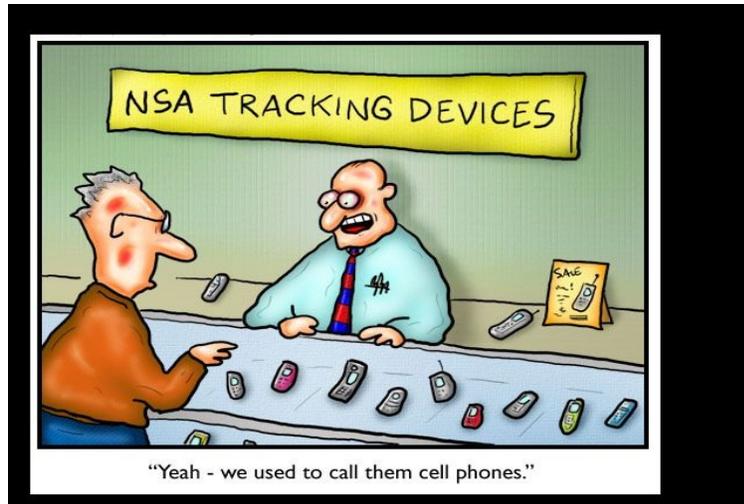


**Beyond *Jones*: Electronic Surveillance  
And The Fourth Amendment**

**AFPD Lisa Hay  
District of Oregon  
June 2012**

BEYOND JONES:  
*Electronic Surveillance and the Fourth Amendment*



“The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone - the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.”

*Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

“The [Fourth] Amendment guarantees the privacy, dignity and security of persons against certain arbitrary and invasive acts by officers of the Government or those acting at their direction.”

*Skinner v. Ry. labor Execs. Ass'n*, 489 U.S. 602, 613-14 (1989).

“The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.”

*Kyllo v. United States*, 533 U.S. 27, 34 (2001).

## TABLE OF CONTENTS

I.	List of Surveillance Techniques.....	1
II.	Chronological Summary of Surveillance Statutes.....	2
III.	What’s Wrong With Surveillance?.....	5
IV.	Pen Register and SCA examined.....	7
V.	Location Information and “Hybrid Orders”.....	9
VI.	Possible Areas for Litigation, By Evidence Obtained.....	13
VII.	Issues To Raise with U.S. Magistrates.....	18

## APPENDIX

A.	Materials For Understanding and Attacking Improper Authorization for Cell Site Location Data:	
	• <i>In Re: Application</i> , 405 F.Supp.2d 435 (S.D.N.Y 2005) (explaining “hybrid order” by the govt and allowing application, but with limitations).....	1
	• Testimony of the Honorable Stephen William Smith, US Magistrate Judge, U.S. House Hearing on Electronic Communications Privacy Act Reform (June 24, 2010) (describing the chaos among statutes).....	16
	• <i>In Re Application</i> , 2010 WL 4286365 (S.D. Tex) (Smith, MJ) (rejecting govt application for cell site data and explaining why statutes do not authorize request), <i>appeal pending</i> , No. 11-20884 (5 <sup>th</sup> Cir).....	33
	• Amicus brief of ACLU and EFF in Support of Affirmance, No 11-20884 (5 <sup>th</sup> Cir. 2012) (providing arguments in support of MJ Smith and opposing use of § 2703(d) orders for location data).....	51
	• <i>See also In Re: Application</i> , 620 F.3d 304 (3d Cir. 2010) (analyzing request for cell tower location information and determining a warrant is not required BUT that magistrate judge has discretion to require one ..... (not included)	
	• <i>In Re: Application</i> , 2011 WL 3423370 (D. Md. Aug. 2011) (M.J. Gauvey)	

(denying application for location data without showing of probable cause.. (not included)

• *IN Re Application*, 10-MC-897 (E.D.N.Y. Aug 2011) (MJ Garaufis) (denying govt application after lengthy discussion of location data and cases). . . . . (not included)

B. News Articles and Advertisements

• Drones: “*Here’s Looking at You*,” The New Yorker (May 14, 2012) (law enforcement use of drones). . . . . 118

• IMEI Catcher/Man-in-the -middle in Arizona case. . . . . 125

• “*DOJ: Stingray Cellphone Device Falls Under Fourth Amendment, But Don’t Ask About It*.” (Webpost, Nov. 6, 2011 re: Arizona case *US v. Rigmaiden*); related article and advertisement for IMEI Catcher. . . . . 127

• ACLU Press Release on Cell Phone Tracking (April 6, 2012). . . . . 133

• UFED Mobile Forensics – advertisement explaining capabilities for extracting deleted phone data, call history, text messages, images, contacts lists, geotags etc. from cellphones; ACLU press release regarding police use of such devices during traffic stops in Michigan (April 13, 2011). . . . . 136

C. Government Response Re: Motion For Discovery (Nov. 2011), *US v. Rigmaiden*, 08-CR-0814-PHX-DGC (D. AZ.) with attached Affidavit of Special Agent Bradley Morrison (describing IMEI catcher used, assuming *arguendo* that this constitutes a Fourth Amendment search, but relying on Rule 41 Tracking Warrant to authorize search). . . . . 141

## I. SURVEILLANCE TECHNIQUES<sup>1</sup>

- Wiretaps – real-time monitoring of telephone communications or bugging of locations (*compare*: body wire)
- “Slap On” GPS trackers – small device attached to vehicle to provide location info; also can be wired to receive power from the car battery.
- Precision locators– remote activation and monitoring of GPS location of a particular cell phone
- Pen Registers – Originally, device that provides real time disclosure of numbers dialed out on a monitored telephone; now more information sought and provided
- Trap and Trace Devices – Identical to Pen Register, but discloses numbers calling in to a monitored telephone
- Pole Cameras – Stationary cameras installed on utility poles outside a residence or building and recording either by video or fixed number of still images per minute
- Cellphone site location – Historic or real-time data from cellphone towers to locate cellphones; accuracy can be increased by triangulation, the hand-off between towers, and other factors.
- CIPAV – “Computer internet protocol address verifier” – FBI spyware that infiltrates a person’s computer and monitors user’s internet use.
- Accessing Unsecured Wireless Routers – *See US v. Ahrndt*, 2012 WL 1142571 (9<sup>th</sup> Cir. April 2012)
- Drones – FAA to authorize law enforcement use of drones (unmanned aerial vehicles) by May 2012
- Emerging technology: Cellphone “readers”; Stingray/Trigger fish or man-in-the-middle or IMEI catchers; Moochercatchers; Carrier IQ software. See articles in Appendix.

---

<sup>1</sup> Thanks to AFPD Amy Baggio for her earlier version of the materials in this outline.

## II. CHRONOLOGICAL SUMMARY OF ELECTRONIC SURVEILLANCE LAWS

The federal code contains authorization for electronic surveillance and information collection in numerous sections. Below is a brief chronology that may help orient the reader in the law. The progress in technology has rendered some definitions redundant or obsolete, created over-lapping coverage under some statutes, and exposed large gaps in the law. Defense attorney efforts can be aimed at exposing the prosecution’s misuse of statutory authority. For a good statement of how this developing law affects arguments about cell site location information, for example, see *In Re: Application*, 405 F.Supp.2d 435 (S.D.N.Y 2005) (appendix).

DATE ENACTED	TITLE AND CITATION	PURPOSE/IMPORTANCE
1934	<i>Communications Act of 1934</i> , 48 Stat. 1065, as amended, 47 USC § 153	<ul style="list-style-type: none"> <li>• defines “common carrier,” “wire communications” and other terms. Later statutes refer to these.</li> </ul>
1968	<i>Wiretap Act</i> , Pub.L. 90-351, Title III § 802, June 19, 1968,as amended, 18 USC § 2510 et seq.	<ul style="list-style-type: none"> <li>• defines “wire communication” and other terms; refers to Communications Act for some definitions.</li> <li>• amended by ECPA (see below)</li> <li>• prohibits real-time interception and disclosure of certain wire, oral or electronic communications, except as authorized by this statute;</li> <li>• requires that government establish probable cause that a crime has been, or is about to be, committed <b>and</b> that wiretap is necessary because traditional law enforcement techniques are not likely to be successful or are too dangerous.</li> <li>• includes an exclusionary rule if unauthorized interceptions occur.</li> </ul>

DATE ENACTED	TITLE AND CITATION	PURPOSE/IMPORTANCE
1978	<p><b><i>Foreign Intelligence Surveillance Act (FISA)</i></b>, Pub.L. 95-511, Oct. 25, 1978, as amended, 50 USC § 1801 et seq.</p>	<ul style="list-style-type: none"> <li>• authorizes electronic surveillance (including searches of residences) without court orders for specific foreign intelligence purposes of up to one year;</li> <li>• special FISA court to authorize other surveillance; sealed proceedings</li> </ul>
1986	<p><b><i>Electronic Communications Privacy Act</i></b> – (ECPA) Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510, et. seq.</p> <p><b>Three Titles:</b></p> <p><b>I.</b> Wiretap Act, 18 USC § 2510-2522</p> <p><b>II.</b> Stored Communications Act, 18 USC § 2701-2712</p> <p><b>III.</b> Pen Register &amp; Trap and Trace Devices, 18 USC § 3121-27</p>	<ul style="list-style-type: none"> <li>• amends the old wiretap statute.</li> <li>• distinguishes between access to real-time data vs. stored records;</li> <li>• defines tracking device</li> </ul> <p>• <b>Wiretap Act:</b> prohibits real-time interception and disclosure of certain wire, oral or electronic communications, except as authorized by this statute; standards stricter than constitutionally required</p> <p>• <b>SCA:</b> applies to historic (non- real time) communications in “electronic storage” or “remote computing storage” by “electronic communications service (ECS).” See details below.</p> <p>• <b>Pen/TT</b> order provide real-time data on numbers called from and calling a phone, plus other data</p> <p>• Pen/TT order under § 3123, or FISA, are the <i>exclusive</i> authorizations for installing or using a Pen/TT (18 USC § 3121(a)); USA Patriot Act expands to include “all dialing, routing, addressing, or signaling information.”</p>

DATE ENACTED	TITLE AND CITATION	PURPOSE/IMPORTANCE
1986	Further, ECPA defines <b>mobile tracking devices</b> at 18 USC § 3117	<ul style="list-style-type: none"> <li>• defines MTD as “electronic or mechanical device which permits the tracking of the movement of an object or person.”</li> <li>• new authorization to install such devices, based on a warrant, added to chapter 205 among warrant requirements</li> </ul>
1994	<i>Communications Assistance for Law Enforcement Act (CALEA)</i> , 47 USC 1001-1010	<ul style="list-style-type: none"> <li>• amends wiretap, SCA and Pen sections of ECPA</li> <li>• requires companies that provide communications services (like phone or internet) to utilize a communications system that will allow the government a basic level of access.</li> <li>• forbids carriers from providing location information “solely” under pen register and trap &amp; trace orders: 47 USC § 1002(a)(2)(B);</li> <li>• expands privacy protections of ECPA to cordless phones and data transmitted by radio</li> </ul>
1999	<i>Wireless Communication and Public Safety Act</i> , 47 USC § 222(f)	<ul style="list-style-type: none"> <li>• limits carriers’ disclosure of “CPNI” - customer proprietary network information, including specifically location information, “unless required by law.”</li> </ul>
2001	<i>USA Patriot Act</i> , Pub.L. 107-56, Title II § 216(a)	<ul style="list-style-type: none"> <li>• expands definition of available data under pen register order to include “all dialing, routing, addressing, or signaling information.”</li> </ul>

### III. WHAT'S WRONG WITH SURVEILLANCE?

The unavoidable difficulty with any Fourth Amendment litigation is that the police, in fact, caught the bad guy. That's why you, the criminal defense attorney, are in the picture and filing motions to suppress. With electronic surveillance techniques as with any other method that violates the Fourth Amendment, it is critical to answer the question "Isn't that just good police work?" The answer is that yes, the police work was excellent, just get a warrant. Long-term surveillance or surreptitious entry into homes or protected spaces risks creation of a police state and violates cherished American ideas of individual liberty and freedom from government interference. We have a system set up – in which the judiciary is key – to protect against abuse of government authority, and it is important that every player with power respect that system. A number of cases describe in eloquent ways the dangers of surveillance and the importance of judicial oversight, including Judge Kozinski's concise summary: "it's creepy and un-American." Use these cases to educate judges about the importance of these issues, not just for your little no-good petty thief, but for everyone in the country:

- *U.S. v. Maynard*, 615 F.3d 544 (D.C.Cir. 2010), *aff'd sub. nom.*, *U.S. v. Jones*, 132 S. Ct. 945 (2011), on surveillance:

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. 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.

- *U.S. v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing *en banc*), cert granted, judgment vacated, 132 S.Ct. 1533 (Feb. 21, 2012):

The modern devices used in Pineda-Moreno's case can record the car's movements without human intervention-quietly, invisibly, with uncanny precision. A small law enforcement team can deploy a dozen, a hundred, a thousand such devices and keep track of their various movements by computer, with far less effort than was previously needed to follow a single vehicle. The devices create a permanent electronic record that can be compared, contrasted and coordinated to deduce all

manner of private information about individuals. By holding that this kind of surveillance doesn't impair an individual's reasonable expectation of privacy, the panel hands the government the power to track the movements of every one of us, every day of our lives.

