executive acting free of oversight "in light of the Fourth Amendment's goal to curb arbitrary exercises of policy power and prevent a 'too permeating police surveillance'") (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

As the preceding discussion shows, government acquisition of location data shares the same features of wiretapping, bugging and silent video surveillance that make those investigative methods particularly invasive and particularly subject to abuse. In recognition of that, requiring that law enforcement agents demonstrate probable cause to a neutral magistrate before they may compel the disclosure of location data is the minimum constitutional safeguard.

II. THE GOVERNMENT DOES NOT ADVANCE A COMPELLING REASON NOT TO VIEW ACQUISITION OF LOCATION DATA AS A SEARCH

A. A Third Party Rule Does Not Govern Acquisition of Location Data

Contrary to the government's claim, *see* Gov. Brief at 16-28, no third party rule excuses the government from the constitutional requirement of a warrant. The Sixth Circuit persuasively limited application of any "third party" rule in the recent *Warshak* case, 631 F.3d 266, 288 (6th Cir. 2010), and the Third Circuit found it inapplicable to location data in its recent decision. *See Third Circuit Opinion*, 620 F.3d at 317-18. None of the government's arguments calls either persuasive precedent into question. The government fails to establish that either *United States v. Miller*, 425 U.S. 435 (1976), or *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), governs location data, particularly in light of Justice Sotomayor's discussion of those cases in *Jones*.

Essentially, the government urges this court to find records containing location data to be analogous to the bank records that the Supreme Court found unprotected by the Fourth Amendment in *Miller*. *See* Gov. Brief at 17-18 (relying on the *Miller* case). By characterizing location data as the "business records of the provider," *id*. at 17, the government presses for an analytical short-cut, by which some lower courts have rejected constitutional protection for "third party records" without fully conducting an inquiry into reasonable expectations of privacy. *See*

generally, Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. ¶36-¶44 (criticizing courts for using third party rule to avoid reasonable expectations of privacy analysis.) The government also claims that *Smith v*. *Maryland* precludes Fourth Amendment protection for location information because users voluntarily convey it to service providers in the same way that telephone users conveyed telephone numbers to the phone companies in 1979. Gov. Brief at 18-23.

The Third Circuit, which is the only federal appellate court to consider the Fourth Amendment regulation of historical location data, squarely rejected the application of both *Miller* and *Smith* to location data. *See Third Circuit Opinion*, 620 F.3d at 317. The Third Circuit rejected that idea that a cell phone user "voluntarily expose[s]" his location data in the same way that he exposes the telephone numbers that he dials. *Id*. at 317-18. The government disputes that holding, without directly confronting it, by arguing that users voluntarily expose their location data because they are purportedly aware that it is generated. *See* Gov. Brief at 20-21 (asserting that users know about their providers' location data uses). Whatever awareness users have of their providers' practices, however, they do not assume the risk that their location data will be retained and disclosed to government agents without a warrant. *See Jones*, 132 S. Ct. at 964 (Sotomayor, J., concurring) ("Those who disclose certain facts to a bank or phone company for a

limited business purpose need not assume that this information will be released to other persons for other purposes.") (quoting *Smith*, 442 U.S. at 747 (Marshall, J., dissenting)).

Moreover, because location data reveals so much more information than the limited information conveyed by dialed telephone numbers, the *Smith* decision is inapposite. *See, e.g., United States v. Forrester*, 512 F.3d at 500, 511 (9th Cir. 2008) (stating that its holding "does not imply that more intrusive techniques . . . are also constitutionally identical to the use of a pen register."). As discussed above, location data is much closer to the GPS data that the *Jones* Court found to be protected by the Fourth Amendment despite the fact that it is non-content data. *See Jones,* 132 S. Ct. at 964 (Sotomayor, concurring) (calling the approach in *Smith* and *Miller* "ill suited to the digital age").

In a similar context, the Sixth Circuit rejected the government's argument that a "third party rule" defeats an email user's expectation of privacy. According to the *Warshak* panel, an email user does not convey his email to his service provider to be put "to use 'in the ordinary course of business.'" *Warshak*, 631 F.3d at 288. Instead, the service provider is a mere "intermediary, not the intended recipient of the emails," whose access does not defeat the user's reasonable expectation of privacy. *See id*. (citing Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 165 (2008)).

Similarly, a cell phone service provider is much more like an intermediary who processes location data in order to facilitate cell phone users' communications with *other people*. Service providers are quite distinct from the bank in *Miller*, which the Supreme Court considered to be a party to the transactions with the defendant that generated the records. *See Miller*, 425 U.S. at 440-41 ("The records of respondent's accounts … pertain to transactions to which the Bank itself was a party.") The analogy that the Supreme Court drew between Miller's confiding in the bank and a person confiding in his friends, *id*. at 443, does not describe the way in which location data is generated. *See Smith Opinion*, 747 F. Supp. 2d at 844 ("Cell site data is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal.")

