ELECTRONIC SURVEILLANCE AND TRACKING POST *JONES*

29TH ANNUAL RUSTY DUNCAN ADVANCED CRIMINAL LAW COURSE
TEXAS CRIMINAL DEFENSE LAWYERS ASSOCIATION

June 13-15, 2013
Hyatt Regency
San Antonio, Texas

Presented by:
Donald H. Flanary, III.
GOLDSTEIN, GOLDSTEIN & HILLEY
29TH FLOOR TOWER LIFE BUILDING
SAN ANTONIO, TEXAS 78205
(210) 226-1463
donflanary@hotmail.com

Table of Contents

I. INTRODUCTION

Imagine yourself driving down a country road. The weather is beautiful. Someone special is by your side. Suddenly, you see red and blue lights behind you. The rental car you are driving has a burned out tail light. You pull over and stop in a rest area. A police officer asks for your license. He is friendly and polite. He asks you to step out of the car and walk to the rear of the vehicle. He asks you to empty out your pockets. You take out your wallet, a few bucks in cash and your cell phone. He tells you that because you are in a rental he is only going to give you a warning. Without you noticing, he slips your cell phone into his pocket. He walks back to his squad car to run your license. While in his car, the officer uses a handheld device to extract all of the information off of your cell phone, including contacts, photos and videos, and most importantly, GPS data, even though your aren't even a suspect to a crime. This scenario sounds like a sci-fi movie script or some paranoid Orwellian prophecy of a future police-state. But, it is not. This scenario is already taking place right here in the U.S.

Cnet.com has reported that Michigan State Police have been using these "extraction devices" already.[1] These handheld devices can work with different phones and even bypass security passwords.[2] In 2011, the Michigan State Police has "admitted to owning five of the devices."[3]

This article will examine the current state of electronic surveillance and tracking in the aftermath of the recent Supreme Court decision in *United States v. Jones*, 132 S. Ct. 645, (2012). Part II will focus on post-*Jones* cases. Part III will examine how cell phone data is kept and how records are maintained and how the government accesses this information. Part IV will examine case law for cell phone searches incident to arrest. Part V will examine how cell phones work and how the information is collected. Part VI will take a look at the new technologies that the government is using for surveillance today.

II. THE ELECTRONIC FRONTIER POST-*JONES*

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

In *U.S. v. Jones*, the Supreme Court held that the installation of a GPS tracking device on a suspect's vehicle, as well as the monitoring of the movements of that vehicle did constitute a search under the Fourth Amendment. *United States v. Jones*, 132 S. Ct. 945, 949 (2012). The Court held accordingly due to the government's physical occupation of private property for the purpose of gathering information. *Id*.

Antoine Jones, a nightclub owner in Washington D.C., had become the focus of an investigation by the FBI and Metropolitan Police Department. *Id*. at 947. Based on information gathered from a variety of sources, including visual surveillance of the nightclub and a wiretap of Jones' cell phone, the government obtained a warrant for the use of an electronic tracking device to be installed on the undercarriage of the vehicle registered to Jones' wife. *Id*. The warrant authorized the installation of the device in the District of Columbia within 10 days. *Id*. The GPS tracking device was installed on the 11th day in Maryland. *Id*.

By use of the device, the government obtained over 2,000 pages of data over a 4-week period. *Id*. at 948–49. In 2007, after a hung jury the year before, the government used, once again, the data obtained from the use of the GPS device to connect Jones to the location that contained 97 kilograms of cocaine and $850,000 in cash. *Id*. at 949. Jones was sentenced to life in prison. *Id*. The U.S. Court of Appeals for the District of Columbia Circuit reversed the conviction of Jones, explaining that the warrantless use of the GPS device was a violation of the Fourth Amendment. *United States v. Maynard*, 615 F.3d 544, 568 (D.C. Cir. 2010).

The Supreme Court unanimously affirmed the decision of the appeals court. *Jones*, 132 S. Ct. at 945. The reasoning employed by the Justices, however, differed. Justice Scalia based the majority opinion on the fact that the government had "physically occupied private property for the purpose of obtaining information" without a warrant. Id. The text of the Fourth Amendment, Justice Scalia explained, demonstrates the close connection to property. *Id*. The Court explained the "common-law trespassory test" for what could be described as a Fourth Amendment violation *per se*. *Id*. at 952. Looking to language previously used by the Court, Justice Scalia explained, "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." *Id*. at 951 (citing *United States v. Knotts*, 460 U.S. 276, 286 (1983)). Essentially, if the government takes up space on private property without a warrant, there is a strong presumption that a violation of the Fourth Amendment has occurred. The Court went on to distinguish the facts in *Jones* from the previous cases, *United States v. Knotts*, 460 U.S. 276 (1983) and *United States v. Karo*, 468 U.S. 705 (1984) where the Court upheld government actions in which tracking devices were placed in a defendant's care by noting that in both *Knotts* and *Karo*, the "beeper" used by the government was installed in the container to be tracked before the container came into the possession of the defendant. *Id*. at 952 ("As in *Knotts*, at the time the beeper was installed the container belonged to a third party and it did not come into possession of the defendant until later." (citing *United States v. Karo*, 468 U.S. 705, 708 (1984))).

Justice Sotomayor noted in her concurrence that in situations involving new forms of electronic surveillance the majority opinion's trespassory test would not provide the necessary guidance. *Id*. at 955 (Sotomayor, J., concurring). With Justice Scalia-like wit, Justice Alito began his concurrence by noting the irony of the majority of the Court deciding a case involving 21st-century surveillance techniques by applying 18th-century tort law and pointing out that in *Jones*, the government might have provided grounds for a 1791 suit for trespass to chattels. *Id*. at 957 (Alito, J., concurring).

The main point of difference in the Court was the analysis of when and how to apply the two part test developed in *Katz v. United States*, 389 U.S. 347 (1967). This test was explained by Justice Harlan in his concurrence and has become the strong point of the *Katz* opinion. The test inquires if a private citizen can meet two requirements in order to establish that a violation has occurred, "first that a person have exhibited an actual (subjective) expectation of privacy and, second that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The majority opinion in *Jones* did point out, "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Jones*, 132 S. Ct. at 953. Justice Scalia opined that the *Katz* test "*added to*, not *substituted for*, the common-law trespassory test." *Id*. at 952 Justice Alito, on the other hand, stated that *Katz* "finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation." *Id*. at 959 (Alito, J., concurring).

The opinion of the Court did establish that in situations in which officers have "physically occupied private property of the purpose of obtaining information," a "search" within the meaning of the Fourth Amendment has occurred. *Id*. at 949. The Court, however, did not provide further guidance as to when and how to apply the *Katz* test to situations involving 21st-century surveillance techniques or as Justice Alito would have framed the issue before the

Court, "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id*. at 958 (Alito, J., concurring).

The holding in *Jones* did not, as the media reported, require a search warrant to attach a GPS device, that question was not answered. Both the concurring opinions by Justices Sotomayor and Alito raise several more questions that the majority's reliance on trespass theory seems inadequate to answer. A decision on factory or owner installed vehicle track devices or GPS enabled smartphones are absent from the opinion of the Supreme Court. *Id* at 956 (Sotomayor, J,. concurring). In a companion case Chief Judge Kozinski of the Ninth Circuit dissenting from the denial of rehearing en banc proclaims "1984 may have come a bit later than predicted, but it's here at last." *United States v. Pineda-Moreno*, 617 F.3d 1120 (9th Cir. 2010).