\* \* \* \*

[T]here's no hiding from the all-seeing network of GPS satellites that hover overhead, which never sleep, never blink, never get confused and never lose attention. Nor is there respite from the dense network of cell towers that honeycomb the inhabited United States. Acting together these two technologies alone can provide law enforcement with a swift, efficient, silent, invisible and cheap way of tracking the movements of virtually anyone and everyone they choose. *See, e.g.*, GPS Mini Tracker with Cell Phone Assist Tracker, <http://www.spyville.com/passive-gps.html> (last visited July 17, 2010). Most targets won't know they need to disguise their movements or turn off their cell phones because they'll have no reason to suspect that Big Brother is watching them.

The Supreme Court in *Knotts* expressly left open whether “twenty-four hour surveillance of any citizen of this country” by means of “dragnet-type law enforcement practices” violates the Fourth Amendment's guarantee of personal privacy. 460 U.S. at 283-84, 103 S.Ct. 1081. When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that “such dragnet-type law enforcement practices” are already in use. This is precisely the wrong time for a court covering one-fifth of the country's population to say that the Fourth Amendment has no role to play in mediating the voracious appetites of law enforcement. *But see Maynard*, 615 F.3d at 557.

\* \* \*

I don't think that most people in the United States would agree with the panel that someone who leaves his car parked in his driveway outside the door of his home invites people to crawl under it and attach a device that will track the vehicle's every movement and transmit that information to total strangers. There is something **creepy and un-American** about such clandestine and underhanded behavior. To those of us who have lived under a totalitarian regime, there is an eerie feeling of déjà vu. This case, if any, deserves the comprehensive, mature and diverse consideration that an en banc panel can provide. We are taking a giant leap into the unknown, and the consequences for ourselves and our children may be dire and irreversible. Some day, soon, we may wake up and find we're living in Oceania.

*Groh v. Ramirez*, 540 U.S. 551 (2004):

“The point of the Fourth Amendment ... is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. **Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.** Any assumption that evidence sufficient to support a magistrate's disinterested determination to issue a search warrant will justify the officers in making a search without a warrant would reduce the Amendment to a nullity and leave the people's homes secure only in the discretion of police officers .... When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or government enforcement agent.” *Johnson v. United States*, 333 U.S. 10, 13–14, 68 S.Ct. 367 (1948) (footnotes omitted).

See also *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (need to protect privacy from technology); *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010) (reviews importance of emails; protection of privacy from technology); *U.S. v. Warshak*, 631 F.3d 266 (6<sup>th</sup> Cir. 2011) (privacy and technology, addresses and rejects many gov't arguments).

#### IV. PEN REGISTER AND SCA EXAMINED

Pen Register and Trap and Trace Devices, 18 USC § 3121-3127
<p><b>Scope:</b></p> <ul style="list-style-type: none"><li>• a pen register is a device that “records or decodes dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,” provided that it not include the <i>contents</i> of any communication. Trap and Trace is the same, but for incoming numbers.</li></ul>
<p><b>Authorizations:</b></p> <ul style="list-style-type: none"><li>• under § 3122, govt can apply to court if “information likely to be obtained” will be <i>relevant</i> to an on-going criminal investigation.</li><li>• under § 3121, no person may install a pen or TT without getting a court order under § 3123 or FISA; a knowing violation can result in one year incarceration.</li></ul>

**Legal Questions:**

- since pen orders allow the government to obtain “signaling information,” and since cellphones “signal” to cell towers, creating CSLI (celltower site location information), shouldn’t the government be able to obtain this location information with pen registers? Answer: NO; even the DOJ seems to have moved away from any claim that a pen register *alone* is sufficient to obtain location data. See “Hybrid order” below.

**The Stored Communications Act, 18 USC § 2701-2712****Scope:**

- Addresses access to records held by both “electronic communications services” and “remote computing storage.” Most ISPs do both now, so this distinction is outdated but retains a statutory significance.
- retrospective, not prospective – that is, the statute refers to “stored” items, not yet-to-be-created items; therefore, the government should not get “real-time” data under this statute.
- the term “electronic communication,” which is used in the SCA, does not include information from tracking devices , which are defined in 18 USC § 3117(b) and incorporated by reference. *See* 18 USC § 2711 (adopting definitions in 18 USC § 2510); 18 USC § 2510 (defining “electronic communication” to exclude tracking devices).

**Authorizations:**

- under § 2703(a), the govt can require providers to disclose the *contents* of stored communications that are less than 180 days old if they have a *warrant*;
- under § 2703(b), the govt can require provider to disclose *contents* of stored communications *stored by a remote computing service or older than 180 days* if they have a *warrant or 2703(d) order*.
- under § 2703(c), the govt can obtain records pertaining to the subscriber (but not content) by warrant, or court order under (d), or with consent of subscriber, or if other exceptions apply, or by administrative subpoena.
- under § 2703(d), the govt can obtain a court order to obtain content of stored communications if it offers specific and articulable facts showing that there are reasonable grounds to believe that the contents are relevant and material to an ongoing criminal investigation.

**Legal Issues:**

- Is a 2703(d) order really constitutionally sufficient to obtain the contents of emails (and text messages?), which are our written words? *NO* – says *U.S. v. Warshak*, , 631 F.3d 266 (6<sup>th</sup> Cir. 2010).
- Can a 2703(d) order, in combination with a pen register order, allow the govt to obtain celltower site location information? Split in the courts – see Hybrid Order below.
- Is a 2703(c) administrative subpoena really constitutionally sufficient to obtain all non-content subscriber information, when the reasoning in *Smith* is so outdated and was limited to “numbers dialed”?

**V. LOCATION INFORMATION AND HYBRID ORDERS**

As the ACLU survey has made clear (see Appendix), state and federal law enforcement agents are tracking cellphones and obtaining location information in extraordinary numbers. Whether it is “pinging” phones, collecting cell tower site location information, activating GPS on phones, or collecting stored GPS data, the police are watching. As Judge Kozinski summarized in *Pineda-Moreno*:

If you have a cell phone in your pocket, then the government can watch you. Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, Mar. 1, 2010, available at <http://www.newsweek.com/id/233916>. At the government's request, the phone company will send out a signal to any cell phone connected to its network, and give the police its location. Last year, law enforcement agents pinged users of just one service provider-Sprint-over eight million times. See Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, Slight Paranoia (Dec. 1, 2009) <http://paranoia.dubfire.net/2009/12/8-million-reasons-for-realsurveillance.html>. The volume of requests grew so large that the 110-member electronic surveillance team couldn't keep up, so Sprint automated the process by developing a web interface that gives agents direct access to users' location data. *Id.* Other cell phone service providers are not as forthcoming about this practice, so we can only guess how many millions of *their* customers get pinged by the police every year. See Justin Scheck, *Stalkers Exploit Cellphone GPS*, Wall St. J., Aug. 5, 2010, at A1, A14 (identifying AT&T and Verizon as providing “law-enforcement[ ] easy access to such data”).

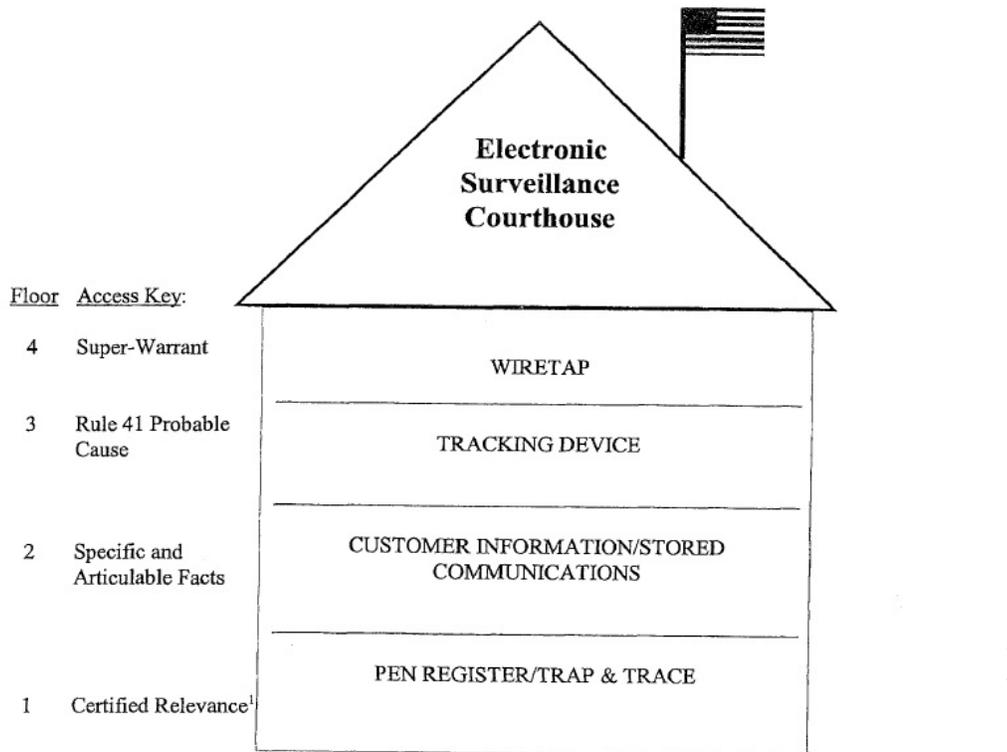
Use LoJack or OnStar? Someone's watching you too. *E.g.*, OnStar Stolen Vehicle Assistance, [http://www.onstar.com/us\\_english/jsp/plans/sva.jsp](http://www.onstar.com/us_english/jsp/plans/sva.jsp) (last visited July 17, 2010). And it's not just live tracking anymore. Private companies are starting to save location information to build databases that allow for hyper-targeted advertising. *E.g.*, Andrew Heining, *What's So Bad About the Google Street View Data Flap?*, Christian Sci. Monitor, May 15, 2010, available at <http://>

www. csmonitor. com/ USA/ 2010/ 0515/ What- s- so- bad- about- the- Google- Street- View- data- flap. Companies are amassing huge, ready-made databases of where we've all been.

And most players don't seem to know – or care – what law applies to all of this. Cellphone companies are making money by selling data to the police; as long as they have some “authorization,” they are covered. Police are getting tips and tracking suspects and innocent people alike from their desks, without oversight. They have no interest in clarifying the law. The people who are being tracked and watched are never notified by the cellphone companies of what occurs, and only those charged with a crime find out – maybe – that location data was used. So it is up to U.S. Magistrate Judges to make the right decisions when signing warrants or 2703(d) orders, and up to criminal defense attorneys to use discovery tools to ferret out what surveillance techniques were used, then question them.

Here is Magistrate Judge Smith's explanation of the law of the “Electronic Surveillance Courthouse:”

**EXHIBIT A**



**The Hybrid Theory  
or What Judge Smith Calls the “Three-Rail Bank Shot”**

**Pen Register Statute, 18 USC 3121-27:**

a pen register is a device that “records or decodes dialing, routing, addressing or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,” provided that it not include the contents of any communication.

no person may install or use a pen register or TT without getting a court order under § 3123 or FISA;

**CALEA- 47 USC 1002:**

“a telecommunications carrier shall ensure that its ... facilities ... are capable of ... expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier”

BUT:

“with regard to information acquired **solely pursuant to the authority for pen registers** and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information *shall not include any information that may disclose the physical location of the subscriber* (except to the extent that the location may be determined from the telephone number)”

**Stored Communications Act, 18 USC § 2701-2712**

A company providing electronic communication services or remote computing services shall not knowingly divulge a record or other information pertaining to a subscriber to any government entity

Except: if the gov’t can present the court specific and articulable facts showing reasonable grounds to believe the contents of the communication or other information sought are relevant and material to an on-going investigation, then a 2703(d) order permits such disclosure.

Electronic communications do not include information from tracking devices.

Under the theory, although Pen registers *alone* are not enough to obtain location data because of the restriction in CALEA, a pen register order *plus* an SCA 2703(d) order is sufficient, because location data is “stored” data.

**Question:** where CALEA says “solely pursuant” to pen devices, why is that not a reference to possible FISA or wire tap orders in conjunction with a pen order? Courts say this shows an SCA order plus a pen was contemplated, but isn’t that a stretch?

Cases have recorded the progression (back tracking?) of government arguments for what information may be permissibly obtained under these statutes:

- Early on, the govt began seeking “hybrid orders” under the SCA and Pen Statute for the prospective, ongoing cellphone location data. *See, e.g., In re Application*, 396 F. Supp.2d 747 (S.D. Tex. 2005) (Smith, MJ); *In re Application of U.S. for Order*, 497 F.Supp.2d 301, 302 (D.Puerto Rico,2007) (rejecting application by govt for “orders under 18 U.S.C. §§ 2703 and 3122, ... for the installation and use of pen register and trap and trace devices, Enhanced Caller ID special calling features, and the capture of limited geographic or cell site information, all for a period of sixty days from the date of the order”). Under the govt theory, although location data cannot be obtained by pen registers, and although the SCA only applies to “stored” communications not on-going information, the combination of the two statutes allows real-time access to location data. This argument for prospective/real-time data has been rejected by numerous courts. *See, e.g., In re Application*, 2006 WL 1876847 (N.D.Ind. July 5, 2006); *In re Application*, 396 F.Supp.2d 747, 765 (S.D.Tex.2005); *In re Application*, 396 F.Supp.2d 294, 327 (E.D.N.Y.2005).

- the government now argues that “historic” cellsite location data is different and can be obtained under a hybrid of the Pen and SCA. The theory is that this is simply “stored’ data, and was voluntarily turned over by the cellphone used to the carrier. Courts are split on this. *Compare In Re Application*, 620 F.3d 304 (3d Cir. 2010) (hybrid theory allowed for historic data, but MJs may require a higher showing, *e.g.*, probable cause, if the situation warrants it), *with In Re Application*, 10-MC-897 (E.D.N.Y. Aug 2011) (MJ Garaufis) (denying govt application after lengthy discussion of location data and cases); *In Re Application*, 2010 WL 4286365 (S.D. Tex) (Smith, MJ) (rejecting govt application for cell site data and explaining why statutes do not authorize request), *appeal pending*, No. 11-20884 (5<sup>th</sup> Cir).