The *Warshak* panel persuasively reasoned that a user's consent to service provider access to email does not forfeit a reasonable expectation of privacy vis-à-vis law enforcement access. Service provider access is sufficiently extensive "to snuff out a reasonable expectation of privacy" only in limited situations, such as when the provider "expresses an intention to 'audit, inspect and monitor' its subscriber's emails." *Warshak*, 631 F.3d at 287. Notably, the Sixth Circuit rejected a monolithic expectation of privacy that is defeated whenever the information at issue is seen by anyone. Instead, and appropriately, the court recognized that we may permit a service provider to run its business without

relinquishing the protections of the warrant requirement: the interposition of a neutral magistrate to review the propriety and need for the government to pry into our personal communications.

Applying that approach to location data means that just because the service provider may retain access to our location information does not mean that we waive a reasonable expectation of privacy in that data vis-à-vis law enforcement access. Permitting a service provider to access information to run its business does not imply consent to give up Fourth Amendment protections. *See, e.g.*, *Warshak*, 631 F.3d at 287 ("[U]nder *Katz*, the degree of access granted to [the service provider] does not diminish the reasonableness of Warshak's trust in the privacy of his emails.").

The government distinguishes *Jones*, which recognized a constitutional privacy interest in location data, primarily based on its claim that its applications seek historical records rather than prospective tracking. *See* Gov. Brief at 39. The government's distinction, though currently reflected in the federal surveillance statute, is not of constitutional significance. In fact, law enforcement acquisition of historical location data can intrude into personal privacy even more than acquisition of real-time or prospective location information. A law enforcement agent seeking prospective location data could get an order on January 1 to track the target's movements for three months, but then would have to wait until March 31

to obtain three months of location data to review. Alternatively, the agent could ask the provider for historical data and immediately obtain a year's worth or more of the target's location information.

Moreover, the government's applications realize the concerns about there being no practical difference between historical and prospective data. *See* Freiwald, *Location Data*, at 739 n.368 ("Historical location data could contain data of quite recent vintage."). As discussed above, in addition to records previously generated, the applications requested that, following the order, records be continuously stored and then delivered to the government. By waiting just long enough for the provider to make a record, the government eliminated the difference between historical and prospective data. Had they been generated, the resulting forward-looking records would not be business records generated in the ordinary course of business, because they would have been generated at the request of law enforcement in response to a court order.

B. Disclosure of Location Data May Not be Compelled Without A Warrant

The government renews a remarkably circular argument that it made in the *Warshak* litigation when it contends that because a 18 U.S.C. §2703(d) order ("D order") permits the compelled disclosure of service provider records, and because a D order is more like a subpoena than a warrant, "a reasonableness standard rather than the warrant requirement" obtains in this case. Gov. Brief at 13. That

statement begs a key question: does the Fourth Amendment permit the government to compel disclosure of the location data it seeks without first obtaining a warrant based on probable cause? The answer to that question requires an analysis of reasonable expectations of privacy in location data. *Cf*. *Warshak v*. *United States*, 490 F.3d 455, 473 (6th Cir. 2007), *vacated on ripeness grounds*, 532 F.3d 521 (6th Cir. 2008) (en banc) ("The government's compelled disclosure argument, while relevant, therefore begs the critical question of whether an e-mail user maintains a reasonable expectation of privacy in his e-mails vis-à-vis the party who is subject to compelled disclosure – in this instance, the ISPs.") As I argued in Part I, the Fourth Amendment requires a warrant for compelled disclosure of location data. Its acquisition intrudes upon reasonable expectations of privacy and requires the interposition of a neutral magistrate to ensure that government investigators stay within constitutional limits.

A statutory provision that purports to permit the government to compel disclosure of location data with fewer procedural protections than those provided by a warrant is unconstitutional. Magistrate Judge Smith implied as much in an appropriate exercise of the judicial review power. *See Smith Opinion*, 747 F. Supp. 2d at 846 (denying the governments' requests for information under the authority of the Stored Communications Act ("SCA") because "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment"); *see also E.D.N.Y.*

Opinion, 809 F. Supp. 2d at 115 (requiring a warrant and showing a probable cause for acquisition of cell site location records "[d]espite the SCA.").

The Sixth Circuit ruled similarly in *Warshak*. After analyzing the nature of modern email and how intrusive it is for government to acquire it, the Sixth Circuit held that "it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment." *Warshak*, 631 F.3d at 286. The court elaborated 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." *Id*. The Court went on to conclude "[m]oreover, to the extent the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." *Id*. at 288.