In an almost fatalistic dissent Chief Judge Kozinski lays out the argument that seemed to have great sway over Justice Sotomayor. The facts of *Pineda-Moreno* are very similar to *Jones* and yet the Ninth Circuit came to the conclusion that that entering onto Pineda-Moreno's property and attaching a tracking device to his car required no warrant, probable cause, founded suspicion or by-your-leave from the homeowner, the panel holds that downloading the data from the GPS device, which gave police the precise locus of all of Pineda-Moreno's movements, also was not a search, and so police can do it to anybody, anytime they feel like it." *Pineda-Moreno*, 617 F.3d at 112. Kozinski continues that:

> "if you have a cell phone in your pocket, then the government can watch you. 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. The volume 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* at 1125 (internal quotations omitted).

The Government has this power but it still must establish and the 5th circuit and the Western District of Texas have their individual case law regarding it.

B. Standing related to *Jones*

Standing rules still apply for both placement of GPS and its use in the 5th Circuit. In *United States v. Hernandez*, 647 F. 3d 216 (5th Cir. 2011) the defendant filed a motion to suppress the use of GPS information obtained when he drove his brother's car to California to retrieve 20 pounds of methamphetamine. The GPS was placed without a warrant, however was not a 24 hour device but was more akin to a beeper because it emitted a "ping" at intervals of 15 minutes to two hours. *See United States v. Knotts*, 460 U.S. 267 (1983). Hernandez argued that both placement and use of the GPS device "independently violated his Fourth Amendment rights." *Hernandez*, 647 F.3d at 219. The Fifth Circuit focused on the "reasonable expectation of privacy" as set forth in *Rakas v. Illiniois*, 439 U.S. 128, 143 (1978) and holds that "Hernandez lacks standing to challenge the placement of the GPS device on his brother's truck." *Hernandez*, 647 F.3d, at 219. However, the Court found that since Hernandez had permission to drive his brothers truck he did have a reasonable expectation of privacy and thus the use by the government of the data that tracked Hernandez to California could be challenged. The Court then immediately shuts the door by declaring that the use of the GPS device was not an unconstitutional warrantless search under the Fourth Amendment. *See Id* at 220. Conceding that "Hernandez may be correct that some GPS systems offer significantly enhanced monitoring

options" the court holds that this "GPS" was more of a *Knotts* beeper and used simply to enhance not track. *Id* at 221. *Jones* therefore has no effect on this decision which had no trespass element.

Also consider *United States v. Hanna*, 2012 WL 279435 (January 30, 2012) from the Southern District of Florida. The officers attached a GPS to the vehicle then activated it later only to obtain the location of the vehicle at that moment so they could get visual contact with the suspects, and it was established that both at the time of installation and activation of the device no person occupied the vehicle. *Hanna*, 2012 WL 279435 at 1-2. This District Court concludes, similar to *Hernandez* that the defendant's did not have standing to challenge the trespass upon the property of the co-defendant's vehicle because they had no property right to that vehicle. *Id* at 3. The Court then addressed the activation of the GPS:

> "In *Jones,* five members of the Court concluded that Justice Scalia's trespass theory did not form a sufficiently comprehensive analysis of the Fourth Amendment implications of GPS monitoring and argued that GPS monitoring should also (in the case of Justice Sotomayor) or only (in the case of Justice Alito) be analyzed to determine whether it has invaded a reasonable expectation of privacy." *United States v. Hanna*, 11-20678-CR, 2012 WL 279435 (S.D. Fla. Jan. 30, 2012).

The District Court then concluded that the defendant's did not have a reasonable expectation of privacy in the vehicle at the time of the activation, and by the time they did occupy the vehicle an actual officer has shown up and had the vehicle under traditional visual surveillance. *Id* at 4. Thus a limited use of the GPS although it accomplishes something that no officer could conceivably do in person does not fall under the Fourth Amendment in the Southern District of Florida if no one occupies the vehicle at the time of the GPS activation.

Jones could and has lead us in all sorts of directions as the ink on it dries. *See Montana State Fund v. Randall Simms* No. DA 11-0342 (Montana Supreme Court, 2012) (Nelson, J,. concurring) (Relying on *Jones* to suggest that public camera surveillance by a state agency can violate the Fourth Amendment and require a warrant).

C. "Good Faith Reliance" and *Davis v. United States*, 131 S. Ct. 2419 (2011).

After the ruling in *Jones*, courts now have at least a clear version of how the physical occupation of private property is a violation of the Fourth Amendment. The full force of *Jones*, however, has yet to be seen. In several cases, federal courts have upheld the validity of actions taken by officers, which now, after the ruling in Jones, would be considered a violation of the Fourth Amendment and subject to the exclusionary rule. This is due to the "good faith reliance" on binding appellate precedent exercised by the officers. Justice Alito described the exception in *Davis v. United States*, 131 S. Ct. 2419 (2011). In *Davis*, the Court explained that the exclusionary rule was created to serve as a deterrent sanction by barring the prosecution from introducing evidence that was gathered by a Fourth Amendment violation. *Davis v. United States*, 131 S. Ct. 2419, 2423 (2011). The Court deduced that there would be no deterrent effect in excluding evidence obtained in "searches conducted in objectively reasonable reliance on binding appellate precedent." *Id*. at 2423–24. Therefore, that evidence would not be subject to the exclusionary rule. *Id*. This has led to the limbo period now faced by defense attorneys in which courts are upholding the introduction of evidence gathered in an unconstitutional manner. *See United States v. Sparks*, Nos. 11–1134, 11–1143, 2013 WL 1197741 (1st Cir. 2013) ("The good-faith exception is, however, properly applied in cases like this one (or Davis itself), where new developments in the law have upended the settled rules on which the police relied."); *see also United States v. Nwobi*, No. CR10–952(C) GHK–7, 2012 WL 769746 (C.D. Cal. 2012) ("Because the officers acted in objectively reasonable, good faith reliance on *McIver* when using

GPS tracking devices during their investigation of Defendant, the exclusionary rule has no application here based on the Supreme Court's decision in *Davis*."). "To defeat a claim of good-faith, defendant's argument must focus on the illegality of the search under the Fourth Amendment. Defendant must argue that the officers 'exhibit[ed] deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights,' when they relied on the Order." *United States v. Muniz*, No. H–12–221, U.S. Dist. 2013 WL 391161, at *3 (S.D. Tex. Jan. 29, 2013) (citing *Davis*, 131 S. Ct. at 2427.).

As recently as January of this year, Federal District Court Judge Lee H. Rosenthal, out of the Southern District of Texas, Houston Division, issued a memorandum and order in response to a motion to suppress evidence obtained pursuant to an order under 18 U.S.C. § 2703(c) and (d) for historical cell-site location information. *Muniz*, 2013 WL 391161 at 1. The government intended to use location information to show that Demi Mischel Muniz made a trip from Texas to California with illegal aliens. *Id*. Once again, the government argued the voluntary disclosure doctrine as well as the good-faith exception. *Id*. In the memorandum and order, the Judge states that it is not necessary to reach the question of what standard law enforcement must meet in order to obtain historical cell-site location information, as "[t]he good-faith exception applies, making it unnecessary to decide whether obtaining CSLI is a Fourth Amendment search." *Id*.

