



Electronic Surveillance Issues

Scott Davis
scott_davis@fd.org



Roadmap

- Post-*Jones* landscape
- Cell phone data
- New methods of surveillance

United States v. Jones, 132 S.Ct. 945 (2012)

- Held: The installation of a GPS tracking device on a suspect's vehicle, as well as the monitoring of the movements of that vehicle, constitute a search under the Fourth Amendment.
- Emphasis on physical occupation of private property.

United States v. Jones, 132 S.Ct. 945 (2012)



- Warrant authorized installation of GPS device of vehicle registered to Jones' wife within 10 days in the District of Columbia.
- Installed on the 11th day in Maryland.

United States v. Jones, 132 S.Ct. 945 (2012)

- Data collected over a four week period.
- Used at trial to connect Jones to a location that contained 97 kilograms of cocaine and \$850,000 in cash.
- Convicted, sentenced to life in prison.

United States v. Jones, 132 S.Ct. 945 (2012)

- *United States v. Maynard*, 615 F.3d 544 (D.C. Cir 2010)
 - Warrantless use of GPS device was violation of Fourth Amendment.
- Supreme Court granted cert:
 - Whether the warrantless use of a tracking device on Jones' vehicle to monitor its movements on public streets violated the Fourth Amendment.
 - Whether the government violated Jones' Fourth Amendment rights by installing the GPS tracking device on his vehicle without a valid warrant and without his consent.

United States v. Jones, 132 S.Ct. 945 (2012)

- Majority opinion (Scalia)
 - Based on the fact that the government had “physically occupied private property for the purpose of obtaining information” without a warrant.
 - Trespass test – “when the government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.”
 - *United States v. Knotts*, 460 U.S. 276 (1983)
 - *United States v. Karo*, 468 U.S. 705 (1984)

United States v. Jones, 132 S.Ct. 945 (2012)

- Concurring opinion (Sotomayor)
 - Trespass test will not provide necessary guidance in future cases involving new types of surveillance.
- Concurring opinion (Alito)
 - Irony of deciding a 21st-century surveillance case by applying 18th-century tort law.

United States v. Jones, 132 S.Ct. 945 (2012)

- Application of *Katz* test.
- Two part test:
 - A person has exhibited an actual (subjective) expectation of privacy, and
 - The expectation is one that society is prepared to recognize as “reasonable.”
- *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)

United States v. Jones, 132 S.Ct. 945 (2012)

- Majority (Scalia)
 - “[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.”
 - *Katz* test “added to, not substituted for, the common-law trespassory test.”
- Concurrence (Alito)
 - *Katz* “finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation.”

United States v. Jones, 132 S.Ct. 945 (2012)

- A search occurs when officers have “physically occupied private property for the purpose of obtaining information.”
- When and how to apply *Katz* to situations involving modern surveillance techniques?
- *Jones* does not require a search warrant to attach a GPS device.

United States v. Jones, 132 S.Ct. 945 (2012)

- What about standing?
- *United States v. Hernandez*, 647 F.3d 216 (5th Cir. 2011)
 - GPS device placed without a warrant.
 - Defendant argued that placement and use violated Fourth Amendment.
 - Brother's car – no standing to challenge trespass.
 - Focus on "reasonable expectation of privacy."
 - More akin to a "beeper" – use upheld.
 - As to placement, *Jones* not applicable since there was no trespass element.

Good Faith Reliance

- *Davis v. United States*, 131 S.Ct. 2419 (2011)
 - Exclusionary rule intended to serve as deterrent.
 - No deterrent in excluding evidence obtained in “searches conducted in objectively reasonable reliance on binding appellate precedent.”
 - Defeating a claim of good faith requires showing that officers acted with “deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights.”

Cell Phone Tracking



Cell Phone Data and Records

- Cell phones work by sending and receiving signals to and from cell-sites, or towers, which are operated by service providers.
- Providers keep and store records of which cell towers phones have communicated with.
- This information strongly suggests the whereabouts of their customers from almost all points of the day, every day of the year.
- Cell site location information (CSLI)

Cell Phones as Tracking Devices

- *In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government*, 620 F.3d 304 (3d Cir. 2010)
- Allowed law enforcement to acquire “cell site location information” (CSLI) without a warrant or probable cause.
- Reasonable suspicion only.

