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

APPENDIX

I. SURVEILLANCE TECHNIQUES[1]

- 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 (9th 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.

---

[1] 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	***Communications Act of 1934***, 48 Stat. 1065, as amended, 47 USC § 153	• defines "common carrier," "wire communications" and other terms. Later statutes refer to these.
1968	***Wiretap Act***, Pub.L. 90-351, Title III § 802, June 19, 1968,as amended, 18 USC § 2510 et seq.	• defines "wire communication" and other terms; refers to Communications Act for some definitions. • amended by ECPA (see below) • prohibits real-time interception and disclosure of certain wire, oral or electronic communications, except as authorized by this statute; • requires that government establish probable cause that a crime has been, or is about to be, committed **and** that wiretap is necessary because traditional law enforcement techniques are not likely to be successful or are too dangerous. • includes an exclusionary rule if unauthorized interceptions occur.

DATE ENACTED	TITLE AND CITATION	PURPOSE/IMPORTANCE
1978	***Foreign Intelligence Surveillance Act (FISA),*** Pub.L. 95-511, Oct. 25, 1978, as amended, 50 USC § 1801 et seq.	• authorizes electronic surveillance (including searches of residences) without court orders for specific foreign intelligence purposes of up to one year; • special FISA court to authorize other surveillance; sealed proceedings
1986	***Electronic Communications Privacy Act –*** (ECPA) Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. § 2510, et. seq. **Three Titles:** **I.** Wiretap Act, 18 USC § 2510-2522 **II.** Stored Communications Act, 18 USC § 2701-2712 **III.** Pen Register & Trap and Trace Devices, 18 USC § 3121-27	• amends the old wiretap statute. • distinguishes between access to real-time data vs. stored records; • defines tracking device • **Wiretap Act**: prohibits real-time interception and disclosure of certain wire, oral or electronic communications, except as authorized by this statute; standards stricter than constitutionally required • **SCA**: applies to historic (non- real time) communications in "electronic storage" or "remote computing storage" by "electronic communications service (ECS)." See details below. • **Pen/TT** order provide real-time data on numbers called from and calling a phone, plus other data • Pen/TT order under § 3123, or FISA, are the *exclusive* 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."

DATE ENACTED	TITLE AND CITATION	PURPOSE/IMPORTANCE
1986	Further, ECPA defines **mobile tracking devices** at 18 USC § 3117	• defines MTD as "electronic or mechanical device which permits the tracking of the movement of an object or person." • new authorization to install such devices, based on a warrant, added to chapter 205 among warrant requirements
1994	***Communications Assistance for Law Enforcement Act (CALEA),*** 47 USC 1001-1010	• amends wiretap, SCA and Pen sections of ECPA • 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. • forbids carriers from providing location information "solely" under pen register and trap & trace orders: 47 USC § 1002(a)(2)(B); • expands privacy protections of ECPA to cordless phones and data transmitted by radio
1999	***Wireless Communication and Public Safety Act,*** 47 USC § 222(f)	• limits carriers' disclosure of "CPNI" - customer proprietary network information, including specifically location information, "unless required by law."
2001	***USA Patriot Act***, Pub.L. 107-56, Title II § 216(a)	• expands definition of available data under pen register order to include "all dialing, routing, addressing, or signaling information."

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 (6th 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
Scope: • 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. Trap and Trace is the same, but for in-coming numbers.
Authorizations: • under § 3122, govt can apply to court if "information likely to be obtained" will be *relevant* to an on-going criminal investigation. • 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.

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 (6th 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*:

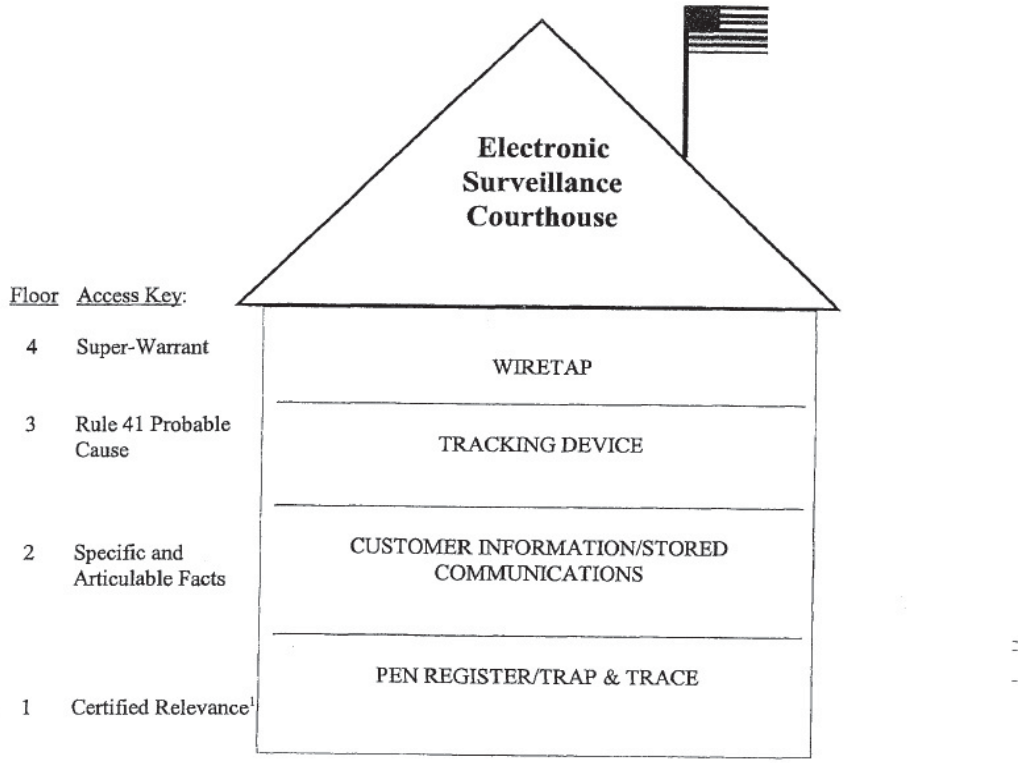
> If you have a cell phone in your pocket, then the government can watch you. Michael Isikoff, *The Snitch in Your Pocket,* Newsweek, Mar. 1, 2010, *available at* http:// www. newsweek. com/ id/ 233916. At the government's request, the phone company will send out a signal to any cell phone connected 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- re asons- for- re alsurveillance. 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 (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 (5th 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
<u>E-MAIL Content</u> • Did they get a search warrant?	Rule 41 F.R.C.P	*US v. Warshak*, 631 F.3d 266 (6th Cir. 2010) says obtaining email content without a warrant violates the 4th Amendment, and if the SCA authorizes this, it is unconstitutional; split in the case law. **Raise this Issue!**
• Did they provide the notice required by FRCP 41?	SCA, 18 USC § 2703(a) incorporates the procedures of Rule 41 warrants	*Warshak,* 631 F.3d 266 (reviews notice provisions but finds any violation not relevant because of good faith issue); *See* 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.
• Did they send a *prospective* "evidence retention" letter to the ISP, asking it to hold everything created until the warrant is obtained?	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.	•*Warshak,* 631 F.3d 266: the concurrence especially is troubled by this "back-door wiretapping," and believes this violates the 4th. 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 4th?

EVIDENCE SOUGHT	AUTHORITY	ISSUES
• 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?	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. *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004); other circuits disagree. Preserve this issue if no warrant is used.
• Was the search warrant overbroad or insufficiently particularized?	FRCP 41; 4th A	Search warrants often ask for "all" email content. Use *Warshak* ("email provides an account of its owner's life") and the Ninth Circuit's case *CDT*, 621 F.3d 1162 (9th Cir. 2010), to argue that grabbing *all* 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.
TEXT MESSAGES • Did they get a warrant? (Probably not – they rely on SCA § 2703(d))	FRCP 41	Apply the reasoning of *US v. Warshak*, 631 F.3d 266 (6th Cir. 2010): if obtaining email content without a warrant violates the 4th 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 *Quon*, 130 S.Ct. 2619 (2010) which dodges the issue but has good language. Ninth Circuit case analogizes IM chat to private call for purposes of consent by one party. *United States v. Meek*, 366 F.3d 705, 711 (9th Cir. 2004).