III. CELL PHONE DATA AND RECORDS

A. Cell phones as tracking devices

Cell phones work by sending and receiving signals to and from cell-sites, often called towers, operated by service providers. *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info*., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011). If a cell phone has sent and received signals from a particular tower, it is strongly suggested that the cell phone user was in a particular range of the tower. *Id*. Cell phone service providers keep and store records of which cell towers phones have communicated. *Id*. Therefore, cell phone service providers have the information that can strongly suggest the whereabouts of their customers from almost all points of the day, every day of the year. *See Id*. ("The implication of these facts is that cellular service providers have records of the geographic location of almost every American at almost every time of day and night.").

B. The Stored Communications Act

For years, when the government has wanted to trace someone's phone or obtain numbers they were calling, the government would use a pen register or trap and trace device. A pen register is:

> a device or process which 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, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business. 18 U.S.C. § 3127(3).

A trap or trace device refers to:

> a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and

> signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication. 18 U.S.C. § 3127(4).

These devices allow law enforcement to trace the numbers to which calls are received and sent. It is important to note that these devices to not allow law enforcement to listen in to phone conversations or make a record of the conversations that transpire.

An application for the installation of these devices can be made by an attorney for Federal Government or by State investigative or law enforcement officer.[4] Application only need to certify that the "information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[5] So, this information can be obtained by State or Federal law enforcement not upon a showing of specific and articulable facts and not upon a showing of probable cause, but only upon a showing of relevance.

In obtaining data from cellular service providers, the government relies on the Stored Communications Act, which states in relevant part:

> (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--
>
> (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 this section;
>
> (C) has the consent of the subscriber or customer to such disclosure;
>
> (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
>
> (E) seeks information under paragraph (2).
>
> (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--
>
> (A) name;
>
> (B) address;
>
> (C) local and long distance telephone connection records, or records of session times and durations;
>
> (D) length of service (including start date) and types of service utilized;
>
> (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
>
> (F) means and source of payment for such service (including any credit card or bank account number),

> of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).
>
> (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.
>
> (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.

18 U.S.C. § 2703(b)–(d).

So, section 2703(d) does not require probable cause in order to obtain historical cell-site data. The Stored Communications Act allows the government to obtain a court order for the disclosure of cell-phone site data upon offering, "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."[6] What does that mean for everyone who owns a cell phone in America? Federal Judge Nicholas G. Garaufis of the Eastern District of New York answered that question saying, "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." *In re* U.S. for an Order, 809 F. Supp. 2d at 115.

In *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), Judge Garaufis' court was faced with the issue of whether the "lower-than-probable-cause standard" is consistent with the Fourth Amendment. *Id*. The court held that the obtaining of records in the case before it did constitute a search and "it is presumed that the Government must, at a minimum, obtain a warrant on a showing of probable cause." *Id*. at 116. The ruling was based, in part, on the fact that these cell site data records enable the government to easily track the vast majority of Americans. *Id*. at 119. This fact raises greater Fourth Amendment concerns than a surveilled car trip, as it allows for "mass" or "wholesale" electronic surveillance. *Id*. at 115. "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. *Id*. at 119–20.

The government also argued, the Third-Party-Disclosure Doctrine, attempting to demonstrate that cell phone users abandon their expectation of privacy by voluntarily communicating location information to the service provider simply by choosing to carry and use their cell phone. *Id*. at 120 The Supreme Court "has consistently held that a person has no

legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979). The Federal Court in New York reasoned that while, technically, cell phone users do not convey their location to cell towers, they do voluntarily expose cell phone signal to the cell towers, information that is collected by the service provider in the ordinary course of business. *In re U.S. for an Order*, 809 F. Supp. 2d at 122. Under the third-party-disclosure doctrine, the court held that this disclosure does eliminate a reasonable expectation of privacy. *Id*. However, the court applied an exception to the doctrine for *cumulative* cell-site-location records. *Id*. at 120. In the case before the court, the government used an order to obtain records for a period of 113 days. *Id*. at 114. Just as Justice Alito noted in *Jones*, "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." *Jones*, 132 S. Ct. at 957 (Alito, J., concurring. Much is the same in reference to movements of a cell phone, logged by the service provider.

The opinion went on to recognize the greater issue before the court, although it still remains unresolved. In *Katz*, the Supreme Court noted that a narrow reading of the Constitution ignored the role public telephones played in private communication. See *In re U.S. for an Order*, 809 F. Supp. 2d at 126 ("In changing Fourth Amendment doctrine in order to accommodate changes in technology, the Court noted that '[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.'" (quoting *Katz v. United States*, 389 U.S. 347, 352 (1967))). Today, the public phone has gone the route of the dodo bird and been replace by cell phones. *Id*. at 114. However, Fourth Amendment doctrine has not evolved to recognize the role cell phones fulfill in private communication and the Supreme Court certainly has yet to address the Fourth Amendment challenges created by this relatively new form of technology. *Id*. at 126–27. The court concluded by warning that Big Brother's surveillance of citizen's movements via new technologies, like the warrantless collection of data from cell-site-locations, places our nation far closer to the Oceania of George Orwell's 1984 than our Constitution allows. *See id*. at 127 ("…such as the collection of cell-site-location records, without the protections of the Fourth Amendment, puts our country far closer to Oceania than our Constitution permits.").

In a case from October of 2005, the U.S. District Court in Houston addressed the issue of warrantless cell site data collection. *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005). The court recognized it was a case of first impression and contained "serious implications for the balance between law enforcement and privacy." *Id*. at 748–49. The government sought cell site data in order to locate suspects in an ongoing investigation. *Id.* The court articulated the question before it as whether the location information sought could be obtained by a showing of "specific and articulable facts," as the government argued or if the information required the stronger standard of probable cause. *Id*. at 749–50 ("More particularly, is this location information merely another form of subscriber record accessible upon a showing of "specific and articulable facts" under 18 U.S.C. § 2703(d), as the government contends? Or does this type of surveillance require a more exacting standard, such as probable cause under Federal Rule of Criminal Procedure 41?").

In a very logical opinion, United States Magistrate Judge, Stephen Wm. Smith looked to the definition of tracking device in 18 U.S.C. § 3117(b), which states "[a]s 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." *See Id*. at 753 ("The ECPA's definition of tracking device is concise and straight-forward…"); *see also* 18 U.S.C.A. § 3117(b) (West 1986). The

court noted, while "the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data." *In re Application for Pen Register*, 396 F. Supp. 2d at 754. The court held that even the possibility of the invasion of Fourth Amendment rights is sufficient to require a search warrant under rule 41 of the Federal Rules of Criminal Procedure, which require the issuance of a search warrant if the probable cause standard has been met. *Id*.; *see also* FED. R. CRIM. P. 41(d)(1) ("After receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.").