Cell Phones as Tracking Devices

18 U.S.C. § 2703(d)

A court order for disclosure. . . may be issued by any court. . . 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 the wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Cell Phones as Tracking Devices

- *In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government*, 620 F.3d 304 (3d Cir. 2010)
- “CSLI may resemble a tracking device which provides information as to the actual whereabouts of the subject.”
- Distinguishes *Knotts* and *Karo*

Cell Phones as Tracking Devices

- *In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government*, 620 F.3d 304 (3d Cir. 2010)
- “[Their] opinions make clear that the privacy interest at issue are confined to the interior of the home.”
- “There is not evidence in this record that historical CSLI, even when focused on cell phones that are equipped with GPS, extends to that realm.”

The Stored Communications Act

- Classic methods
 - Pen register
 - Trap or trace device
- 18 U.S.C. § 3122
 - Application need only certify that the “information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.”
 - Relevance, not specific and articulable facts and not probable cause.

The Stored Communications Act

18 U.S.C. § 2703

(c) Records concerning electronic communication service or remote computing service –

(1) A governmental entity may require a provider of electronic communication service or remote computing 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 –

The Stored Communications Act

- Obtains a warrant
- **Obtains a court order under subsection (d)**
- Has the consent of the subscriber or customer
- Submits a written request with detailed information concerning suspected telemarketing fraud.

The Stored Communications Act

18 U.S.C. § 2703(d)

Requirements for court order. – 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.** In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

The Stored Communications Act

- Does not require probable cause in order to obtain historical cell-site data.
- How does this square with the Fourth Amendment?
- Constitutionality upheld by a majority of courts that have considered the issue.

The Stored Communications Act

- *In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F.Supp.2d 113 (E.D.N.Y. 2011)
- “That at all times, our physical movements are being monitored and recorded, and once the Government can make a showing of less-than-probable-cause, it may obtain these records of our movements, study the map of our lives, and learn the many things we reveal about ourselves through our physical presence.”

The Stored Communications Act

- *In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F.Supp.2d 113 (E.D.N.Y. 2011)
- The obtaining of historical cell-site records did constitute a search and “it is presumed that the Government must, at a minimum, obtain a warrant on a showing of probable cause.”

The Stored Communications Act

- *In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F.Supp.2d 113 (E.D.N.Y. 2011)
- Cell site data records enable the government to easily track the vast majority of citizens.
- This fact raises greater Fourth Amendment concerns than a surveilled car trip, as it allows for “mass” or “wholesale” electronic surveillance.

The Stored Communications Act

- *In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F.Supp.2d 113 (E.D.N.Y. 2011)
- “This further supports the court’s conclusion that cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location data records and that the Government’s obtaining these record constitutes a Fourth Amendment search.”

The Stored Communications Act

- *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013)
- “Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional.”
- “[S]pecific orders within that category certainly may be unconstitutional because of additional facts involved in the case.”

The Stored Communications Act

- *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013)
- Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain historical cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional. We do not address orders **requesting data from all phones that use a tower during a particular interval, orders requesting cell site information for the recipient of a call from the cell phone specified in the order, or orders requesting location information for the duration of the calls or when the phone is idle** (assuming the data are available for these periods). Nor do we address situations where **the Government surreptitiously installs spyware on a target's phone or otherwise hijacks the phone's GPS**, with or without the service provider's help.

The Stored Communications Act

- 18 U.S.C. § 2703(d)
- 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.

The Stored Communications Act

- *In re Application of United States of America for Order Directing Provider of Electronic Communication Service to Disclose Records to Government*, 620 F.3d 304 (3d Cir. 2010)
- Discretionary, magistrate can still require a showing of probable cause.

The Stored Communications Act

- *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013)
- “Reading the provision as a whole, we conclude that the ‘may be issued’ language is permissive—it grants a court the authority to issue the order—and the ‘shall issue’ term directs the court to issue the order if all the necessary conditions in the statute are met.”