EVIDENCE SOUGHT	AUTHORITY	ISSUES
CELLPHONE CONTENT • when phone is in the physical possession of the officers, did they get a warrant to search before flipping through it?	4th Amendment	See *Schlossberg v. Solesbee*, 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; *US v. Davis*, 10-CR-339-HA (D. Or 2011) (suppressing evidence derived from warrantless search of cellphone seized incident to arrest); *US v. Wall*, 2008 WL 5381412 (S.D. Fla 2008) (same); *United States v. Park*, No. CR 05-375 SI, 2007 WL 1521573 (N.D.Cal. May 23, 2007) (unpublished); *But see People v. Diaz* (Cal. S.Ct.) (Cellphone is just a "container" that can be opened on search incident to arrest).
• when phone information (texts, contact book, photos) is accessed electronically, did they get a search warrant or rely on the SCA?	18 USC § 2703(a) and (d) – purport to authorize access to stored content	See arguments against warrantless access to email, above under *Warshak*. Challenge this!
GPS Data • GPS precision locators placed on vehicles What about GPS precision locators, if they were present already but just activated by police?	Warrant required warrant? Use *Jones* concurrence by Alito to argue for one; also 18 USC § 3117.	*Jones,* 132 S. Ct. 945. **previous circuit split:** *Compare US v Marquez,* 605 F.3d 604 (8th Cir 2010) (no warrant required); *US v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010) (no warrant required), cert. granted, judgment vacated, 132 S.Ct. 1533 (Feb. 21, 2012), *with US v. Maynard,* 615 F.3d 544 (D.C.Cir. 2010), aff'd sub. nom, *US v. Jones*, 132 S. Ct. 945 (2011).

EVIDENCE SOUGHT	AUTHORITY	ISSUES
• GPS from Cellphones? What kind of order did they get?	18 USC § 3117? 18 USC § 2703(d)? Warrant?	Argue that the principles from *Jones*, *Maynard* and the *Pineda-Moreno* dissent apply. *US v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010) (dissent), cert granted, judgment vacated, 132 S.Ct. 1533 (Feb. 21, 2012); *US v. Maynard,* 615 F.3d 544 (D.C.Cir. 2010), aff'd sub. nom, *US v. Jones*, 132 S. Ct. 945 (2011). Tracking requires a warrant. Rely on *In Re Application*, 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).
<u>Cell Site Data</u> • what kind of order did they use, and what kind of information was sought? - distinguish real time v. historical – plain pen order vs. "hybrid order" • should they need a warrant?		Rely on *In Re Application*, 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).
• what equipment was used to capture the information?		If they use man-in-the-middle or IMEI catchers or other clones, the govt cannot rely on *Smith* and the argument that data was voluntarily given to a third party - argue this is a statutory and 4th Amendment violation

EVIDENCE SOUGHT	AUTHORITY	ISSUES
<u>Pen Register/TT Data</u> • how broad was the information gathered?	Pen statute - 18 USC § **3121-3127**	Argue that modern technology goes far beyond what was imagined in the early Pen cases, so distinguish *Smith v. Maryland,* 442 U.S. 735 (1979) (no expectation of privacy in numbers dialed out); *see In Re Applications*, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (distinguishing *Smith*).
• 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 *after* the call connects (e.g., your bank account number, or passwords) – this is clearly "content"	Pen statute - 18 USC § **3121-3127**	See *In Re Applications*, 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) Note: violations of pen register law do not fall under exclusionary rule. *United States v. Forrester*, 512 F.3d 500, 512 (9th Cir. 2008). Need to articulate as constitutional violation, not statutory violation.

EVIDENCE SOUGHT	AUTHORITY	ISSUES
Pole Camera/Videos Drones? • did the camera intrude on a protected space, e.g. a home? (Church?) • did the surveillance last so long that it created a picture of the person's life? • does it feel "creepy and un-American?"		Some bad law, but revisit this post-*Jones* and *Maynard*. *United States v. McIver*, 186 F.3d 1119 (9th Cir. 1999)(warrant not required if defendant did not have reasonable expectation of privacy in public area); *United States v. Vankesteren,* 553 F.3d 286 (4th Cir. 2009) (camera installed to record defendant's open field does not implicate 4th) *United States v. Jackson*, 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). But: *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987) (video surveillance of home constituted search, warrant required).

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 (5th 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 (6th Cir. 2010) (obtaining email content without a warrant in some circumstances violates the 4th 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 (9th 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 (9th 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) – 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/Deafult.aspx (comprehensive state-by-state chart of surveillance statutes).