- Post-*Jones*, the official DOJ position is that search warrants should be obtained for any GPS data, but that the hybrid 2703(d) +Pen orders are still sufficient for historic cellsite location information.

## VI. POSSIBLE AREAS FOR LITIGATION

EVIDENCE SOUGHT	AUTHORITY	ISSUES
<p><b><u>E-MAIL Content</u></b></p> <ul style="list-style-type: none"> <li>• Did they get a search warrant?</li> </ul>	<p>Rule 41 F.R.C.P</p>	<p><i>US v. Warshak</i>, 631 F.3d 266 (6<sup>th</sup> Cir. 2010) says obtaining email content without a warrant violates the 4<sup>th</sup> Amendment, and if the SCA authorizes this, it is unconstitutional; split in the case law. <b>Raise this Issue!</b></p>
<ul style="list-style-type: none"> <li>• Did they provide the notice required by FRCP 41?</li> </ul>	<p>SCA, 18 USC § 2703(a) incorporates the procedures of Rule 41 warrants</p>	<p><i>Warshak</i>, 631 F.3d 266 (reviews notice provisions but finds any violation not relevant because of good faith issue); <i>See</i> case 08-mc-9147 (Dist. Oregon). The judge says notice is required but can be made to the ISP rather than the subscriber. This is worth challenging. See the cited cases in the opinion and the Fed Defender brief on ECF.</p>
<ul style="list-style-type: none"> <li>• Did they send a <i>prospective</i> “evidence retention” letter to the ISP, asking it to hold everything created until the warrant is obtained?</li> </ul>	<p>SCA, 18 USC § 2703(f) allows agency to ask ISP to retain evidence “in their possession” at the time of the letter, but not to hold future evidence.</p>	<ul style="list-style-type: none"> <li>• <i>Warshak</i>, 631 F.3d 266: the concurrence especially is troubled by this “back-door wiretapping,” and believes this violates the 4<sup>th</sup>.</li> </ul> <p>Consider: if property rights include the right to dispose of property, hasn’t the govt meaningfully interfered with a property interest by preventing disposal of emails, so that this is a seizure under the 4<sup>th</sup>?</p>

EVIDENCE SOUGHT	AUTHORITY	ISSUES
<ul style="list-style-type: none"> <li>If govt relies on the SCA and not a warrant, did they request email less than 180 days old? Was it opened or unopened email?</li> </ul>	Compare § 2703(a) and (b) – different standards for old and new email, and different rules based on where email is held– in “electronic storage” or in a “remote computing service.”	Once email is opened, does it move from electronic storage to a “remote computer service” and therefore can be obtained under § 2703(b)? The Ninth Circuit says no. <i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9 <sup>th</sup> Cir. 2004); other circuits disagree. Preserve this issue if no warrant is used.
<ul style="list-style-type: none"> <li>Was the search warrant overbroad or insufficiently particularized?</li> </ul>	FRCP 41; 4 <sup>th</sup> A	Search warrants often ask for “all” email content. Use <i>Warshak</i> (“email provides an account of its owner’s life”) and the Ninth Circuit’s case <i>CDT</i> , 621 F.3d 1162 (9 <sup>th</sup> Cir. 2010), to argue that grabbing <i>all</i> content from an email account is excessive and like grabbing a full computer or a business’s entire cabinet of files without any limitations. Email is easy to search using terms; officers should be required to identify those terms in the warrant and not be permitted indiscriminate rummaging.
<p><b><u>TEXT MESSAGES</u></b></p> <ul style="list-style-type: none"> <li>Did they get a warrant?</li> </ul> <p>(Probably not – they rely on SCA § 2703(d))</p>	FRCP 41	<p>Apply the reasoning of <i>US v. Warshak</i>, 631 F.3d 266 (6<sup>th</sup> Cir. 2010): if obtaining email content without a warrant violates the 4<sup>th</sup> Amendment, so should obtaining text messages. In fact, shouldn’t the govt beheld to even need the higher wiretap standard because text is like a phone call? Cite <i>Quon</i>, 130 S.Ct. 2619 (2010) which dodges the issue but has good language.</p> <p>Ninth Circuit case analogizes IM chat to private call for purposes of consent by one party. <i>United States v. Meek</i>, 366 F.3d 705, 711 (9<sup>th</sup> Cir. 2004).</p>

EVIDENCE SOUGHT	AUTHORITY	ISSUES
<p><b><u>CELLPHONE CONTENT</u></b></p> <ul style="list-style-type: none"> <li>• when phone is in the physical possession of the officers, did they get a warrant to search before flipping through it?</li> </ul>	<p>4<sup>th</sup> Amendment</p>	<p>See <i>Schlossberg v. Solesbee</i>, 10-6014-TC (D. Ore 2012) (Coffin, MJ): search of any electronic devices capable of holding information requires a warrant, even if the item is seized incident to arrest. Great case with cites, distinguishing or rejecting other cases; <i>US v. Davis</i>, 10-CR-339-HA (D. Or 2011) (suppressing evidence derived from warrantless search of cellphone seized incident to arrest); <i>US v. Wall</i>, 2008 WL 5381412 (S.D. Fla 2008) (same); <i>United States v. Park</i>, No. CR 05-375 SI, 2007 WL 1521573 (N.D.Cal. May 23, 2007) (unpublished); <i>But see People v. Diaz</i> (Cal. S.Ct.) (Cellphone is just a “container” that can be opened on search incident to arrest).</p>
<ul style="list-style-type: none"> <li>• when phone information (texts, contact book, photos) is accessed electronically, did they get a search warrant or rely on the SCA?</li> </ul>	<p>18 USC § 2703(a) and (d) – purport to authorize access to stored content</p>	<p>See arguments against warrantless access to email, above under <i>Warshak</i>. Challenge this!</p>
<p><b><u>GPS Data</u></b></p> <ul style="list-style-type: none"> <li>• GPS precision locators placed on vehicles</li> </ul> <p>What about GPS precision locators, if they were present already but just activated by police?</p>	<p>Warrant required</p> <p>warrant? Use <i>Jones</i> concurrence by Alito to argue for one; also 18 USC § 3117.</p>	<p><i>Jones</i>, 132 S. Ct. 945.</p> <p><b>previous circuit split:</b> Compare <i>US v Marquez</i>, 605 F.3d 604 (8th Cir 2010) (no warrant required); <i>US v. Pineda-Moreno</i>, 591 F.3d 1212 (9th Cir. 2010) (no warrant required), cert. granted, judgment vacated, 132 S.Ct. 1533 (Feb. 21, 2012), with <i>US v. Maynard</i>, 615 F.3d 544 (D.C.Cir. 2010), aff’d sub. nom, <i>US v. Jones</i>, 132 S. Ct. 945 (2011).</p>

EVIDENCE SOUGHT	AUTHORITY	ISSUES
<ul style="list-style-type: none"> <li>• GPS from Cellphones?</li> </ul> What kind of order did they get?	18 USC § 3117? 18 USC § 2703(d)? Warrant?	<p>Argue that the principles from <i>Jones, Maynard</i> and the <i>Pineda-Moreno</i> dissent apply. <i>US v. Pineda-Moreno</i>, 591 F.3d 1212 (9th Cir. 2010) (dissent), cert granted, judgment vacated, 132 S.Ct. 1533 (Feb. 21, 2012); <i>US v. Maynard</i>, 615 F.3d 544 (D.C.Cir. 2010), aff'd sub. nom, <i>US v. Jones</i>, 132 S. Ct. 945 (2011).</p> <p>Tracking requires a warrant. Rely on <i>In Re Application</i>, 2010 WL 4286365 (S.D. Tex 2010) (Smith, M.J.); ACLU brief in Fifth Circuit appeal (attached), and testimony of Judge Smith before Congress (attached).</p>
<p><b>Cell Site Data</b></p> <ul style="list-style-type: none"> <li>• what kind of order did they use, and what kind of information was sought?               <ul style="list-style-type: none"> <li>- distinguish real time v. historical</li> <li>– plain pen order vs. “hybrid order”</li> </ul> </li> <li>• should they need a warrant?</li> </ul>		Rely on <i>In Re Application</i> , 2010 WL 4286365 (S.D. Tex 2010) (Smith, M.J.); ACLU brief in Fifth Circuit appeal (attached), and testimony of Judge Smith before Congress (attached).
<ul style="list-style-type: none"> <li>• what equipment was used to capture the information?</li> </ul>		If they use man-in-the-middle or IMEI catchers or other clones, the govt cannot rely on <i>Smith</i> and the argument that data was voluntarily given to a third party - argue this is a statutory and 4 <sup>th</sup> Amendment violation

EVIDENCE SOUGHT	AUTHORITY	ISSUES
<p><b>Pen Register/TT Data</b></p> <ul style="list-style-type: none"> <li>• how broad was the information gathered?</li> </ul>	<p>Pen statute - 18 USC § <b>3121-3127</b></p>	<p>Argue that modern technology goes far beyond what was imagined in the early Pen cases, so distinguish <i>Smith v. Maryland</i>, 442 U.S. 735 (1979) (no expectation of privacy in numbers dialed out); see <i>In Re Applications</i>, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (distinguishing <i>Smith</i>).</p>
<ul style="list-style-type: none"> <li>• did they ask for or get cut through numbers or “post cut through dialed digits?” Did they get them? These are the numbers you enter <i>after</i> the call connects (e.g., your bank account number, or passwords) – this is clearly “content”</li> </ul>	<p>Pen statute - 18 USC § <b>3121-3127</b></p>	<p>See <i>In Re Applications</i>, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (no authorization for govt to seek post cut through dialed digits through pen register order; application denied)</p> <p>Note: violations of pen register law do not fall under exclusionary rule. <i>United States v. Forrester</i>, 512 F.3d 500, 512 (9th Cir. 2008). Need to articulate as constitutional violation, not statutory violation.</p>

EVIDENCE SOUGHT	AUTHORITY	ISSUES
<p><b><u>Pole Camera/Videos</u></b>  <b><u>Drones?</u></b></p> <ul style="list-style-type: none"> <li>• did the camera intrude on a protected space, e.g. a home? (Church?)</li> <li>• did the surveillance last so long that it created a picture of the person's life?</li> <li>• does it feel "creepy and un-American?"</li> </ul>		<p>Some bad law, but revisit this post-<i>Jones</i> and <i>Maynard</i>. <i>United States v. McIver</i>, 186 F.3d 1119 (9th Cir. 1999)(warrant not required if defendant did not have reasonable expectation of privacy in public area); <i>United States v. Vankesteren</i>, 553 F.3d 286 (4<sup>th</sup> Cir. 2009) (camera installed to record defendant's open field does not implicate 4th) <i>United States v. Jackson</i>, 213 F.3d 1269 (10th Cir. 2000) (No reasonable expectation of privacy because cameras were incapable of viewing inside house...any passerby could easily observe same thing).</p> <p>But: <i>United States v. Cuevas-Sanchez</i>, 821 F.2d 248 (5th Cir. 1987) (video surveillance of home constituted search, warrant required).</p>

## VII. ISSUES TO RAISE WITH U.S. MAGISTRATES

### 1. Location Data – make the govt get a warrant

- see *In Re: Application*, 620 F.3d 304 (3d Cir. 2010) (analyzing request for cell tower location information and determining a warrant is not required BUT that magistrate judge has discretion to require one;

- see *In Re Application*, 2010 WL 4286365 (S.D. Tex) (Smith, MJ) (rejecting govt application for cell site data and explaining why statutes do not authorize request), *appeal pending*, No. 11-20884 (5<sup>th</sup> Cir);

- see *In Re Application*, 10-MC-897 (E.D.N.Y. Aug 2011) (MJ Garaufis) (denying govt application after lengthy discussion of location data and cases).

2. Email and Texts – make the govt get a warrant
  - *see US v. Warshak*, 631 F.3d 266 (6<sup>th</sup> Cir. 2010) (obtaining email content without a warrant in some circumstances violates the 4<sup>th</sup> Amendment)
3. Computer and Cellphone Searches – warrants are overbroad and unparticularized
  - *see In Re Application for Search Warrant*, 770 F.Supp.2d 1138 (W.D.Wash 2011) (Donohue, MJ) (denying warrant application for electronic devices as overbroad);
  - *see United States v. Comprehensive Drug Testing (“CDT”)*, 621 F.3d 1162 (9<sup>th</sup> Cir. 2010) (*en banc*) (offering “concluding thoughts” and guidance for magistrates on how to require more particularized warrants for computer searches, including requirement that gov’t waive reliance on the plain view doctrine in digital evidence cases);
  - *see Schlossberg v. Solesbee*, 10-6014-TC (D. Ore 2012) (Coffin, MJ) (holding search of any electronic devices capable of holding information requires a warrant, even if the item is seized incident to arrest).
4. Internet Tools and Searches
  - accessing an unsecured wireless router is a search? *See US v. Ahrndt*, 2012 WL 1142571 (9<sup>th</sup> Cir. April 2012) (remanding for further fact-finding);
  - standing outside a residence with a Moochercatcher antennae is a search? Check with Marketa Sims in Pennsylvania for update on her case.
  - follow *US v. Rigmaiden* (D. AZ) for developments on use of IMEI catchers/ man-in-the-middle.
5. Notice to Subscribers or Secrecy?
  - *see In re Application*, 2011 WL 5528247 (C.D.Cal.,2011) (rejecting govt motion for 2705(b) order to prevent notice to subscribers of grand jury subpoena);

## *Sources and Resources*

*American Civil Liberties Union*, <http://www.aclu.org/protecting-civil-liberties-digital-age> : Up to date information on ACLU project to fight secrecy by cellphone carriers, pending legislation, and other issues.