Interestingly, the Sixth Circuit did not address the government's argument that statutory provisions authorizing compelled disclosures are not subject to the warrant requirement. *See* Government Brief to the Sixth Circuit, 2009 WL 3392997, at 106-109 (arguing that "the Fourth Amendment does not impose particularity, probable cause or notice requirements on compelled disclosures (as opposed to warrants)"). Apparently the Sixth Circuit did not feel it necessary to point out that the decisions the government cited in which compelled disclosure

(without notice, probable cause, or particularity) was permitted were those in which the target lacked a reasonable expectation of privacy. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 141-47 (2008) (discussing and rejecting the government's compelled disclosure argument when users have a reasonable expectation of privacy); Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens,* 72 Geo. Wash. L. Rev. 1375, 1397-1413 (2004) (discussing compelled disclosure precedents). When the records at issue implicate a reasonable expectation of privacy, as location data does, the compelled disclosure argument falls away. *See Warshak*, 490 F.3d at 473 (explaining that if the user does not have a reasonable expectation of privacy in the data sought, the government may meet the reasonableness standard applicable to compelled disclosures, but if the user has a reasonable expectation of privacy, then the warrant requirement applies).

C. The Government Must Not Police Itself

This Court may not permit the government to limit its own acquisition of location data. Foundational constitutional principles require that the courts not trust executive branch officials to police themselves. In its appeal to this Court, the government renews its suggestion that if, contrary to its belief, cell phone providers do in fact create cell phone records when the phone is in an idle state, "it is willing to exclude such information from the scope of its application." Gov.

Brief at 7. The government does not state whether it will amend its application and resubmit it without a request for idle state (registration data), nor does it clarify whether it will also omit its request for forward-looking duration data, which, as discussed above, also contributes significantly to the richness and intrusiveness of cell site location data.

Even if the government amended its applications to exclude the most intrusive information, the risk would remain that the targeted providers would furnish that information nevertheless. Nothing in the statute explicitly limits the nature of the "records" obtainable. *Austin Opinion,* 747 F. Supp. 2d at 579 n.15 ("[T]here is nothing in any of the relevant statutes that makes a distinction between "limited" location information and fully robust, minute-by-minute location information.") In the absence of a legal directive, there is no reason for providers to filter location data to ensure that they deliver only that which the government requests. *Cf*. Gidari, Jr., *Keynote Address*, 41 U.S.F. L. Rev. at 549 (explaining that "[u]nder every pen register order implemented, the government gets location. . . . The location information is just flowing as part of the solution"); *see also id*. at 550 (Service providers "are paying a fortune for the CALEA hardware and software, and they are not paying to filter it further.").

The persistent uncertainty about what the government would ask for and what providers would disclose show why there is no substitute for the judicial

review provided by the meaningful protections of the warrant requirement. *See Austin Opinion*, 747 F. Supp. 2d at 581 (indicating that such protections include a return of the warrant and notice to the target, which may be delayed). This Court must reject the government's request that it be able to safeguard constitutional privacy through its own self-restraint. *Katz v. United States*, 389 U.S. 347, 356 (1967) (requiring that restraints on investigating agents be imposed "by a judicial officer" and not "by the agents themselves."); *see also* Catherine Crump and Christopher Calabrese, *Location Tracking: Muddled and Uncertain Standards Harm Americans' Privacy*, 88 Crim. L. Reporter 1, 3 (2010) (reporting that two U.S. Attorney's offices failed to obtain warrants for access to "the most precise cell tracking information," despite the Department of Justice's recommendation that they do so). The oversight role must be entrusted solely to members of the judiciary. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (noting the need to "consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse.").

CONCLUSION

Location data may provide an essential tool to government agents engaged in law enforcement. Just as with wiretapping, some silent video surveillance, and conventional searches, however, acquisition of location information must be subject to Fourth Amendment safeguards, because users have a reasonable

expectation of privacy in their location data, whether the data is prospective or historical. When government agents acquire location data, they do so in a manner that is hidden, intrusive, indiscriminate and continuous. Therefore, location data acquisition must be subject to at least the protections of a warrant based on a showing of probable cause. Neither a third party rule nor the fact that location data disclosure is compelled obviates the warrant requirement. The lower courts properly denied the government's requests for location data without a warrant based on probable cause and the District Court's opinion should be affirmed.

Respectfully submitted

Date: March 16, 2012 s/ Susan Freiwald

Susan Freiwald
Professor of Law
University of San Francisco
School of Law
2130 Fulton Street
San Francisco, CA 94117
NY2557627
Phone: (415) 422-6467
E-mail: freiwald@usfca.edu

CERTIFICATE OF SERVICE

I hereby certify that on March 16, 2012, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification to the appropriate parties. Paper copies of this brief will also be sent to the Clerk by a third party by commercial carrier.

s/ Susan Freiwald

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 6832 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 proportionally spaced typeface using Microsoft Word 2010 version 14 in Times New Roman 14 point font (footnotes in 12 point font).

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

4. The digital submission has been scanned for viruses with Sophos Endpoint Security and Control Version 9.5 (last updated 3/16/2012), and according to that program, is free of viruses.

/s Susan Freiwald

Dated: March 16, 2012