What About Real-Time Monitoring?



- SCA part of a larger statute, the Electronic Communications Privacy Act.
- “Tracking” treated separately.

18 U.S.C. § 3117

(a) In General-

If a court is empowered to issue a **warrant** or other order for the installation of a **mobile tracking device**, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

(b) Definition-

As used in this section, the term “**tracking device**” means **an electronic or mechanical device which permits the tracking of the movement of a person or object.**

18 U.S.C. § 3117

- Definition incorporated into amendments to Rule 41.
- Makes sense that all “tracking” authority be sought under 3117/Rule 41, right?

18 U.S.C. § 3117

- *In re Order Authorizing Prospective and Continuous Release of Cell Site Location Records*, 31 F.Supp.3d 889 (S.D. Tex. 2014)
- Under what statutory authority is law enforcement permitted to continuously monitor a cell phone's location in (or near) real time?
- 3117/Rule 41 is proper avenue

prospective cell site data or continuous monitoring.

Even so, given law enforcement persistence in pursuing this authority, it seems appropriate to revisit our 2005 statutory holding in light of the Fifth Circuit's recent constitutional ruling. The main questions are (1) whether the SCA authorizes ongoing surveillance of cell phone use; (2) whether cell phone tracking is distinguishable from other forms of tracking covered by the Tracking Device Statute and Rule 41; and (3) whether the hybrid theory – a combination of the SCA with other statutes – offers a plausible alternative legal regime for cell phone tracking. The answer to each question is

constitutional ruling. The main questions are (1) whether the SCA authorizes ongoing surveillance of cell phone use; (2) whether cell phone tracking is distinguishable from other forms of tracking covered by the Tracking Device Statute and Rule 41; and (3) whether the hybrid theory – a combination of the SCA with other statutes – offers a plausible alternative legal regime for cell phone tracking. The answer to each question is no, for reasons explained below.

These considerations compel me to respectfully disagree with my colleague from New York, and to reject the SCA as stand-alone authority for prospective, continuous, and contemporaneous cell site monitoring. Both in fact and in law, this type of surveillance converts a smartphone into a tracking device, and it is governed by the standards of Rule 41, not the SCA.

These considerations compel me to respectfully disagree with my colleague from New York, and to reject the SCA as stand-alone authority for prospective, continuous, and contemporaneous cell site monitoring. Both in fact and in law, this type of surveillance converts a smartphone into a tracking device, and it is governed by the standards of Rule 41, not the SCA.

3. Hybrid Theory

⁵⁰See FED. R. CRIM. P. 41(a)(2)(E) (“‘Tracking device’ has the meaning set out in 18 U.S.C. § 3117(b).”).

⁵¹In this district the government’s practice is to invoke at least three different legal mechanisms to track a target: a SCA 2703(d) order for tracking a cell phone by single tower cell data; a “precise location” warrant based on probable cause for tracking a cell phone’s precise location by GPS or triangulation and a Rule 41 tracking warrant for GPS tracking by device other than a cell phone.

18 U.S.C. § 3117

- *In re Application of the U.S. for an Order for Authorization to Obtain Location Data Concerning an AT&T Cellular*, 2015 WL 1842761 (N.D. Miss. March 30, 2015)
- 2703 is acceptable.

nearby cell tower in order to wirelessly connect his call” and that the “use of their phones, moreover, is entirely voluntary.” *Id.* at 613. Moreover, in quite broad language, the logic of which seems to apply in the prospective cell phone data context, the Fifth Circuit wrote that:

We understand that cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, *Greenwood*, 486 U.S. at 40–41, 108 S.Ct. 1625, or the view of their property from 400 feet above the ground, *Florida v. Riley*, 488 U.S. 445, 451, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989), to remain so. But the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections. The Fourth Amendment, safeguarded by the courts, protects only *reasonable* expectations of privacy.

Id. at 615. Thus, there is clearly binding Fifth Circuit precedent finding that there is no reasonable expectation of privacy in historical cell phone data, and this court doubts that prospective cell phone data is sufficiently different from historical cell phone data to warrant a different result.