Electronic Frontier Foundation ([www.eff.org](http://www.eff.org)) – nonprofit devoted to “defending your digital rights”; provides research materials and has acted as amicus in electronic evidence litigation. *See particularly*, Electronic Frontier Foundation, *Privacy: Stored Communications Act - Internet Law Treatise*, <http://ilt.eff.org/index.php/Privacy: Stored Communications Act> (discussion of SCA)

National Conference of State Legislatures, *Electronic Surveillance Laws* (last updated April 2009) available at <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/ElectronicSurveillanceLaws/tabid/13492/Default.aspx> (comprehensive state-by-state chart of surveillance statutes).

## APPENDIX – TABLE OF CONTENTS

A.	Materials For Understanding and Attacking Improper Authorization for Cell Site Location Data:	
	• <i>In Re: Application</i> , 405 F.Supp.2d 435 (S.D.N.Y 2005) (explaining “hybrid order” by the govt and allowing application, but with limitations).....	1
	• Testimony of the Honorable Stephen William Smith, US Magistrate Judge, U.S. House Hearing on Electronic Communications Privacy Act Reform (June 24, 2010) (describing the chaos among statutes). ....	16
	• <i>In Re Application</i> , 2010 WL 4286365 (S.D. Tex) (Smith, MJ) (rejecting govt application for cell site data and explaining why statutes do not authorize request), <i>appeal pending</i> , No. 11-20884 (5 <sup>th</sup> Cir).....	33
	• Amicus brief of ACLU and EFF in Support of Affirmance, No 11-20884 (5 <sup>th</sup> Cir. 2012) (providing arguments in support of MJ Smith and opposing use of § 2703(d) orders for location data).....	51
	• <i>See also In Re: Application</i> , 620 F.3d 304 (3d Cir. 2010) (analyzing request for cell tower location information and determining a warrant is not required BUT that magistrate judge has discretion to require one ..... (Not included in Appendix)	
B.	News Articles and Advertisements	
	• Drones: “ <i>Here’s Looking at You</i> ,” excerpts from <u>The New Yorker</u> (May 14, 2012) (law enforcement use of drones). ....	118
	• IMEI Catcher/Man-in-the -middle in Arizona case.....	125
	• “ <i>DOJ: Stingray Cellphone Device Falls Under Fourth Amendment, But Don’t Ask About It.</i> ” (Webpost, Nov. 6, 2011 re: Arizona case <i>US v. Rigmaiden</i> ); related article and advertisement for IMEI Catcher. ....	127
	• ACLU Press Release on Cell Phone Tracking (April 6, 2012).....	133
	• UFED Mobile Forensics – advertisement explaining capabilities	

for extracting deleted phone data, call history, text messages, images, contacts lists, geotags etc. from cellphones; ACLU press release regarding police use of such devices during traffic stops in Michigan (April 13, 2011)..... 136

C. Government Response Re: Motion For Discovery (Nov. 2011), *US v. Rigmaiden*, 08-CR-0814-PHX-DGC (D. AZ.) with attached Affidavit of Special Agent Bradley Morrison (describing IMEI catcher used, assuming *arguendo* that this constitutes a Fourth Amendment search, but relying on Rule 41 Tracking Warrant to authorize search)..... 141

Before the  
Committee on the Judiciary  
Subcommittee on the Constitution, Civil Rights, and Civil Liberties  
2237 Rayburn House Office Building  
Washington, D.C. 20515

HEARING ON ELECTRONIC COMMUNICATIONS PRIVACY ACT REFORM  
AND THE REVOLUTION IN LOCATION BASED  
TECHNOLOGIES AND SERVICES

June 24, 2010

Written Testimony of  
United States Magistrate Judge  
Stephen Wm. Smith

Mr. Chairman, Ranking Member, and Members of the Subcommittee:

I am honored by your invitation to testify at today's hearing. I am a U.S. Magistrate Judge for the Southern District of Texas, sitting in Houston. While this testimony is my own, and not offered as the official position of any group or organization, it is a view from the trenches shared by many of my fellow magistrate judges across the country. Before reaching the substance of my testimony, it might be helpful to outline the role of magistrate judges in handling law enforcement requests under ECPA.

### **1. Role of Magistrate Judges in Electronic Surveillance<sup>1</sup>**

There are over 500 federal magistrate judges serving in district courts around the country. In addition to civil matters, our responsibilities on the criminal side generally include almost everything except conducting felony trials. We conduct initial appearances, appoint counsel for indigents, set bail conditions, hold detention hearings, issue criminal complaints and arrest warrants, take grand jury returns, handle extradition requests, misdemeanor trials, competency hearings, and suppression motions. One of our chief functions is to issue search warrants and other orders in aid of criminal investigations. These include electronic surveillance orders for pen registers, trap and trace devices, tracking devices, 2703(d) orders for telephone and e-mail account records and activity. That is where our experience with ECPA comes in.

Although different districts may handle it differently, in most districts there is at least one magistrate judge on criminal duty at all times, ready to take a call 24 hours a day, 7 days a week. In the Houston division we have 5 magistrate judges, and we rotate the criminal duty among ourselves every two weeks. While on duty we carry either a beeper or dedicated cell phone to allow instant access by law enforcement. It is not uncommon for a magistrate judge to be contacted at night or on a weekend to issue electronic surveillance orders in cases of emergency, such as a kidnaping or alien smuggling. With rare exceptions, ECPA orders pertain to ordinary crimes and criminals, not national security or terrorism cases.

The process is *ex parte*, meaning only one party – law enforcement – appears before the magistrate judge. Since this is at the criminal investigation stage, no

---

<sup>1</sup> For purposes of my testimony, "electronic surveillance" includes pen registers, trap and trace devices, tracking devices, cell site information ("CSI"), stored e-mail, telephone and e-mail activity logs, and customer account records from electronic service providers. Wiretap orders, which are issued only by district judges, are not included.

defendant has yet been charged so no defense counsel is there to challenge the government's request. Likewise, no representative of the electronic service provider or the target phone's subscriber is present. In fact, the orders routinely contain gag orders precluding the service provider from advising their customers that the government is accessing their cell phone or e-mail account records. The public rarely learns about these orders, even long after issuance, because they are routinely placed under indefinite (*i.e.*, permanent) seal.

Actual data on the number of electronic surveillance orders issued under ECPA is not readily available, as far as I know.<sup>2</sup> However, some idea can be gleaned from a recent survey by the Federal Judicial Center.<sup>3</sup> This study, which looked at the prevalence of completely sealed cases in federal court, surveyed every federal case filed in all federal courts during 2006. It found that of the 97,155 criminal matters handled by magistrate judges that year, 15,177 were completely sealed from public. The vast majority of those were warrant-related applications.

Another data point is provided by a local survey of such orders issued by our court in Houston from 1995 through 2007. According to that survey, Houston's five magistrate judges issued a total of 4,234 electronic surveillance orders, or about 325 every year.<sup>4</sup> Considering that this volume was generated by less than 1% of the federal magistrate judges in the country, it is safe to conclude that the 2006 total in the FJC study was not a fluke. A reasonable estimate is that the total number of electronic surveillance orders issued at the federal level each year substantially exceeds 10,000.<sup>5</sup>

---

<sup>2</sup> ECPA requires the Attorney General to report to Congress the number of pen registers applied for annually. See 18 U.S.C. § 3126. However, there is no separate reporting requirement for tracking devices under § 3117 or location information obtained under § 2703(d).

<sup>3</sup> The study is available online at: [www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/\\$file/sealcafc.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/sealcafc.pdf/$file/sealcafc.pdf).

<sup>4</sup> See *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F.Supp.2d 876, 895 (S.D. Tex. 2008).

<sup>5</sup> This does not include the number of such orders issued by state courts.

## 2. In Pursuit of Hidden Elephants<sup>6</sup>

I took the bench in 2004, having no background in criminal law. In fact I had never heard of a trap and trace device until I was confronted with an application for one on my first day of criminal duty. The application also asked for something called “cell site information.” Reluctant to sign what I did not understand, I turned to the United States Code and encountered ECPA for the first time. The experience was frustrating: the terminology was unfamiliar, the organization not intuitive, and the syntax far from straightforward. The casenotes accompanying the statute shed no light; they cited only a handful of lower court decisions not particularly relevant to my questions. No appellate court had ever addressed the issue. I asked my colleagues on the bench, and found they were just as puzzled as I was. I tried to look at sample orders from other courts, but found that they were sealed. I met (several times) with the AUSAs, who basically argued that their request should be granted because other judges had done so.

Still unsatisfied, I plunged into the legislative history of ECPA, reading every committee report and law review article I could find. I contacted law professors who had written about ECPA, as well as a former Congressional staffer who had helped draft the law and subsequent amendments. I met with our local U.S. Marshals, who gave me a tour of their local electronic surveillance shop and a demonstration of the technology. I called various service providers to get their perspective. I then spent several months drafting a memo, setting out my tentative conclusions and supporting analysis. I sent the memo to our local U.S. Attorney, asking him exactly what was wrong with my analysis and why. He forwarded the memo to DOJ, which responded months later with a detailed rebuttal, advocating what has since come to be known as the hybrid theory. Unpersuaded, I issued my first opinion on cell site information in October 2005.<sup>7</sup>

**Prospective CSI.** From my research, I came to understand that ECPA authorized various criminal investigative tools under four different legal standards.

---

<sup>6</sup> “[Congress] does not, one might say, hide elephants in mouseholes.” *Whitman v. American Trucking Ass’n*, 531 U.S. 457, 468 (2001) (Scalia, J.).

<sup>7</sup> *In re Application*, 396 F.Supp.2d 747 (S.D. Tex. 2005). This was actually the second published decision on the topic. Magistrate Judge James Orenstein had issued a decision reaching the same conclusion two months earlier, although the government did not make the hybrid argument in support of that application. See *In re Application of the U.S.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005).

Generally speaking, the more intrusive the investigative tool, the greater the legal process necessary to access it. Visualize it as a 4-story courthouse: pen registers and trap/trace devices are on the ground floor, having the least demanding standard (“certified relevance”); stored communications and account records are on the second floor, accessible with “specific and articulable facts”;<sup>8</sup> tracking device warrants are on the third floor, covered by the familiar Rule 41 “probable cause” standard; wiretap orders are on the top floor, with their “super-warrant” requirements. A chart illustrating this “Electronic Surveillance Courthouse” is attached as Exhibit A.<sup>9</sup>

The essential difficulty, of course, is that ECPA does not explicitly refer to “cell site” or other location information from a cell phone. In the case before me, the Government sought compelled access to a full range of cell site information (CSI) on a prospective basis.<sup>10</sup> My basic approach was to determine which floor of the courthouse was the best fit for this type of request. Because the Government’s stated purpose was to locate the target phone user in real time, the most obvious candidate seemed to be the third floor, for tracking devices. The statutory definition of a tracking device is very broad and unqualified, and could easily be read to encompass the unlimited CSI sought here.<sup>11</sup> Moreover, none of the other categories of electronic surveillance seemed to fit. The pen register standard was ruled out by a proviso in a 1994 statute known as CALEA.<sup>12</sup> The wiretap standard did not apply because CSI does not reveal the contents of a communication. The Stored Communications Act (SCA) standard did not seem to apply for two reasons: the definition of “electronic

---

<sup>8</sup> This is an oversimplification, but sufficient for our purpose. *See* 18 U.S.C. § 2703.

<sup>9</sup> Again, this chart oversimplifies in several respects. For example, it ignores the complicating distinction between communications held in a remote computing service and those held in electronic storage by an electronic communications service provider. It also excludes non-judicial processes such as administrative and grand jury subpoenas.

<sup>10</sup> The application sought “the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls) and, if reasonably available, during the progress of a call,” in addition to “the strength, angle, and timing of the caller’s signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture.” 390 F. Supp. 2d at 749.

<sup>11</sup> *See* 18 U.S.C. § 3117(b) (“the term ‘tracking device’ means an electronic or mechanical device which permits the tracking of the movement of a person or object.”).

<sup>12</sup> The Communications Assistance to Law Enforcement Act, 47 U.S.C. § 1002(a)(2).

communication” specifically excludes information from a tracking device;<sup>13</sup> and the structure of the SCA was inherently retrospective, allowing access to documents and records already created, as opposed to prospective real time monitoring. I concluded that there was “no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. § 3117, which routinely require probable cause.”<sup>14</sup>

Other magistrate judges soon began to weigh in with published decisions of their own. Many agreed with me, some did not. The first opinion with a contrary view was issued in December 2005 by Magistrate Judge Gabriel Gorenstein in the Southern District of New York.<sup>15</sup> He held that a limited form of prospective CSI<sup>16</sup> could be obtained under the SCA standard of specific and articulable facts, a lesser showing than probable cause. His opinion accepted the Government’s hybrid theory and provided what remains its most cogent expression to date. In essence, that theory argued that a lesser standard for obtaining this information could be implied from a combination of provisions in three separate statutes.<sup>17</sup> Even as he was adopting the hybrid theory’s conclusion, Judge Gorenstein declared the result “unsatisfying,”

---

<sup>13</sup> 18 U.S.C. § 2510(12)(C).