However, as recently as the summer of 2012, the Sixth Circuit upheld the use of historical cell-site location data in a criminal case. In *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), the court applied the Katz test and determined that "[b]ecause authorities tracked a known number that was voluntarily used while traveling on public thoroughfares, Skinner did not have a reasonable expectation fo privacy in the GPS data and location of his cell phone." *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012).

IV. SEARCHES OF CELL PHONES INCIDENT TO ARREST

"The Fourth Amendment to the United States Constitution as well as article I, § 9 of the Texas Constitution protect against unreasonable searches and seizures conducted by the government. Furthermore, a search conducted without a warrant is presumptively unreasonable, *United States v. Karo,* 468 U.S. 705, 717, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984) and, when it is initially shown that a warrantless search occurred, the State has the burden of legitimizing it in some manner. *Roth v. State,* 917 S.W.2d 292, 299 (Tex.App.-Austin 1995, no pet.)." *State v. Granville*, 373 S.W.3d 218, 221 (Tex. App.—Amarillo 2012, pet. granted).

So the question remains…"may an officer conduct a warrantless search of the contents or stored data in a cell phone when its owner was required to relinquish possession of the phone as part of the booking or jailing process?" *State v. Granville*, 373 S.W.3d 218, 222 (Tex. App.—Amarillo 2012, pet. granted).

Currently, the most notable case supporting the search incident to arrest of a cell phone is the Fifth's Circuit decision in *United States v. Finley*. In *Finley*, police conducted a warrantless search of Jacob Finley's cell phone incident to arrest for selling drugs. *United States v. Finley*, 477 F.3d 250 (5th Cir.2007). As a result of their warrantless search, the police were able to acquire incriminating text messages related to drug trafficking which help lead to Finley's conviction. *Id*. at 255.

Finley appealed on the grounds that his Fourth Amendment rights were violated when the police conducted the warrantless search of his cell phone. To justify their conclusion, the Fifth Circuit refused to acknowledge the difference between modern technologies and containers used to hold physical objects. Relying on *United States v. Chan*, 830 F.Supp 531 (N.D.Cal. 1993) the Fifth Circuit explained that "police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial." *Finley* at 259-60.

In *Chan*, the Federal Court upheld a warrantless search of Chan's pager by analogizing a pager to an "electronic" container. The Court did not find it relevant that Chan could not possibly have used the pager as a weapon nor that Chan could have destroyed any evidence that could be collected from the pager. In *Finley*, the Fifth Circuit continued to refuse recognition of any

conceptual difference searching electrical devices for digital data and information from searching physical containers for contraband.

A. Cell Phones Contain "Private" Information

There are several Courts that refuse to accept *Finley*. *Granville* 373 S.W.3d at 226. These Courts base their rejection of *Finley* on the analysis of "the purpose of a cell phone, the quantity of data stored in them, and the private nature of those contents. For example, the court in *Schlossberg v. Solesbee,* 844 F. Supp. 2d 1165 (D. Or. 2012), noted that cell phones and cameras 'are capable of holding large volumes of private information' and that 'legitimate concerns exist regarding the effect of allowing warrantless searches of such devices.' Often they 'include some combination of email services and internet browsing' and the information stored within them may include 'phonebook information, appointment calendars, text messages, call logs, photographs, audio and video recordings, web browsing history, electronic documents and user location information.' (quoting *Schlossberg v. Solesbee*, 844 F.Supp.2d at 1169).

B. Cell Phones Are Not "Containers"

Other courts have also rejected the "container" analogy set forth in *Finley*. In *New York v. Belton* the court held that a phone is not a "container" in the literal sense because it is not capable of actually holding an object. *See State v. Smith*, 920 N.E.2d 949 (Ohio 2009). This supported the Ohio State Supreme Court's rejection of the "container" analysis. *Id*. In *Smith*, the Court refused to accept the crucial premise that cell phones are just like any other containers that might hold objects inside them. *Id*. at 954. The Court held that the search incident to arrest doctrine should not apply explaining that even the most basic cell phones are capable of string a wealth of digitalized information wholly unlike and physical object found within a closed container. *Id*. Therefore, the Ohio State Supreme Court demanded police must obtain a warrant before conducting a search of an individual's cell phone. *Id*. at 955.

C. Arrestee's Immediate Control

In *United States v. Park*, the Court used different rationale for rejecting search of cell phones incident to arrest. *United States v. Park*, 2007 WL 1521573 (N.D. Cal. May 23, 2007). In *Park*, police conducted a search of the defendant's cell phone at the station which was located more than 90 minutes away from the location of the arrest. *Id*. While the Court did not expressly reject the idea that cell phones were "containers", the Court did explain that cell phones are possessions within an arrestee's immediate control and therefore protected by the Fourth Amendment per *United States v. Chadwick*. *Id*. The Court also focused on the immense amounts of private information that can be stored on cell phones, explaining that address books, calendars, voice and text messages, email, video, and pictures could reveal highly personal information. *Id*.

D. Texas Court of Criminal Appeals to Rule

The Texas Court of Criminal Appeals will soon decide the issue of whether police can search a cell phone incident to arrest. The most logical and outspoken rejection of *Finley* can be found in *State v. Granville. Granville*, 373 S.W.3d 218. In *Granville*, the Amarillo Court of Appeals reviewed the State's argument for a presence of probable cause to believe a crime was committed and the supposed lack of any reasonable expectation of privacy in the device." *Id*. at 222. The Court explained "we know of no authority that allows the State to search property merely because its officers have probable cause to believe that a crime occurred and evidence of that crime can be found on the property to be searched. Those two indicia simply provide a basis to secure a warrant. *See State v. Jordan,* 342 S.W.3d 565, 568–69 (Tex.Crim.App.2011) (describing the prerequisites to obtaining a warrant). They alone do not allow a search. Without

such a warrant, the search is presumptively unreasonable. *McGee v. State,* 105 S.W.3d 609, 615 (Tex.Crim.App.2003). So, the State's suggestion that the search of the phone was permissible since probable cause to believe a crime had occurred and that Granville's cell phone contained evidence of it, without more, is wrong." *Id*.

The State argued "that it "was a phone taken pursuant to a lawful arrest and therefor was subject to being searched" and that the "manipulation of the phone is no different that [sic] looking at clothing or searching through papers an inmate has in his possession when ... booked into jail." Added to those comments was one expressing that "society has never accepted or suggested an individual has an expectation of privacy in a jail setting." Starting with the latter, we find it global and inaccurate." *Id*.

The Court explained that "should the State's contention be accepted, it would be free to look for whatever it cared to just because it could. Exposing a detainee to having his private thoughts, relationships, finances, and the like to arbitrary intrusion seems antithetical to the societal and civil norm mandating the presumption of innocence until proven guilty." *Id*. at 225. "In effect, the State fights to enable any, if not every, law enforcement officer the ability to walk into a property room, pick up whatever cell phone, ipad, ipod, or like device he may discover therein, turn it on, and use it as he cares to just because the device was within the property room. The State pursues this end by saying little to nothing about the nature of the electronic instrument involved or the vast quantity of personal information about their owner and others that may be contained in them." *Id*. at 226. In conclusion, the Court explained "consequently, 'warrantless searches of such devices are not reasonable incident to a valid arrest absent a showing that the search was necessary to prevent the destruction of evidence, to ensure officer safety, or that other exigent circumstances exist,' according to the court." *Id*. at 226-27.