It seems to this court that, both as a practical matter and as a constitutional matter, there is no great distinction between historical and prospective cell phone location data. As a practical matter, a number of federal courts have found persuasive the “instantaneous storage theory.”

It seems to this court that, both as a practical matter and as a constitutional matter, there is no great distinction between historical and prospective cell phone location data. As a practical

government.”); *In re Application*, 632 F. Supp. 2d 202, 207 n. 8 (E.D. N.Y. 2008) (Garaufis) (“The prospective cell-site information sought by the Government ... becomes a ‘historical mobile phone records’).

record" as soon as it is recorded by the provider."); *In re Application*, 460 F. Supp. 2d 448, 459 (S.D. N.Y. 2006) (Kaplan) ("[T]he information the government requests is, in fact, a stored, historical record because it will be received by the cell phone service provider and stored, if only momentarily, before being forwarded to law enforcement officials."); *In re Application*, 405 F. Supp. 2d 435, 444 (S.D. N.Y. 2005) (Gorenstein) (nothing in the SCA limits when "information may come into being").

As a constitutional matter, it is not clear to this court that a defendant has a significantly different expectation of privacy with regard to historical cell phone location data than he does with regard to prospective cell phone data. This is particularly true when the monitoring of

government wanted to ascertain the location of a suspect's home, its best bet would be to obtain his historical cell phone data and simply ascertain the location to which he returns each night.

It seems clear enough that prospective cell phone data is most useful to the government in cases where a suspect is actively moving from location to location, such as in *Skinner*'s scenario involving a drug trafficker traveling to a drug buy. In such a scenario, it must be asked whether

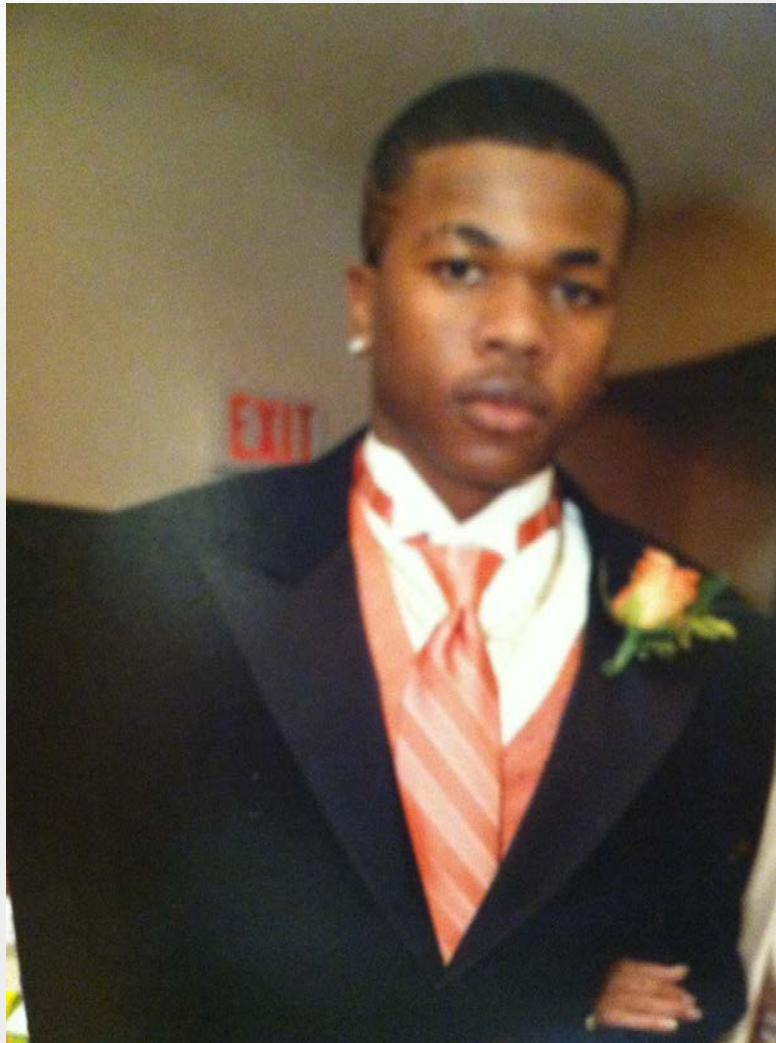
As a constitutional matter, it is not clear to this court that a defendant has a significantly different expectation of privacy with regard to historical cell phone location data than he does with regard to prospective cell phone data. This is particularly true when the monitoring of