<sup>14</sup> 396 F. Supp.2d at 757. The opinion closed by expressing hope “that the government will seek appropriate review by higher courts so that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis.” *Id.* at 765. Unfortunately, with a single exception in five years, that plea has fallen on deaf ears.

<sup>15</sup> 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

<sup>16</sup> His order “contemplates the production only of: (1) information regarding cell site location that consists of the tower receiving transmissions from the target phone (and any information on what portion of that tower is receiving a transmission, if available); (2) tower information that is tied to a particular telephone call made or received by the user; and(3) information that is transmitted from the provider to the Government.” 405 F. Supp. 2d at 450.

<sup>17</sup> I have compared this analysis (perhaps uncharitably) to a three-rail bank-shot: The first rail is the Pen Register Statute (as amended by the 2001 Patriot Act), asserted to be the exclusive means by which law enforcement might acquire non-content signaling information such as cell site data. The second rail is the 1994 CALEA statute, which provides that location information such as cell site data cannot be obtained “solely pursuant” to a pen/trap order. This was interpreted to mean that, while a pen/trap order is still a necessary condition for compulsory disclosure of cell site data, it is no longer sufficient, and must be combined with some additional authority. According to the Government, this authority is found in the third rail, otherwise known as the SCA, which allows Government access to cell phone customer records upon a showing of “specific and articulable facts.”

given the lack of clear guidance from Congress.<sup>18</sup> Finally, he emphasized that his ruling was restricted to a limited form of CSI yielding only generalized location data.<sup>19</sup>

A spate of magistrate judge opinions followed in the next three years, and eventually even a few district judges weighed in. Surveying the published opinions, it is fair to conclude that the majority held that probable cause is the appropriate standard for government access to prospective cell site information. A minority of published decisions, following Judge Gorenstein, allow access under the lesser “specific and articulable facts” standard. Significantly, each of these opinions also restrict their holdings to limited CSI; not one reported decision has ever allowed access to unlimited (*i.e.*, multi-tower, triangulation or GPS) location data on anything other than a probable cause showing.<sup>20</sup> A chart of all published decisions to date concerning prospective cell site information is attached as Exhibit B.

**Historical CSI.** A later round of published decisions centered on the question of government access to historical cell site data. The first wave of CSI decisions, even those requiring probable cause for prospective location information, had assumed or suggested that historical location information was not materially different from other forms of account records or customer information in the hands of the phone company, and therefore obtainable under the lesser standard of SCA § 2703(d). Although not the first decision to challenge that consensus, the most prominent was issued in 2008 by Magistrate Judge Lisa Pupo Lenihan on behalf of all magistrate judges sitting in the Western District of Pennsylvania.<sup>21</sup> Judge Lenihan reasoned that the text and legislative history of ECPA and its amendments warranted no “distinction between real-time (‘prospective’) and stored (‘historic’) cell-phone-derived

---

<sup>18</sup> 405 F. Supp. 2d at 442.

<sup>19</sup> *Id.* at 449-50.

<sup>20</sup> Most magistrate judges have not taken the time to issue published opinions on this question, so the possibility exists that published opinions are not a representative sample of magistrate judge opinion as a whole. Indeed, some standard government applications make the claim that “the silent majority of magistrate and district courts that routinely grant pen/trap/cell orders under the combined authority of Pen/Trap and SCA continue to do so without resort to publishing decisions affirming their current practice thus permitting the minority view to appear more pervasive than it is.”

<sup>21</sup> 534 F. Supp. 2d 585 (W.D.Pa. 2008).

movement/location information.”<sup>22</sup> Her decision is currently on appeal before the U.S. Court of Appeals for the Third Circuit. It is the first and to my knowledge the only time the Government has appealed any district court ruling on cell phone tracking. A listing of decisions addressing the standard for historical cell site information is included on Exhibit B.

Uncertainty over cell phone location information is hardly the only difficulty magistrate judges have encountered in dealing with ECPA. For example, there is the issue of post-cut-through dialed digits;<sup>23</sup> many others could be added. Those matters are beyond the scope of today’s hearing, so there is no need to address them here. But when the Subcommittee does decide to take up those matters we hope that you will again afford magistrate judges the opportunity to offer you the benefit of our experience.

### **3. A Modest Prescription: Simplicity and Transparency**

ECPA was passed in 1986 as a laudable attempt to balance the privacy rights of citizens and the legitimate interests of law enforcement, given the communications technology of that day. In reforming and updating ECPA for the 21<sup>st</sup> century, the task of finding the appropriate balance belongs first of all to the political branches. Obviously, there are important First and Fourth Amendment concerns to be weighed. As a judicial officer, I do not presume to advocate for either side of that debate. That said, from a magistrate judge’s perspective, there are two systemic flaws in the existing statutory scheme that ought not be preserved in the next.

***Undue complexity.*** The new statute should clearly specify the types of information available and the legal showing required for government access. To the extent distinctions must be made, legal standards should not be tied to a particular device or form of technology, which is probably on the road to obsolescence as you debate it. That type of standard inevitably presents judges with the most vexing of interpretive choices, forcibly fitting the round peg of tomorrow’s technology into the square hole of yesterday’s.

As a matter of logic, the legal standards for government access to location information should be geared to the level of intrusion into citizens’ privacy. But in

---

<sup>22</sup> Id. at 601.

<sup>23</sup> See *In re Application of U.S.*, 622 F. Supp. 2d 411 (S.D. Tex. 2007) (Rosenthal, D.J.); *In re Application of U.S.*, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (Azrack); *In re Application*, 441 F. Supp. 2d 816 (S.D. Tex. 2006) (Smith).

my view the temptation to draw fine distinctions for different ways of monitoring cell phone location ought to be resisted. Even as to existing technology, those distinctions can be difficult to draw in the abstract. CSI comes in a wide variety of forms, offering differing tracking capabilities: Is there a meaningful distinction between CSI from a single urban tower and that from multiple rural towers? Between registration information or call-identifying information? What about “pings” or calls initiated by law enforcement? Should a different standard apply for location information pertaining to third parties calling or called by the target phone? How does one calibrate the relative degree of intrusion of such monitoring techniques, given that the precision of the location information obtained will vary from case to case, often depending on inferences drawn from other sources? For instance, when law enforcement already knows the business and residential addresses of the target (or the target’s family, friends, and associates), a single phone call signal captured from a single tower may be all that’s needed to reliably pinpoint a target’s exact location at a given time.

Similar difficulties will plague any attempt to distinguish between historical and prospective cell phone information. How is “historical” to be defined – one second after transmission?<sup>24</sup> One hour? One day? One month? The case law to date has understandably sidestepped this knotty issue.<sup>25</sup> To avoid confusion, any dividing line will have to be explicit, and necessarily arbitrary. The term “prospective” is also ambiguous; although often employed as a synonym for “real-time,” they are not really the same thing.<sup>26</sup> Real-time monitoring captures CSI the instant it is transmitted; it is the polar opposite of historical CSI. On the other hand, prospective CSI may be understood as referring to that generated anytime after the court issues its order. Thus, prospective CSI may well include not only real-time CSI, but also historical CSI generated while the order is in effect.<sup>27</sup> And what about historical CSI that is captured only at the instigation of law enforcement, and for which the provider has

---

<sup>24</sup> See Albert Gidari Jr., *Companies Caught in the Middle*, 41 U.S.F. L. Rev. 535, 544 (2007) (“In essence, [cell tower registration information] becomes historical, transactional information within a millisecond of when the provider receives it.”).

<sup>25</sup> In my orders I take the position that “historical” CSI means any data existing as of the date of the order. This avoids the need to pick an arbitrary age limit.

<sup>26</sup> See *In re Application of the U.S.*, 402 F. Supp. 2d 597, 599 & n.5 (D. Md. 2005) (Bredar).

<sup>27</sup> Pen/trap orders typically expire after 60 days, although they may be renewed an unlimited number of times. 18 U.S.C. § 3123(c)(2).

no legitimate business reason to generate or maintain on its own. Should the standard to *create* CSI be different than that to *retrieve* CSI maintained in the ordinary course of business?

The task of drafting a rational, readily comprehended, easily administered statutory scheme to govern law enforcement access to electronic communications is daunting. Complicating that effort – by multiple distinctions based on predicted intrusion levels for different forms of location data – seems not only ill-advised, but also counter-productive. It’s also likely to prove a waste of time in the wake of technology’s inexorable advance.

**Undue Secrecy.** As pointed out earlier, the vast majority of electronic surveillance orders are issued under seal. This of course is understandable – immediate disclosure of the target’s name and number might defeat the purpose of the surveillance. The problem is the duration and extent of that secrecy.

Under ECPA, secrecy is achieved in two-ways: (1) gag orders preventing service providers from informing customers about law enforcement monitoring of their cell phone and e-mail usage; and (2) sealing orders denying public access to judicial orders.<sup>28</sup> Typically, electronic surveillance orders contain both types of provisions, but rarely impose an expiration period; instead, those orders remain in place “until further order of the court.”<sup>29</sup> The catch is that there is no mechanism in place for the judge to revisit the sealing order. She does not retain jurisdiction over the case, which is not a “case” at all but an investigation that may or may not ripen into a real case. Other surveillance applications pertaining to that investigation will be given a separate case number and assigned to the judge on duty at the time.<sup>30</sup> The

---

<sup>28</sup> Pen register orders must be sealed, and must direct the provider not to disclose to anyone the existence of the order or the investigation, “until otherwise ordered by the court.” 18 U.S.C. § 3123(d)(1) & (2). By contrast, the SCA does not require § 2703(d) orders to be sealed, and allows for “preclusion of notice” to others only if there is reason to believe the investigation would be jeopardized or other adverse consequences would result. 18 U.S.C. § 2705(b)(1)-(5). As a practical matter, the government routinely combines pen/trap applications with requests for customer information under § 2703(d), and so gets the benefit of the more restrictive pen register provisions.

<sup>29</sup> *In Re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 879-80 (S.D. Tex. 2008).

<sup>30</sup> In my court I have devised a protocol to deal with this problem: the order is initially sealed for 180 days, subject to extension upon a certification from the AUSA that the investigation is still active or that exceptional circumstances warrant the extension. *Id.* at 895.

upshot of this system is that, once sealed, an electronic surveillance order is likely to remain sealed long after the underlying investigation is closed, if not forever. This has been confirmed by a study of electronic surveillance orders issued by the Houston Division from 1995 through 2007. Out of 3,886 orders initially sealed “until further order of the court,” 3,877 or 99.8% were still under seal as of April 2008.<sup>31</sup>

The brunt of such secrecy is not necessarily borne by the surveillance targets who are ultimately charged with a crime. After all, they are entitled to discover the nature and source of the prosecution’s evidence, including electronic surveillance orders leading to arrest. Suppression motions are available in the event of a constitutional violation.<sup>32</sup> But not everyone caught up in the web of electronic surveillance is ultimately charged with a crime. Any target is likely to call or be called by family, friends, associates, or even total strangers who have no connection to a criminal enterprise. Yet by the fortuity of a single call, these by-standers may be swept up in a criminal investigation, their cell phone use monitored and their location tracked in real time. Unlike criminal defendants, however, these presumably law-abiding citizens will never find out. The phone company cannot tell them, and court-house records will disclose nothing. Ordinarily, a citizen whose house or office is searched is provided a warrant duly signed by a judicial officer, giving notice of the particulars of the search.<sup>33</sup> When a citizen wishes to challenge the legitimacy of a law enforcement search of his home pursuant to a warrant, the law affords due process for that purpose. But when searches are shrouded in permanent secrecy, as in most cases of electronic surveillance,<sup>34</sup> due process becomes a dead letter.

Such secrecy also has a pernicious impact on the judicial process of statutory interpretation. Any statute has its share of ambiguity and uncertainty, which is

---

<sup>31</sup> See Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 Fed. Cts. L. Rev. 177, 209-10 (2009) (hereafter “*Kudzu*”).

<sup>32</sup> See *United States v. Forest*, 355 F.3d 942 (6th Cir. 2004).

<sup>33</sup> These procedures are specified in Rule 41, which incidentally was amended in December 2006 to cover tracking device warrants. The rule does allow for deferred notice in special circumstances.

<sup>34</sup> See *Kudzu*, *supra* at 208-211. There is also evidence of a trend toward permanent sealing of ordinary search warrants issued under Rule 41. *Id.* at 210. Until very recently, the sealing of a search warrant was regarded as an “extraordinary action” to be taken only in exceptional circumstances. See 3A Wright, King & Klein, *Federal Practice and Procedure: Criminal* 3D § 672, at 332-33 (2004).

resolved, case by case, through lower court rulings subject to review and correction by the courts of appeal and, ultimately, the Supreme Court. But this process of refinement and correction has not happened for ECPA. In a recent article I described this legal “black hole” for electronic surveillance orders:

Due to a peculiar combination of circumstances, these sealed orders are entirely off the radar screen, not only for the public at large, but also for appellate courts. Consider a typical pen register order. The only affected party which might have an incentive to object – the targeted e-mail customer or cell phone user – is never given prior notice of the order; in fact, the electronic service provider is usually forbidden from disclosing its existence. The provider is compensated for most expenses in complying with the order; any uncompensated inconvenience hardly justifies an appeal. The government obviously has no reason to object when its application is granted; in the rare case of a denial, why risk an appeal that could make “bad law”? There are always other magistrate judges to try.