V. NUTS AND BOLTS OF CELL PHONES AND HOW EVIDENCE IS COLLECTED

When the first call was placed on a handheld mobile phone in 1973, the prototype device used was capable of less than 30 minutes of battery life and took 10 hours to re-charge.[7] Today, the ownership of mobile devices has reached its critical mass both in the United States and globally.[8] These devices function as our primary means of both daily communication and media interaction. In 2012, the average person sent/received 164.5 phone calls per month, used 644.1 voice minutes per month and sent/received 764.2 text messages per month.[9] As Circuit Judge Posner noted in a 2012 opinion, "a modern cell phone *is* a computer." *United States v. Flores-Lopez*, 670 F.3d 803, 804 (7th Cir. 2012).

A. Basic Cell Phone Location Technology

Basically, cell phones are very sophisticated radios. These phones are devices that can make and receive telephone calls over a radio link while moving around a wide geographic area. They accomplish this by connecting to a cellular network provided by a mobile phone operator, allowing access to the public telephone network.[10]

A cellular network or mobile network is a radio network distributed over geographic areas called cells.[11] Each cell is served by at least one fixed-location transceiver. These transceivers are known as a cell sites or base stations.[12] In a cellular network, each cell uses a different set of frequencies from neighboring cells to reduce interference. When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.[13]

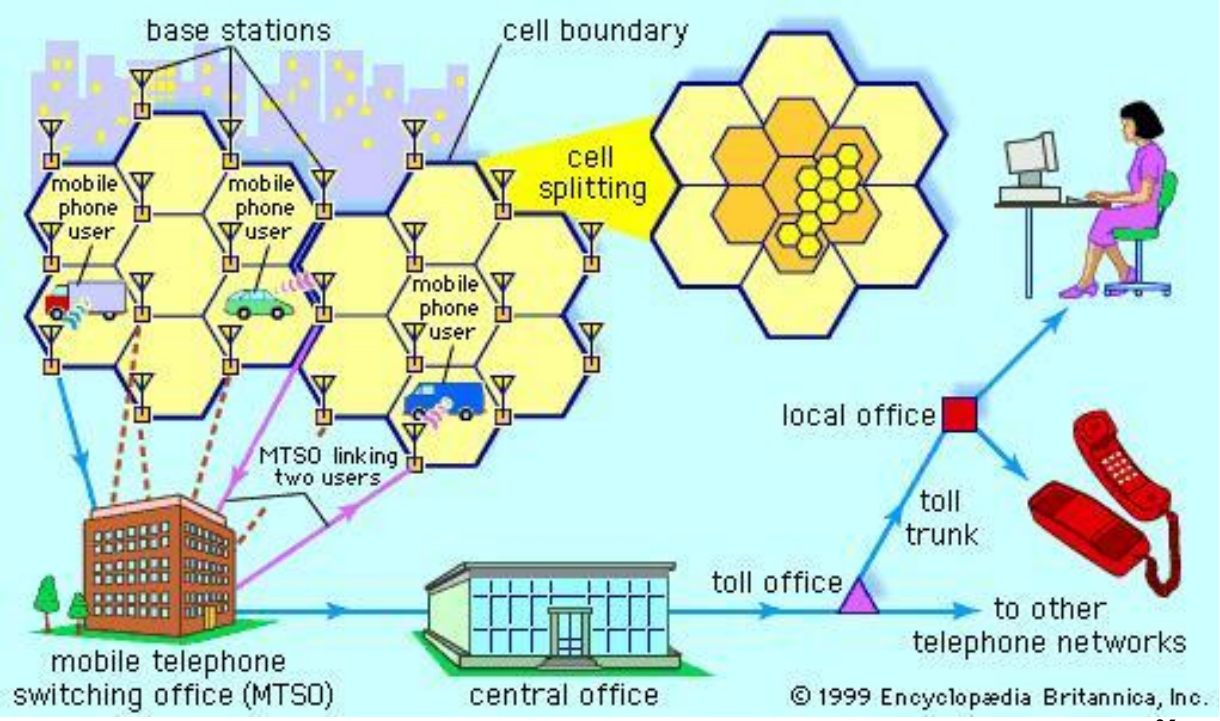
All cell phones have special codes associated with them that are used to identify the phone, the phone's owner and the service provider.[14] When you make a call from your phone it goes through a standard process that allows you to communicate with others.

First, when you turn the phone on, it attempts to locate a System Identification Code (SID)[15]. A SID is a unique 5-digit number that is assigned to each carrier by the Federal Communications Commission (FCC).[16] The phone locates this SID on a control channel. A control channel is a special frequency that your phone and base station use to communicate about things like call set-up and channel changing. If the phone cannot find any control channels to communicate with, it knows it is out of range and displays a "no service" message. When it receives the SID, the phone compares it to the SID programmed into the phone. If the SIDs match, the phone knows that the cell it is communicating with is part of its home system.[17]

In connection with the SID, your phone also transmits a registration request, and the Mobile Telephone Switching Office (MTSO) keeps track of the phone's location in a database.[18] This allows the MTSO to identify which cell you are in when it wants to connect to your phone[19]. A MTSO is used for switching telephone calls among landline subscribers and mobile subscribers, the office controlling the call origination, termination and release of call from both the landline and the mobile subscribers, and providing a separation between the elements associated with each function for regulatory purposes.[20]

When the MTSO receives a call it attempts to locate you.[21] It will search its database to identify which cell zone you are in. The MTSO selects a frequency pair that your phone will use in that cell to take the call. The MTSO communicates with your phone over the control channel to tell it which frequencies to use, and once your phone and the tower switch on those frequencies, the call is connected and you are communicating by two-way radio.[22]

As you move toward the edge of your cell's range, your cell's base station notes that your signal strength is diminishing.[23] Meanwhile, the base station in the cell you are moving toward (which is listening and measuring signal strength on all frequencies, not just its own one-seventh) sees your phone's signal strength increasing. The two base stations coordinate with each other through the MTSO, and at some point, your phone gets a signal on a control channel telling it to change frequencies. This hand off switches your phone to the new cell.[24]



As you travel, the signal from your phone is passed from cell zone to cell zone.[25] Let's say you're on the phone and you move from one cell to another but the cell you move into is covered by another service provider and not your service provider. Rather than dropping your phone's signal, your call will be transferred to the other service provider.[26]

If the SID on the control channel does not match the SID programmed into your phone, then the phone knows it is roaming.[27] The MTSO of the cell zone that you are roaming contacts the MTSO of your home system, which then checks its database to confirm that the SID of the phone you are using is valid.[28] Your home system verifies your phone to the local MTSO, which then tracks your phone as you move through its cells. All of this happens within seconds.[29]

B. Smartphones and Data Storage

A smartphone is both a mobile phone and a computer.[30] While the traditional feature phones allowed us to communicate via voice and text, smartphones allow us to communicate via talk, text and video; access personal and work e-mail; access the Internet; make purchases; manage bank accounts; take pictures and do many other activities.[31] Smartphones are constantly becoming more integrated into our daily lives. For many people, smartphones serve as a primary source of communication with the rest of the world. While smartphones provide us with a seemingly unlimited amount of resources, the fact is that many of us do not consider the massive amount of personal data that is stored, and therefore accessible, in our smartphones.[32]

Since 2007, more than one billion smartphones have been sold around the world.[33] Recent reports show that two thirds of new mobile buyers are now opting for smartphones over traditional feature cellular phones.[34] As of June 2012, 54.9% of U.S. mobile subscribers owned smartphones.[35] It is anticipated that there will be over 192 million smartphone users by the year 2016.[36] The total estimated population for the United States in 2016 is almost 324 million.[37]

Smartphones now have the capabilities for text messaging/SMS, emailing, instant messaging, social networking, streaming online music, videos/mobile TV, various applications, web browsing, mobile shopping, mobile banking, barcode or QR scanning, NFC/mobile wallet and location-based services/GPS.[38] So what is your smartphone capable of revealing about you?