Cell Phone Searches Incident to Arrest



- *Riley v. California*, 134 S.Ct. 2473 (2014)
- Held: The warrantless search and seizure of digital contents of a cell phone during an arrest is unconstitutional.

Riley v. California, 134 S.Ct. 2473 (2014)



Cell Phone Searches Incident to Arrest

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans “the privacies of life.” The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

Riley, at 2494-95.

Other Methods of Surveillance



Cell Phone Data Extractors



- Allows access to GPS info, contacts, photos, videos, browser information, etc.
- Impact of *Riley*

StingRays



- International Mobile Subscriber Identity (IMSI) locator
- Used to located cell phones regardless of whether the phone is being used to make calls.

SEPTEMBER 19

**Report Says Series of Problems Allowed
Man to Reach White House**

11:13 PM

5
KPIX

StingRays

How a 'Stingray' Cellphone Tracking Device Works



Law-enforcement officials are quietly using gadgets referred to generically as 'stingrays' to locate cellphones as part of investigative work.

1. Often the device is used in a vehicle along with a computer with mapping software.



2. The stingray system, which mimics a cellphone tower, gets the target phone to connect to it.

3. Once the cellphone is detected by the stingray, the phone's signal strength is measured.



4. The vehicle can then move to another location and again measure the phone's signal strength.



5. By collecting signal strength in several locations, the system can triangulate and map a phone's location.

Source: WSJ research and government documents

StingRays

- What type of authorization is needed?
 - None?
 - Pen register/trap and trace order?
 - 2703 order?
 - Warrant?
- DOJ official guidance
 - Warrant – Rule 41
 - “This policy guidance is intended only to improve the internal management of the Department of Justice. It is not intended to and does not create any right, benefit, trust, or responsibility, whether substantive or procedural, enforceable at law or equity by a party against the United States, its departments, agencies, instrumentalities, entities, officers, employees, or agents, or any person, nor does it create any right of review in an administrative, judicial, or any other proceeding.”

StingRays

- How to know if an IMSI catcher has been used?
 - Terminology
 - ISMI catcher, cell site simulator, Stingray, Kingfish, Amberjack, digital analyzer, mobile tracking device.
 - How the authorities find out your client's cell phone number?
 - How did the authorities locate your client?

StingRays

- Issues to raise:
 - ISMI catchers trigger Fourth Amendment scrutiny.
 - ISMI catchers engage in the electronic equivalent of a “general search,” which violates the Fourth Amendment.
 - Statutory orders are not sufficient.
 - Even if warrant obtained, use of ISMI catcher is still invalid.
 - Specificity of information in warrant application.
 - Particularity, overbreadth.

StingRays

StingRays: The Most Common Surveillance Tool the Government Won't Tell You About – A Guide for Criminal Defense Attorneys

<https://www.fed.org/docs/training-materials/2015/fjc2015/new-surveillance-tools.pdf>

Subpoena Requests

SUBPOENA

IN THE (STATE) _____ COURT OF _____ COUNTY, _____ ACTION-LAW.

Plaintiff/Petitioner: _____

vs

Defendant/Respondent: _____

Number _____

QUALIFIED ORDER

_____ day of _____

NOW, THIS _____ follows.

_____ action with a final decree dated (_____

_____ participant, is/ was _____

Bulk Metadata Collection



Bulk Metadata Collection

- USA Freedom Act (2015)
 - Ended NSA's ability to collect metadata en masse.
 - Can still access information, but court order is needed and specific queries must be made.
- PRISM
 - Theoretically targets foreign communications.
- Loopholes still exist
 - Section 702 of the Foreign Intelligence Surveillance Act
 - Executive Order 12333



*The
End*