Add a sealing order to this mix, and the outcome is a lacuna of law from which little light escapes. This is especially unfortunate because [ECPA] is fiendishly complex, made more so by the passage of the Patriot Act in 2001. Each year . . . busy magistrate judges issue hundreds of *ex parte* cell phone tracking orders with literally no appellate guidance concerning the proper showing for their issuance – probable cause versus something less. . . Thus, when it comes to marking the bounds of legitimate government intrusion into our electronic lives, each magistrate judge has effectively become a law unto himself. This cannot be a good thing.<sup>35</sup>

The case now before the Third Circuit is the exception that proves the rule. The first appellate court decision on the proper standard for government access to cell site data will be handed down nearly a generation after ECPA was passed, and nearly a decade after its amendment by the Patriot Act. At that rate, cell site data will likely be a quaint technological memory before the next appellate court can consider it.<sup>36</sup>

---

<sup>35</sup> *Kudzu*, *supra* at 211-12.

<sup>36</sup> One of the few appellate cases to deal with electronic surveillance in any respect illustrates the conundrum. *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008). The case arose after

Another consequence of this breakdown in the normal process of appellate review is “rent seeking”<sup>37</sup> on the part of prosecutors. Given the ambiguity and complexity of ECPA, reasonable judges will disagree on its application. Understandably then, prosecutors will tend to gravitate toward a judge who is known to view their requests less critically. The majority of electronic surveillance applications will thus be channeled to judges more inclined to grant them. The inevitable result of such electronic surveillance rent-seeking will be diminished privacy protection for the public as a whole. It may well be that a fully-informed public would not object to this trade-off in personal privacy for the sake of more efficient law enforcement. The problem is that, due to ECPA’s regime of secrecy, the public is not fully informed, and can be only dimly aware of the depth and breadth of electronic surveillance carried out under current law.

**Possible Reforms.** There are a number of ways to reduce secrecy and enhance transparency. Here are some that come to mind:

- elimination of automatic sealing for pen register orders,<sup>38</sup>
- use of less restrictive techniques such as redaction of target names, phone numbers, and other identifying information;
- clear standards and duration limits for sealing and non-disclosure orders;
- clear standards and limits on the number of renewal orders;
- post-acquisition notice of tracking orders to cell phone users,<sup>39</sup>
- more detailed, complete, and public reporting of electronic surveillance

---

a magistrate judge unsealed *ex parte* orders granting government access to plaintiff’s e-mails under the SCA. A panel of the Sixth Circuit initially held unconstitutional parts of the SCA which permitted access to e-mail without prior notice or a probable cause warrant. 490 F.3d 455, 461 (6th Cir. 2007). The panel’s decision was vacated and the case dismissed by the en banc court for lack of ripeness. Twenty-four years after ECPA, and one of its core provisions is not yet ripe for appellate review.

<sup>37</sup> I hesitate to use the term “judge shopping,” because I do not wish to imply that the AUSAs and law enforcement officers with whom I work are anything less than ethical and dedicated professionals. I would do the same in their shoes.

<sup>38</sup> Some judges question the need for any judicial role in the issuance of pen/trap orders. Under ECPA the judge’s role is a purely ministerial one of attesting to the prosecutor’s certification that the requested order is relevant to an ongoing criminal investigation.

<sup>39</sup> See FED. R. CRIM. P. 41(f)(2)(C).

orders by DOJ.<sup>40</sup>

Other commentators have suggested extending the Wiretap Act's exclusionary rule to all types of electronic surveillance orders under ECPA, as well as enhancing civil remedies and penalties for ECPA violations.<sup>41</sup> These ideas are also worth considering.

Whatever the details, the guiding principles for ECPA reform should be brighter lines and more light. Simplicity may not be entirely achievable in a statute dealing with complicated technology. Likewise, transparency is not practicable for every phase of a criminal investigation. But complexity and secrecy take hidden tolls in the form of diminished privacy protection, unchecked judicial power, and public confidence in the judicial system.<sup>42</sup> The 21<sup>st</sup> century version of ECPA must recognize these dangers, and take necessary measures to avoid them.

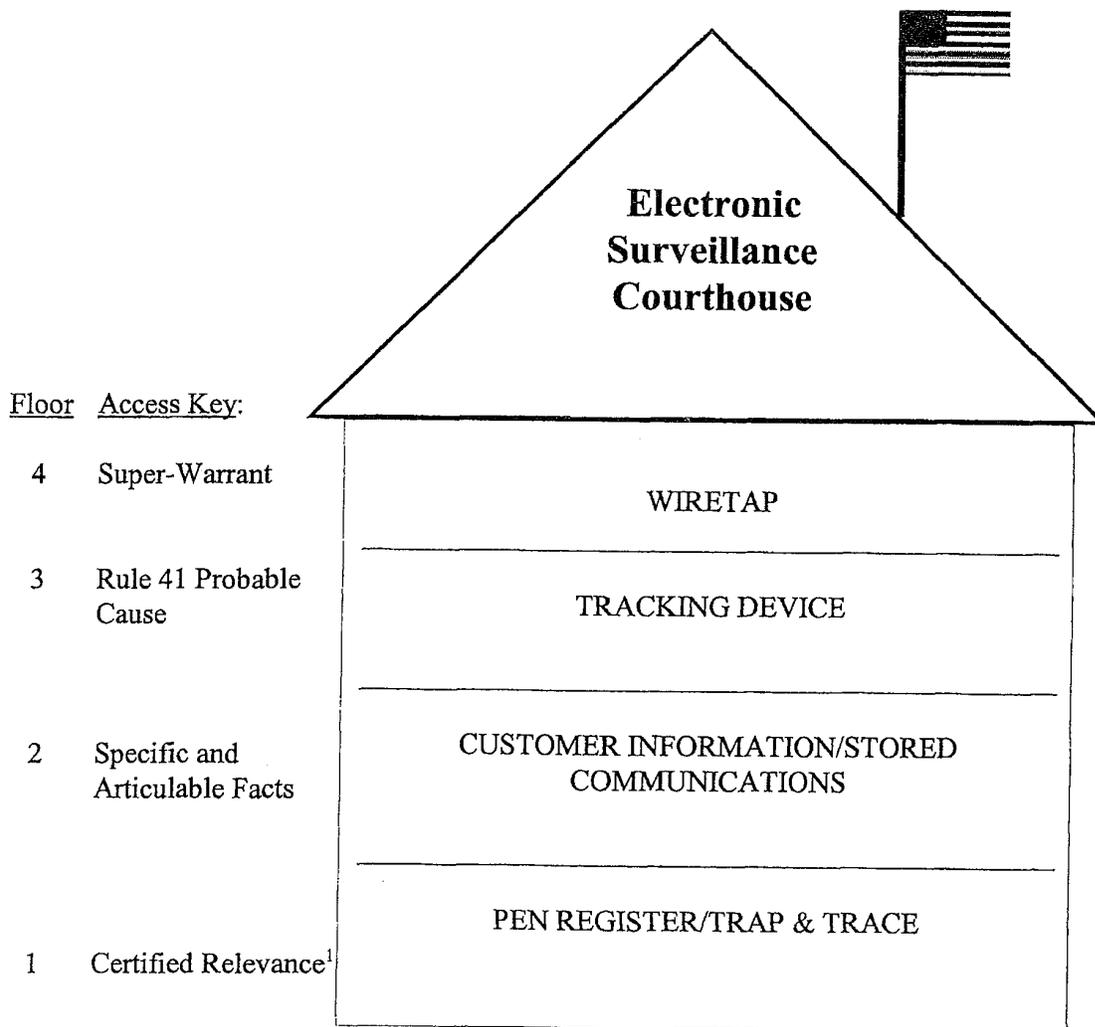
---

<sup>40</sup> See K. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. Rev. 589, 633-34 (2007).

<sup>41</sup> See O. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would change Computer Crime Law*, 54 Hastings L.J. 805 (2003); S. Freiwald, *Online surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9 (2004).

<sup>42</sup> See *Richmond Newspapers Inc. v. Virginia*, 448 U.S. 555, 571-72 (1980) (“[E]specially in the administration of criminal justice, the means used to achieve justice must have the support derived from public acceptance of both the process and its results. . . . People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing.”).

# EXHIBIT A



<sup>1</sup> Not Pictured: Administrative Subpoena  
Grand Jury/Trial Subpoena  
Consent  
Written Request Relating to Telemarketing Fraud

**EXHIBIT B**  
**Summary of Reported Cell Site Decisions**  
**(as of June 1, 2010)**

**I. Prospective Cell Site Information (CSI)**

**A. Applications Denied Without Probable Cause**

**1. Unlimited CSI (multi-tower, triangulation, GPS)**

- *CSI Houston I*, 396 F. Supp. 2d 747 (S.D. Tex. Oct. 14, 2005) (Smith)
- *CSI Washington I*, 2005 WL 3658531 (D.D.C. Oct. 26, 2005) (Robinson)
- *CSI Baltimore I*, 402 F. Supp. 2d 597 (D. Md. Nov. 29, 2005) (Bredar)
- *CSI Washington II*, 407 F. Supp. 2d 132 (D.D.C. Dec. 16, 2005) (Facciola)
- *CSI Washington III*, 407 F. Supp. 2d 134 (D.D.C. Jan. 6, 2006) (Facciola)
- *CSI Fort Wayne*, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Lee, D.J.)
- *CSI Milwaukee II*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (Adelman, D.J.)
- *CSI Corpus Christi*, 2007 WL 3342243 (S.D. Tex. Nov. 7, 2007) (Owsley)
- *CSI Pittsburgh*, 534 F. Supp. 2d 585 (W.D. Pa. Feb. 19, 2008) (Lenihan), *aff'd* 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008) (McVerry, D.J.)

**2. Limited CSI (single tower, call -related)**

- *CSI New York I*, 396 F. Supp. 2d 294 (E.D.N.Y. Oct. 24, 2005) (granting reconsideration of but adhering to result reported at 384 F. Supp. 2d 562 (E.D.N.Y. Aug. 25, 2005) (Orenstein)
- *CSI Milwaukee I*, 412 F. Supp. 2d 947 (E.D. Wis. Jan. 17, 2006) (Callahan)
- *CSI New York III*, 415 F. Supp. 2d 211 (W.D.N.Y. Feb. 15, 2006) (Feldman)
- *CSI Baltimore II*, 416 F. Supp. 2d 390 (D. Md. Feb. 27, 2006) (Bredar)
- *CSI New York IV*, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006) (Peck)
- *CSI Houston III*, 441 F. Supp. 2d 816 (S.D. Tex. July 19, 2006) (Smith)
- *CSI Baltimore III*, 439 F. Supp. 2d 456 (D. Md. July 24, 2006) (Bredar)
- *CSI Puerto Rico*, 497 F. Supp. 2d 301 (D.P.R. July 18, 2007) (McGiverin, D.J.)
- *CSI New York VII*, 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009) (McMahon, D.J.)

**B. Applications Granted With Less Than Probable Cause**

**1. Unlimited CSI (multi-tower, triangulation, GPS)**

No reported opinions.

## 2. Limited CSI (single tower, call-related)

- *CSI New York II*, 405 F. Supp. 2d 435 (S.D.N.Y. Dec. 20, 2005) (Gorenstein)
- *CSI Shreveport*, 411 F. Supp. 2d 678 (W.D. La. Jan. 26, 2006) (Hornsby)
- *CSI Charleston*, 415 F. Supp. 2d 663 (S.D.W. Va. Feb. 17, 2006) (Stanley) (granting the application to locate a non-subscriber, while rejecting the hybrid theory to locate subscribers)
- *CSI Houston II*, 433 F. Supp. 2d 804 (S.D. Tex. Apr. 11, 2006) (Rosenthal, D.J.)
- *CSI New York V*, 460 F. Supp. 2d 448 (S.D.N.Y. Oct. 23, 2006) (Kaplan, D.J.)
- *CSI Sacramento* 2007 WL 397129 (E.D. Ca. Feb. 1, 2007) (Hollows)
- *CSI Houston IV*, 622 F. Supp. 2d 411 (S.D. Tex. Oct. 17, 2007) (Rosenthal, D.J.)
- *CSI New York VI*, 632 F. Supp. 2d 202 (E.D.N.Y. Nov. 26, 2008) (Garaufis, D.J.)

## II. Historical Cell Site Information

### A. Applications Denied Without Probable Cause

- *CSI Fort Wayne*, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Lee, D.J.)
- *CSI Pittsburgh*, 534 F.Supp.2d 585 (W.D. Pa. Feb. 19, 2008) (Lenihan), *aff'd* 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008) (McVerry, D.J. ). This case is currently on appeal to the Third Circuit.

### B. Applications Granted With Less Than Probable Cause\*

- *CSI Boston*, 509 F. Supp. 2d 76 (D. Mass Sept. 17, 2007) (Stearns, D.J.) (reversing 509 F. Supp. 2d 64 (D. Mass. July 27, 2007) (Alexander, M.J.))
- *United States v. Suarez-Blanca*, 2008 WL 4200156 (N.D. Ga. April 21, 2008) (Baverman)
- *United States v. Benford*, 2010 WL 12666507 (N.D. Ind. March 26, 2010) (Moody, D.J.)

\*Note: Other decisions have granted such requests without extended discussion.