It is safe to assume that anything you do on your smartphone and any information you store or access is at risk of being accessed by others.[39] Even your service providers collect your data.[40] Unfortunately, service providers are not forthcoming in detailing exactly what data they collect, why the collect it, and what data retention policies they have in place for storage and deletion of your personal data. [41]

What other data should you be aware of on your smartphone? In addition to the data collected by your smartphone service provider, you should also be aware of possible privacy issues surround the collection or disclosures of several other files and data. Any photos, videos, text messages, emails, outgoing and incoming calls, contact information, passwords, financial data, information stored on your phone's calendar, different locations you've visited, your age and your gender are all stored and accessible on your smartphone.[42] This is valuable information for not only criminals and advertisers but also interested law enforcement and government officials.[43]

The ability to collect data on where a person has gone and what they have been doing is valuable information for law enforcement officers.[44] For example, if you are the subject of an investigation or even if you have just been pulled over, police may want to see what you've been doing and where you've been going – things your smartphone may be able to reveal. Thus, the data provided by your smartphone may be used against you in criminal proceedings.[45]

VI. TECHNOLOGIES USED BY THE GOVERNMENT TO COLLECT INFORMATION

A. Cell Phone Software Extractors

In the society we live in today, there are certain States that will allow their police departments to unlawfully search a person's phone without probable cause or a valid search warrant. Michigan for example, has a device that will allow the police to extract the entire contents of a persons' cell phone.[46] These contents include personal contacts, GPS data, videos, pictures and text messages.[47] What's more appalling is the fact that the police are allowed to take this information from a person even if they are not suspected of a crime.[48]

Law enforcement officers could pull a person over for having a tail light out. They would then be allowed to take all the information out of that person's cell phone using the "extraction" device. The officer will have gained access to all private communications stored in the cell phone, as well as GPS information that can tell the officer every location the driver has been to within a set period of time. That officer could then use the GPS information as well as any text communication within the cell phone to create probable cause, obtain a search warrant, and then arrest the driver for a drug smuggling crime that he is involved in.

B. Government Software Surveillance Programs

Between 1997 and 2005, the FBI utilized a software surveillance system called, "Carnivore." Ironically, the FBI chose this name because the system used to "get to the meat of a matter."[49] It worked hand-in-hand with Microsoft Windows operating systems and would filter all internet activity done on the computer.[50] The FBI would use Carnivore to collect information regarding the date and time of emails and was also able to keep track of internet searches.[51] More specifically, Carnivore would match an email being sent or received with warrant information, thereby allowing law enforcement officers to track the internet usage of suspected criminals.[52] This information was believed to be transmitted immediately to the FBI.[53] The FBI has been known to take it a step further and also track the internet usage of anyone that may come into contact with the person under surveillance.[54] Technically the FBI could be watching the internet usage of someone suspected of identity theft and when they log onto Facebook to chat with their cousin, who lives on the other side of the country, the FBI would then feel

justified in invading the reasonable expectation of privacy, the innocent cousin is entitled to, for the simple fact that he was staying in contact with a relative the FBI was watching.

Though the FBI completely abandoned the use of Carnivore in 2005, they had already transitioned to a commercial "tracker" created by NarusInsight called "DCS1000" which stands for Digital Collection System.[55] This unit functions the exact same way as the Carnivore system.

C. Cyber Security Initiatives

In 2010, the Obama Administration released a declassified portion of its cyber security plan.[56] In this report the government partially explains parts of its intrusion detection systems for federal computer systems, as well as, the role the government will play in protecting critical infrastructure.[57] This report stems from a bigger program, the Comprehensive National Cybersecurity Initiative, secretly created by President George W. Bush in 2008.[58] The intrusion detections systems discussed in the report are the Einstein 2 and Einstein 3. The government claims these systems will only be used on federal computer systems for the purpose of inspecting internet traffic entering the network and detecting anything it views as a threat.[59]

The Einstein intrusion detection systems were created by the United States Computer Emergency Readiness Team, which is a branch of the Department of Homeland Security.[60] Einstein 2 is able to analyze the flow of network information and spot possible malicious activity.[61] It is also able to conduct a full inspection of data entering or exiting a network, searching for malicious activity.[62] US-CERT is able to receive immediate alerts from Einstein 2, allowing them to respond quickly.[63] Einstein 3 supports the sharing of information collected with all federal agencies.[64] It gives the Department of Homeland Security the ability to send alerts not containing the content of communications to the National Security Administration, allowing the NSA to support the efforts of the DHS.[65]

Understandably, privacy and civil liberties groups have voiced major opposition to the use of such intrusion detection systems. Mainly because these systems scan the contents of communications in order to intercept "malicious" code before it reaches a "government's" or any other type of network.[66] In 2008, the government released a report detailing the privacy impact on the early versions of Einstein 2.[67] What the government failed to explain in the report was exactly what type of role the National Security Administration would play regarding the programs.[68] The report also fails to mention whether the information that is collected during the scans done by Einstein 2 will be shared with other intelligence agencies or law enforcement officials.[69] As for Einstein 3, the government has yet to release a privacy impact assessment on that program.[70]

The declassified plan also discussed the need for the government to better explain its role when it comes to protecting private critical infrastructure networks.[71] The types of infrastructure the government is referring to includes "electrical grids, telecommunication networks, internet service providers, and the banking and financial industries."[72] The report states that the Department of Homeland Security and other private-sector businesses have been focused on creating "public-private sharing of information regarding cyberthreats and incidents."[73] The report does not get into any more detail about the type of "shared actions" the two sectors have already begun developing.[74] Further proof that the government is already doing what it can behind the scenes to violate our 4th Amendment rights.