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, and the Electronic Frontier Foundation as  
Amici Curiae in Support of Affirmance**

---

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

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, and Electronic Frontier Foundation 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

## TABLE OF CONTENTS

CERTIFICATE OF INTERESTED PERSONS .....	i
TABLE OF AUTHORITIES .....	iv
STATEMENT OF AMICI CURIAE .....	1
STATEMENT REGARDING ORAL ARGUMENT .....	3
INTRODUCTION .....	4
ARGUMENT .....	6
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 ...	6
A. Statutory Background .....	7
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 ...	8
C. None Of Professor Kerr’s Jurisdictional Arguments Alter The Conclusion That § 2703(d) Gives Magistrate Judges Discretion To Require A Search Warrant .....	13
D. The Doctrine Of Constitutional Avoidance Requires This Court To Construe § 2703(d) As Giving Judges Discretion To Require A Warrant ..	18
II. THE GOVERNMENT NEEDS A WARRANT BASED UPON PROBABLE CAUSE TO OBTAIN ACCESS TO 60 DAYS’ WORTH OF HISTORICAL CELL PHONE LOCATION DATA.....	20
A. Obtaining 60 Days’ Worth Of Cell Phone Location Data Is A “Search” Under The Fourth Amendment Requiring A Warrant Based Upon Probable Cause .....	22
B. Cell Phone Providers’ Ability To Access Customers’ Location Data Does Not Eliminate Cell Phone Users’ Reasonable Expectation Of Privacy In That Data .....	33

- C. The Compulsory Process Cases Do Not Change The Result.....45
- III. THE MAGISTRATE JUDGE’S FACTUAL FINDINGS ARE NOT BEFORE THIS COURT, AND EVEN IF THEY WERE, NEITHER LOWER COURT COMMITTED REVERSIBLE ERROR.....48
  - A. The Magistrate’s Findings Of Facts Are Not Before This Court.....49
  - 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 .....50
  - C. Even If This Court Decides To Review The “Findings of Facts,” The Magistrate Judge Did Not Commit Clear Error .....53
- CONCLUSION.....56

## TABLE OF AUTHORITIES

### Cases

<i>Alden Mgmt. Servs., Inc. v. Chao</i> , 532 F.3d 578 (7th Cir. 2008) .....	9
<i>Anderson v. City of Bessemer City</i> , 470 U.S. 564 (1985).....	53
<i>Brinegar v. United States</i> , 338 U.S. 160 (1949).....	32
<i>California v. Hodari D.</i> , 499 U.S. 621 (1991).....	9
<i>Carder v. Continental Airlines, Inc.</i> , 636 F.3d 172 (5th Cir. 2011) .....	7
<i>Chandler v. Miller</i> , 520 U.S. 305 (1997).....	16
<i>City of Ontario v. Quon</i> , 130 S. Ct. 2619 (2010).....	6, 19, 44
<i>Clark v. Martinez</i> , 543 U.S. 371 (2005) .....	18
<i>Doe v. Broderick</i> , 225 F.3d 440 (4th Cir. 2000).....	44
<i>Donaldson v. United States</i> , 400 U.S. 517 (1971).....	42
<i>Donovan v. Lone Steer, Inc.</i> , 464 U.S. 408 (1984).....	46
<i>Duncan v. Walker</i> , 533 U.S. 167 (2001).....	11
<i>Hoffa v. United States</i> , 385 U.S. 293, 302 (1966) .....	42
<i>In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't</i> , 620 F.3d 304 (3d Cir. 2010) .....	passim
<i>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.;</i> <i>and (3) Authorizing Disclosure of Location-Based Servs.</i> , 727 F. Supp. 2d 571 (W.D. Tex. 2010) .....	52
<i>In re Nwamu</i> , 421 F. Supp. 1361 (S.D.N.Y. 1976) .....	46
<i>Katz v. United States</i> , 389 U.S. 347 (1967) .....	passim
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	27, 28, 37, 56

<i>McDonald v. United States</i> , 335 U.S. 451 (1948) .....	17
<i>Newfield v. Ryan</i> , 91 F.2d 700 (5th Cir. 1937) .....	43
<i>Okla. Press Publ'g Co. v. Walling</i> , 327 U.S. 186 (1946).....	46
<i>Powell v. McCormack</i> , 395 U.S. 486 (1969) .....	32
<i>Reporters Comm. for Freedom of the Press v. AT&amp;T</i> , 593 F.2d 1030 (D.C. Cir. 1978).....	43
<i>Robinson v. Shell Oil Co.</i> , 519 U.S. 337 (1997) .....	7
<i>SEC v. Jerry T. O'Brien, Inc.</i> , 467 U.S. 735 (1984).....	41, 42
<i>See v. City of Seattle</i> , 387 U.S. 541 (1967).....	28, 46
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979) .....	passim
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965).....	17
<i>Stoner v. California</i> , 376 U.S. 483 (1964).....	28
<i>Taylor v. Charter Med. Corp.</i> , 162 F.3d 827 (5th Cir. 1998).....	53
<i>Twp. of Tinicum v. U.S. Dep't of Transp.</i> , 582 F.3d 482 (3d Cir. 2009).....	9
<i>United States v. Allen</i> , 106 F.3d 695 (6th Cir. 1997).....	41
<i>United States v. Di Re</i> , 332 U.S. 581 (1948) .....	56
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008).....	43
<i>United States v. Frazier</i> , 26 F.3d 110 (11th Cir. 1994).....	51, 52
<i>United States v. Gonzales</i> , 121 F.3d 928 (5th Cir. 1997) .....	32
<i>United States v. Howard</i> , 106 F.3d 70 (5th Cir. 1997).....	53
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012) .....	passim
<i>United States v. Karo</i> , 468 U.S. 705 (1984) .....	passim
<i>United States v. Maynard</i> , 615 F.3d 544 (D.C. Cir. 2010).....	4, 21

<i>United States v. Miller</i> , 425 U.S. 435 (1976) .....	passim
<i>United States v. N.Y. Tel. Co.</i> , 434 U.S. 159 (1977).....	35
<i>United States v. O’Brien</i> , 130 S. Ct. 2169 (2010) .....	32
<i>United States v. Paige</i> , 136 F.3d 1012 (5th Cir. 1998).....	41
<i>United States v. Perrine</i> , 518 F.3d 1196 (10th Cir. 2008).....	42
<i>United States v. Place</i> , 462 U.S. 696 (1983) .....	44
<i>United States v. Silva</i> , 957 F.2d 157 (5th Cir. 1992) .....	9
<i>United States v. Singer</i> , 345 F. Supp. 2d 230 (D. Conn. 2004).....	51
<i>United States v. Southland Mgmt. Corp.</i> , 288 F.3d 665 (5th Cir. 2002).....	10
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010).....	passim
<i>United States v. Washington</i> , 573 F.3d 279 (6th Cir. 2009).....	41
<i>United States v. Weed</i> , 184 F. Supp. 2d 1166 (N.D. Okla. 2002) .....	51
<i>United States v. X-Citement Video, Inc.</i> , 513 U.S. 64 (1994).....	19
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978) .....	46

**Statutes**

18 U.S.C. § 2703 .....	passim
18 U.S.C. § 3123 .....	10
18 U.S.C. §§ 2701 .....	6
28 U.S.C. § 636 .....	15
Pub. L. No. 103-414, 108 Stat. 4292 (Oct. 25, 1994).....	12
Pub. L. No. 99-508, 100 Stat. 1848 (1986).....	7

**Other Authorities**

CTIA The Wireless Association, *CTIA’s Semi-Annual Wireless Industry Survey* (2009).....29

*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) .....54*

H.R. Rep. No. 103-827 (1994).....12

S. Hrg. 98-1266 (1984) .....12

S. Rep. No. 99-541 (1986).....12

Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 702 (2011).....29

**Rules**

Fed. R. Evid. 1101 ..... 50, 51, 52

Fed. R. Evid. 201 .....52

## **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.

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<sup>1</sup> 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

---

<sup>1</sup> 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.<sup>2</sup> 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

---

<sup>2</sup> 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.<sup>3</sup>

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,

---

<sup>3</sup> 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).<sup>4</sup> 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

---

<sup>4</sup> 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,<sup>5</sup>

---

<sup>5</sup> 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.”<sup>6</sup> *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](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).

<sup>6</sup> 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; *see 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.<sup>7</sup> Nor does this

---

<sup>7</sup> 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.<sup>8</sup> *Warshak*, 631 F.3d at 286-88 (holding that the

---

<sup>8</sup> 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.<sup>9</sup> *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

---

<sup>9</sup> 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 COMMITTED 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.<sup>10</sup> 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.<sup>11</sup>

---

<sup>10</sup> 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](http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf).

<sup>11</sup> 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

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



## You're Getting Warmer...

September 26, 2011

Last week, the [Wall Street Journal](#) [profiled](#) the StingRay. And I don't mean the [sea creature](#). The StingRay is a device that acts like a cell phone tower — except it doesn't help your phone complete calls. Rather, it fools your phone into thinking it's connecting to a cell tower and forces your phone to register its location — with the law enforcement agent wielding the device.

According to [the Journal](#), there are two ways that law enforcement can use a StingRay. Either they can point its antenna at a location and collect the cell numbers there and use those numbers to identify the people present. Or, the device can be used to locate a phone when the agents know the number associated with it but don't know exactly where the phone is. To do so, the agents drive around until they get a signal from the phone in question. Think of it as a space-age metal detector or a grown-up version of the [You're Getting Warmer](#) game.

Patents have existed for StingRays, also called AmberJack, KingFish, TriggerFish, and LoggerHead, since at least 2002, and in 2005 the Department of Justice put out [this manual](#) referencing them in passing, but their use is still shrouded in secrecy. And, the government aims to keep it that way. According to the Journal, "The Federal Bureau of Investigation...has a policy of deleting the data gathered in their use, mainly to keep suspects in the dark about their capabilities." And privacy advocates, oversight officials, and good government watch dogs. Oh, and courts. At least one prosecutor obtained a court order to use a StingRay without disclosing to the court what device he was actually using. His explanation to the judge who questioned him on it during the subsequent criminal trial? "It was a standard practice, your honor." Um.

There is simply [too much secrecy](#) surrounding law enforcement's use of and access to cell phone location information. That's why in August, [35 ACLU affiliates filed 381 public records requests in 32 states](#) seeking to learn how their local law enforcement agencies use and access cell phone location information. Information has been trickling in, and we'll be highlighting more of it on this blog and adding it to [this map](#) in the coming days and weeks, so stay tuned. In the meantime, here's what we know about StingRays:

The good news is that, according to the Wall Street Journal, these "devices are sold only to law-enforcement and government agencies." So your crazy ex is not likely to get one and begin stalking your cell phone. The bad news is that while we know these "devices are only sold to law-enforcement and government agencies," that's about all we know. The public has been kept almost entirely in the dark about how they're being used, and it's now sounding like they might be used pretty frequently. The Journal tells us that the Maricopa County, Arizona Sheriff's Department uses the equipment "about on a monthly basis."

And, we got this salient fact in response to our public records request on cell phone location information: [Gilbert, AZ \(which is in Maricopa County\)](#) informed us that the "Gilbert Police Department obtained a \$150,000 grant from the State Homeland Security Program. These funds, along with \$94,195 of R.I.C.O monies, were used to purchase cell phone tracking equipment in June 2008 (total acquisition cost of 244,195)." Did they purchase a StingRay? What other equipment might they have purchased? These two sentences aren't enough for us to know for sure, but we'll do our darnedest to find out.

In the meantime, this is just another reason to [urge your members of Congress](#) to support the bills introduced by Sen. Wyden (D-OR) and Rep. Chaffetz's (R-UT), both called the "Geolocation Privacy and Surveillance Act," which would create location privacy protections for law enforcement and the commercial sector. Supporting the Wyden and Chaffetz bills is just one way to [Demand our dotRights](#) — we shouldn't have to pay for our cell phones with our privacy rights.

*Learn more about location tracking: [Sign up for breaking news alerts](#), [follow us on Twitter](#), and [like us on Facebook](#).*



# Cell Phone Location Tracking Public Records Request

April 6, 2012

All cell phones register their location with cell phone networks several times a minute, and this function cannot be turned off while the phone is getting a wireless signal. The threat to personal privacy presented by this technology is breathtaking.

To know a person's location over time is to know a great deal about who a person is and what he or she values. As the federal appeals court in Washington, D.C. [explained](#):

"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."

The government should have to obtain a warrant based upon probable cause before tracking cell phones. That is what is necessary to protect Americans' privacy, and it is also what is required under the Constitution. (In certain emergency situations, for example to locate a missing person, tracking a cell phone without a warrant is acceptable.)

In *United States v. Jones*, a majority of the Supreme Court recently concluded that the government conducts a search under the Fourth Amendment when it attaches a GPS device to a car and tracks its movements. The conclusion should be no different when the government tracks people through their cell phones, and in both cases a warrant and probable cause should be required.

Until now, how law enforcement agents use cell phone tracking has been largely shrouded in secrecy. What little was known suggested that law enforcement agents frequently tracked cell phones without obtaining a warrant based on probable cause.

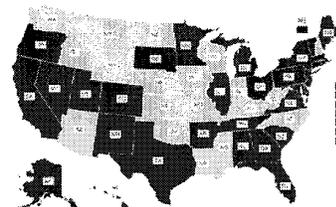
In August 2011, 35 ACLU affiliates filed over 380 public records requests with state and local law enforcement agencies to ask about their policies, procedures and practices for tracking cell phones.

What we have learned is disturbing. While virtually all of the over 200 police departments that responded to our request said they track cell phones, only a tiny minority reported consistently obtaining a warrant and demonstrating probable cause to do so. While that result is of great concern, it also shows that a warrant requirement is a completely reasonable and workable policy.

The government's location tracking policies should be clear, uniform, and protective of privacy, but instead are in a state of chaos, with agencies in different towns following different rules — or in some cases, having no rules at all. It is time for Americans to take back their privacy. Courts should require a warrant based upon probable cause when law enforcement agencies wish to track cell phones. State legislatures and Congress should [update](#) obsolete electronic privacy laws to make clear that law enforcement agents should track cell phones only with a warrant.

## TAKE ACTION

[Tell Congress: Support the GPS Act! »](#)



[MAP: Is Your Local Law Enforcement Tracking Your Cell Phone's Location?](#)

## MORE

[What our Public Records Act Requests Sought »](#)

Below is an overview of our findings and recommendations.

### **The Documents: The Government Is Routinely Violating Americans' Privacy Rights Through Warrantless Cell Phone Tracking**

The ACLU received over 5,500 pages of documents from over 200 local law enforcement agencies regarding cell phone tracking. The responses show that while cell phone tracking is routine, few agencies consistently obtain warrants. Importantly, however, some agencies do obtain warrants, showing that law enforcement agencies can protect Americans' privacy while also meeting law enforcement needs.

The government responses varied widely, and many agencies did not respond at all. The documents included statements of policy, memos, police requests to cell phone companies (sometimes in the form of a subpoena or warrant), and invoices and manuals from cell phone companies explaining their procedures and prices for turning over the location data.

### **The overwhelming majority of the over 200 law enforcement agencies that provided documents engaged in at least some cell phone tracking — and many track cell phones quite frequently.**

Most law enforcement agencies explained that they track cell phones to investigate crimes. Some said they tracked cell phones only in emergencies, for example to locate a missing person. Only 10 said they have never tracked cell phones.

Many law enforcement agencies track cell phones quite frequently. For example, based on invoices from cell phone companies, it appears that Raleigh, N.C. tracks hundreds of cell phones a year. The practice is so common that cell phone companies have manuals for police explaining what data the companies store, how much they charge police to access that data, and what officers need to do to get it.

**Most law enforcement agencies do not obtain a warrant to track cell phones, but some do, and the legal standards used vary widely.** Some police departments protect privacy by obtaining a warrant based upon probable cause when tracking cell phones. For example, police in the County of Hawaii, Wichita, and Lexington, Ky. demonstrate probable cause and obtain a warrant when tracking cell phones. If these police departments can protect both public safety and privacy by meeting the warrant and probable cause requirements, then surely other agencies can as well.

Unfortunately, other departments do not always demonstrate probable cause and obtain a warrant when tracking cell phones. For example, police in Lincoln, Neb. obtain even GPS location data, which is more precise than cell tower location information, on telephones without demonstrating probable cause. Police in Wilson County, N.C. obtain historical cell tracking data where it is "relevant and material" to an ongoing investigation, a standard lower than probable cause.

**Police use various methods to track cell phones.** Most commonly, law enforcement agencies obtain cell phone records about one person from a cell phone carrier. However, some police departments, like in Gilbert, Ariz., have purchased their own cell tracking technology.

Sometimes, law enforcement agencies obtain all of the cell phone numbers at a particular location at a particular time. For example, a law enforcement agent in Tucson, Ariz. prepared a memo for fellow officers explaining how to obtain this data. And records from Cary, N.C. include a request for all phones that utilized particular cell phone towers.

**Cell phone companies have worsened the lack of transparency by law enforcement by hiding how long they store location data.** Cell phone companies store customers' location data for a very long time. According to the U.S. Department of Justice, Sprint keeps location tracking records for 18-24 months, and AT&T holds onto them "since July 2008," suggesting they are stored indefinitely. Yet none of the major cell phone providers disclose to their customers the length of time they keep their customers' cell tracking data. Mobile carriers owe it to their customers to be more forthright about what they are doing with our data.

>>ACLU Open Letter to Wireless Carriers on Location Tracking of Cell Phones

*Click here for detailed findings and analysis of the ACLU's cell phone tracking records requests »*

### **The Solutions: What Can Be Done to Protect Privacy**

Cell phone location data is not the sort of information that law enforcement agents should be obtaining without the safeguard of the probable cause standard and review by a judge. That will ensure that legitimate investigations can proceed, while protecting innocent Americans from unjustified invasions of their privacy.

State and federal lawmakers should pass laws requiring a warrant for police to engage in location tracking in non-emergency situations. In Congress, there are two pending efforts: First, bipartisan legislation, entitled the Geolocation Privacy and Surveillance (GPS) Act, is sponsored in the Senate by Senators Ron Wyden (D-Ore.) and Mark Kirk (R-Ill.) and in the House by Representatives Jason Chaffetz (R-Utah), Peter Welch (D-Vt.) and Jim Sensenbrenner (R-Wisc.). The bills would require law enforcement agents to obtain a warrant in order to access location information.

**TAKE ACTION: Tell your representatives in Washington to support these important pieces of legislation »**

The other effort is part of Democratic Vermont Senator Patrick Leahy's proposal to update the 1986 Electronic Communications Privacy Act (ECPA), which the government also uses to secretly access people's email accounts. The bill includes a warrant requirement for real-time tracking, but not for historical location information.

**TAKE ACTION: Ask Congress to update ECPA today »**

In the meantime, more local law enforcement agencies should voluntarily follow the lead of those police departments that already require a warrant and probable cause to track cell phones.

And more states should pass laws requiring their law enforcement agents to obtain a warrant and probable cause to track cell phones.

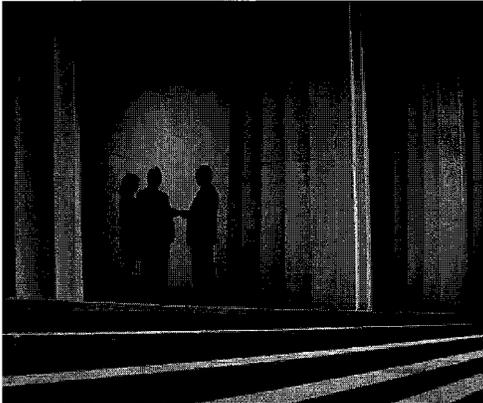
When they have the opportunity, more judges should follow the leads of those judges who have required the government to obtain a warrant based upon probable cause.

Technology is evolving quickly, and often to the detriment of privacy. But how much privacy Americans enjoy is fundamentally a choice that ultimately is ours as a society to make.

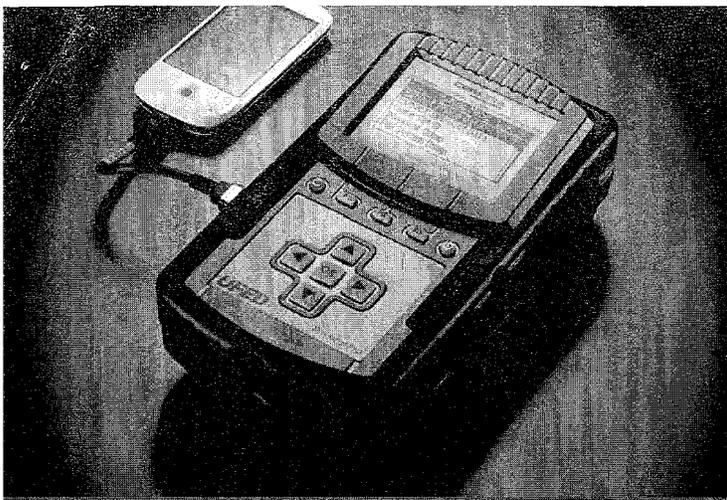
---

Published on *American Civil Liberties Union* (<http://www.aclu.org>)

**Source URL:** <http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request>



**PHYSICAL PRO**  
THE COMPLETE MOBILE FORENSICS SOLUTION



# UFED PHYSICAL PRO

## THE COMPLETE MOBILE FORENSICS SOLUTION

Cellebrite's UFED addresses the growing need for fast, comprehensive mobile forensic capabilities. An add-on module for advanced extraction and analysis of evidence Physical Pro enables the basic UFED system with physical data extraction, file system dump and reconstruction, and password extraction. UFED Physical Pro enables recovery of invaluable evidential information that isn't accessible by logical extraction methods alone. In use by military, law enforcement, governments, and intelligence agencies across the world, UFED Physical Pro allows users to rapidly extract a wide variety of data types in a forensically sound process from both phone and SIM memory. Extracting data in a forensic manner and presenting it with the integrity of the data intact ensures that the evidence will be admissible in court.

### AT A GLANCE

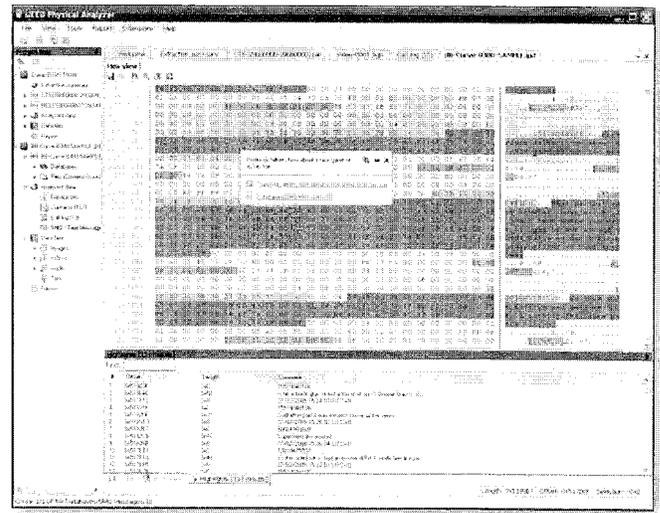
- Complete extraction of existing, hidden, and deleted phone data, including call history, text messages, contacts, images, and geotags
- Powerful search, reconstruction, and analysis of the phone hex dump that can be used for intelligence gathering, investigative research, and as legal evidence in court

Expanded coverage for GPS devices, with mapping of GPS locations on Google Maps and visualization of GPS locations on Google Earth  
 Unrivaled phone coverage and compatibility

### PHYSICAL ANALYZER SOFTWARE TOOL

UFEDs Physical Analyzer provides powerful analysis tools that can be used for intelligence gathering, investigative research:

- Hierarchical "tree" view for easy navigation between phone content, hex dump, files, and analyzed data
- Powerful search tools with parsing and pattern matching
- Presents the location of the analyzed data within the phone memory and file system
- Save, print, customized, and export the extracted data



### MAPPING AND VISUALIZATION

UFED Physical Pro is able to extract extensive information from GPS devices, including latitude and longitude of GPS locations. The Physical Analyzer allows visualization of both existing and deleted locations on Google Earth. In addition, location information from GPS devices and image geotags can be mapped on Google Maps.

## UNRIVALLED PHONE COVERAGE AND COMPATIBILITY

UFED Physical Pro combines the most complete extraction of data with the most comprehensive coverage available on the market.

- Logical data extraction from more than 3,000 mobile phones
- Physical data extraction from more than 700 mobile phones and GPS devices
- File system extraction and reconstruction for more than 900 phones and GPS devices
- Password extraction for more than 650 mobile phones
- Supports all major mobile operating systems, including Windows Mobile, Symbian, iPhone, Brew, Android, and BlackBerry.
- Supports phones regardless of network carrier or technology
- Monthly updates to ensure compatibility with new phones
- Data cables for all supported phones [Live technical assistance, software updates, and cables for all new handsets are included with each product license]

## KEY FEATURES

- Mapping of GPS locations and geotags on Google maps
- Visualization of GPS fixes and locations on Google Earth
- Built in SIM reader
- Unicode supported content extraction
- Multilingual user interface in 14 languages.
- MD5 and SHA256 hash signatures for data verification
- Reports for viewing, saving, printing, exporting, and analyzing extracted data.
- Field-ready mobile forensics – portable, fast and easy to operate, the Ruggedized UFED is battery powered and comes with all accessories needed for harsh field conditions

## UPGRADE TO UFED PHYSICAL PRO

Existing UFED customers can benefit from the Physical Pro's technological advancements with a simple software upgrade, extending the capabilities of both the standard and ruggedized versions of the UFED system.





# ACLU: American Civil Liberties Union of Michigan

## Issues

### ACLU Seeks Records about State Police Searches of Cellphones

FOR IMMEDIATE RELEASE:

April 13, 2011

DETROIT – The American Civil Liberties Union of Michigan urged the Michigan State Police (MSP) today to release information regarding the use of portable devices which can be used to secretly extract personal information from cell phones during routine stops.

For nearly three years, the ACLU has repeatedly asked for this information through dozens of Freedom of Information Act requests, but to date it has not been provided.

Read our letter to the Michigan State Police.

“Transparency and government accountability are the bedrocks of our democracy,” said Mark P. Fancher, ACLU of Michigan Racial Justice Project staff attorney. “Through these many requests for information we have tried to establish whether these devices are being used legally. It’s telling that Michigan State Police would rather play this stalling game than respect the public’s right to know.”

**Several years ago, MSP acquired portable devices that have the potential to quickly download data from cell phones without the owner of the cellphone knowing.**

The ACLU of Michigan expressed concern about the possible constitutional implications of using these devices to conduct suspicionless searches without consent or a search warrant.

In August 2008, the ACLU of Michigan filed its first FOIA request to acquire records, reports and logs of actual use.

Documents provided in response confirmed the existence of these devices, but MSP claimed that the cost of retrieving and assembling the documents that disclose how five of the devices are being used is \$544,680. The ACLU was then asked to pay a \$272,340 deposit before the organization could receive a single document.

In order to reduce the cost, the ACLU of Michigan narrowed the scope of its request. However, each time the ACLU submitted more narrow requests, MSP claimed that no documents exist for that time period and then it refused to reveal when the devices were used so a proper request could be made.

“We should not have to go on expensive fishing expeditions in order to discover whether police are violating the rights of residents they have resolved to protect and serve,” said Fancher.