D. Stingray and Kingfish Cell Phone Tracking Devices

A "Stingray" is a brand name of an International Mobile Subscriber Identity (IMSI) locator.[75] These devices are used to locate a cell phone regardless of whether the cell phone is being used to make calls.[76] The Federal Bureau of Investigation has determined these devices are

so critical to their ability to monitor individuals that it has established a policy of deleting or "purging" all data gathered during their use.[77] This policy was established to protect the secret workings of the device and prevent civilians in the dark about their capabilities.[78] Sherry Sabol, Chief of the Science & Technology Office for the FBI's Office of General Counsel, says that information about stingrays and related technology is "considered Law Enforcement Sensitive, since its public release could harm law enforcement efforts by compromising future use of the equipment."[79]

Stringrays work by acting as a fake cell-phone tower that allows the government to reroute all network traffic to the fake tower.[80] A cell phone sends out signals every 7 to 15 seconds regardless of whether its owner is making calls.[81] These devices are especially dangerous because they have the capabilities to collect the contents of all electronic and wire communications, including innocent people, while locating a targeted individual.[82] The Stringray "tricks the cell phone into connecting to it, rather than a real cell phone tower, which allows the government to determine who, when and to where the user is calling, the precise location of every device within the range, and with some devices, even capture the content of your conversations."[83] But the Stingray does not focus on an individual. The device captures the information of everyone within its range – which can span several kilometers.[84] This means that potentially thousands of people are having their right to privacy violated every time one of these devices is activated.[85]

One of the greatest concerns with these devices is that they allow law enforcement to conduct broad searches amounting to "general warrants," the exact type of evil the Fourth Amendment was intended to eliminate.[86] To add to this concern, law enforcement officers are often interpreting the law as they see fit. These officers may obtain court orders, but not necessarily search warrants, when using the Stingray devices.[87] It is also concerning that government agents and U.S. attorneys making those request don't provide details concerning how the devices work and seem to have difficulty explaining the technology.[88] This has created concern among judges, asking how an order or warrant could even be obtained without first telling the judge what the technology was being used for.[89]

Finally, and perhaps the greatest concern, is that the evidence collected against an individual is destroyed before a case ever goes to trial.[90] The law governing search warrants establishes how warrants are executed and usually requires that information to be returned to the issuing judge.[91] This means an individual is denied access to the same information that was used to arrest him because the evidence is destroyed before either the defendant or the fact finder has the opportunity to review it. Additionally, this policy was established internally through the FBI, not through case law or legislation. The FBI argues that they are justified in destroying the evidence for security purposes and because they don't intend to use the evidence in court because it is only used to establish the general location of their target.[92] The fact is that when the government hides what it is doing, it bypasses an important check on government power and violates fundamental rights established by our Constitution to protect American citizens from this exactly this kind of evil.

One of the most disturbing cases of cell phone tracking devices comes out of Fort Worth. In February 2012, the Fort Worth City Council granted the police department's request to spend $184,000 on technology specifically used to track cell phone locations.[93] The department sent a memo to City Council where it promised to use the "KingFish" tracking system "to establish probable cause in criminal cases."[94] The KingFish is a device which acts like a dummy cell phone tower.[95] Cell phones then unknowingly "ping" off the KingFish device. It is now

unnecessary for police to acquire court orders making the cell phone service providers release that type of information.[96] Law enforcement officials essentially told City Council they are going to erase the 4th amendment of the Constitution and bypass the requirement to show a judge that they have established sufficient probable cause to acquire a search warrant to get the type of information they are now able to acquire on their own.

E. Third Party Records

The Board of Directors for the National Association of Criminal Defense Lawyers in February of 2012 adopted a document on "Electronic Surveillance & Government Access to Third Party Records." At http://www.nacdl.org/reports/thirdpartyrecords/

The document discusses the growing debate over the preliminary showing of proof for obtaining third party information. Court precedent has been clear that a person does not have a reasonable expectation of privacy to thing that they expose to the public. *See United States v. Miller*, 425 U.S. 435 (1976) and its progeny. In this digital age that exposure has grown to almost an all-encompassing summary of your life. As Justice Sotomayor noted in *U.S. v. Jones* "people disclose the phone numbers that they dial or text to their cellular providers; the URL's 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." *Jones*, 132 S.Ct. at 957. Sotomayor continues by stating that "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." *Id.* As the NACDL document reiterates the decision in Jones has cast doubt on the viability of the "third party doctrine." Further Sotomayor did not list facebook entries, SMS text messages (even if deleted), device locator records, keystrokes of a computer, and documents loaded on a cloud but only shared with specific people. All of these reveal intimate personal details of persons lives and yet in many instances they are subject to seizure by a simple subpoena.

The Electronic Communications Privacy Act (ECP), the Stored Communications Act (SCA), the USA Patriot Act, Wiretap Act, and the Foreign Intelligence Surveillance Act (FISA) all govern the standards which control the collection and use of third party data. These provisions create distinctions between content, non-content information, electronic communication service (ECS), remote computing service (RCS). Many of these statutes were created well before the modern proliferation of smart phones and mobile computing technologies leading the NACDL to advocate for a modern rewriting of the laws governing this all important Fourth Amendment doctrine because of the obsolete status of current statutes.

The Board of Directors for the NACDL has thus adopted "Policy Recommendations to Protect the Privacy of Electronic Communications:"

> 1. The content of any electronic communication that is sought by a law enforcement official should only be obtained through a warrant based on probable cause, adhering to the requirements for specificity and particularity in the application for the warrant, the particularity clause of the warrant, as well as the execution of the warrant.
>
> 2. The definition of "content" information should be amended to cover any information that will demonstrate the substance of an electronic communication, to include private emails, instant messages, text messages, word processing documents and spreadsheets, photos, internet search queries and

private posts made over social networks. This would include any information found in any third party records, including information stored within a cloud system, and transactional information that can reveal the content of an electronic communication, including a search query string, a URL, browser history and email subject lines.

3. Congress should amend the Electronic Communications Privacy Act (ECPA) and eliminate the RCS and ECS distinctions, and the 180 day "rule."

4. Law enforcement must be required to obtain a warrant based on probable cause to obtain prospective or retrospective geo-location information-whether by way of a third-party service provider, or by direct use of a GPS device to track a suspect's movements.

5. Opened email, even though found on a third-party service provider's service, should only be obtainable by way of a warrant based on probable cause.

6. Congress should statutorily extend the exclusionary rule to apply to searches that do not comply with these warrant requirements.

These recommendations will help to conform statutes and jurisprudence to the needs of modern technology so that the third party doctrine is consistent with a person's reasonable expectation of privacy.

F. Google Privacy Policies

New privacy policies for Google became effective March 1, 2012. The new polices expand what internet services within the google corporation can have access to your "personal information." Some specific highlights of these policies are listed below.

1. Google may collect device-specific information (such as your hardware model, operating system version, unique device indentifiers, and mobile netwoek information including phone number). Google may associate your device identifiers or phone number with your google Account.

2. When you use Google services or view content provided by Google, they may automatically collect and store certain information in server logs. Including your internet protocol (IP) address.

3. When you use a location-enabled google service, google may collect and process information about your actual location, like GPS signals sent by a mobile device. Google may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.

4. Google may store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.

5. After deleting information from Google services, "we may not immediately delete residual copies from our active servers and may not remove information from our backup systems."

6. Google will share personal information with companies, organizations or individuals outside of Google if they have a "good-faith" belief that access, use, preservation or disclosure of the information is reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request.

These new policies vary significantly from the previous policies which required consent from the user for sharing of sensitive personal information. The old system was one where you had to "opt-in for sharing of sensitive personal information. However they still honored enforceable governmental request to turn over data that Google holds.

G. Millions of Subpoena Requests by Law Enforcement

In early 2012, Congressman Ed Markey asked major phone carriers to reveal "how often they give users' data to the government and under what circumstances."[97] The carriers responded, but left out a lot of key information.[98]

"Sprint received 500,000 subpoenas for its data from law enforcement in the last year. That doesn't include court orders for wiretaps and location data, which Sprint didn't track annually but which added up to 325,982 requests in the last five years. The company also says it doesn't have the resources to track how many of those requests it responded to or rejected. The company has 221 employees dedicated to processing and responding to government requests for its data."[99]

"Verizon received 260,000 requests for its users data in 2011, including wiretaps, calling records, text message information, and location information, but doesn't add how many of them were filled." [100]

"AT&T received 131,400 subpoenas in criminal cases for its information in 2011, as well as 49,700 warrants or orders that it hand over data. It rejected 965 of them. The company says it employs more than 100 staffers full-time to respond to law enforcement demands."[101]

"T-Mobile told Congressman Markey it "does not disclose" the number of law enforcement requests it receives or complies with." [102] "MetroPCS says received fewer than 12,000 requests a month on average for the last six years."[103] "Cricket received 42,000 requests last year, and U.S. Cellular received 19,734 in 2011."[104] "The New York Times counts a total of 1.3 million requests for users' information in the last year based on Markey's data."[105]

The A.C.L.U. used the Freedom of Information Act to obtain information from various law enforcement agencies around the country about their policies regarding "data requests to phone carriers."[106] The information retained by the organization revealed a frightening trend. More agencies are using cell phones as the central tool of their investigations.[107] Growing in popularity amongst law enforcement agencies are requests for "cell tower dumps."[108] Upon the approval of a "tower dump" request, law enforcement officials receive "all the stored information collected from all users of a cell phone tower, without a warrant."[109] For example, if police officers are trying to investigate the alibi of someone they suspect of murder, they would request a "cell tower dump" from towers where the suspect claims to have been. Once the request is approved, not only will officers have the location information and other cell phone data from the person they suspect of a crime, but they will have gained access to thousands of innocent peoples' information because they happened to "ping" off the same cell tower a suspected criminal used.

When it comes to internet surveillance, law enforcement officials are less likely to request information from internet services.[110] Phone companies estimate annual information requests in the hundreds of thousands but Google reports that they received merely 12,271 requests in 2011.[111]

H. Types of Information Law Enforcement Extracts from a Cell Phone

Until recently, most people had no clue as to what law enforcement officials actually harvested from their phones whenever a search was conducted. New information shows that whenever law enforcement officials search a person's phone, they collect all call logs, text

messages, geo-locations, and on certain devices, Apple iPhone, in particular, law enforcement officials are able to collect information from the iMessage application.[112] If law enforcement officials deem it necessary, they can use more advanced methods and acquire a device's "web history, data files, wireless networks, and the user's custom dictionary."[113] The devices that law enforcement officials use to acquire cell phone information also extracts the device's geo-location points, including cell tower information.[114] Once this type of information is obtained, police officers are able to pinpoint where a cell phone has been over a set period of time by tracking the cell towers the cell phone uses while a call is taking place.[115] This is how police officers are able to discover the location of a suspect they are investigating.

With the growing popularity of smart-phones and cell phones that are capable of accessing email and the internet, law enforcement officials are able to gain access to an overwhelming amount of information, when accessing a person's cell phone, whether that information is used in the investigation or not.[116] The Stored Communications Act gives many law enforcement agencies an excuse to bypass the need to give subpoenas or search warrants to service providers, such as, Apple, Google, or anyone who provides email or internet service to the device, because this type of information is already stored on the device of someone law enforcement officials believe committed a crime.[117] This is a big issue for privacy groups, the A.C.L.U., for example, stated their concern, "We would have never carried around several years' worth of correspondence on our person, for example, but today, five-year-old emails are just a few clicks away using the smart-phone in your pocket. The fact that we now carry this much private, sensitive information around with us means that the government is able to get this information, too." [118]

With the use of cell surveillance growing in popularity amongst law enforcement officials, cell phone carriers are being inundated with request from law enforcement agencies to help them with investigations by providing information regarding text messages, caller locations and other information stored by the cell phone service providers.[119] In 2011, cell phone providers reported that they responded to over 1.3 million demands for subscriber information.[120] Though this number is high, many cell phone service providers reject a lot of the requests coming from law enforcement agencies.[121] Carriers report that they've considered many of the demands for information legally questionable or unjustified.[122] Understandably, cell phone carriers are hesitant to jump at the demands of federal agencies. In 2007, the F.B.I. was criticized for improperly sending "emergency" letters to cell phone carriers.[123] The purpose of these letters was to retain information on "thousands" of phone numbers in what they reported to be "counter-terrorism" investigations.[124] The F.B.I. was allowed to side-step the requirement of getting a valid warrant and it was later discovered that none of these reported investigations involved actual emergencies.[125] The reason those carriers never second guessed the F.B.I. is because when law enforcement officials deem a situation an "emergency" there are less formal requirements needed to obtain the information.[126]

Cell phone companies report that it is not only the top federal agencies that are demanding information.[127] They've stated that these demands are coming from all levels of the government.[128] Local police are making request to help aid in their investigations of street crimes, while the higher up State and Federal agencies are requesting information to aid in their investigations of financial and intelligence crimes.[129]

Due to the overwhelming amount of law enforcement agencies requesting information, cell companies have been forced to establish legal departments whose goal is to focus solely on the legitimacy of requests coming from these agencies.[130] In 2012, AT&T reported they

responded to over 700 requests a day.[131] Many of those request being "emergency requests" that do not require the typical search warrant granted by a judge after showing proof of probable cause for the information.[132]

---

[1] Jonathan M. Seidl, *Mich. Cops Can Now Steal Your Cell Phone Data—'Without the Owner Knowing,'* THE BLAZE (April 20, 2011 9:28 AM), http://www.theblaze.com/stories/2011/04/20/mich-cops-can-now-steal-your-cell-phone-data-without-the-owner-knowing/
[2] *Id*.
[3] *Id*.
[4] 18 U.S.C. § 3122(a).
[5] 18 U.S.C. § 3122(b)(2).
[6] 18 U.S.C. § 2703 (2009).
[7] http://www.nielsen.com/us/en/reports/2013/mobile-consumer-report-february-2013.html
[8] *Id*.
[9] *Id*.
[10] http://www.privateline.com/mt_cellbasics/index.html
[11] http://electronics.howstuffworks.com/cell-phone1.htm
[12] http://en.wikipedia.org/wiki/Cellular_network
[13] *Id*.
[14] http://electronics.howstuffworks.com/cell-phone1.htm
[15] http://electronics.howstuffworks.com/cell-phone3.htm
[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] http://www.google.com/patents/US4698839
[21] http://electronics.howstuffworks.com/cell-phone3.htm
[22] *Id*.
[23] *Id*.
[24] *Id*.
[25] *Id*.
[26] *Id*.
[27] *Id*.
[28] *Id*.
[29] *Id*.
[30] https://www.privacyrights.org/fs/fs2b-cellprivacy.htm
[31] *Id*.
[32] *Id*.
[33] http://www.statista.com/topics/840/smartphones/
[34] http://www.nielsen.com/us/en/newswire/2012/two-thirds-of-new-mobile-buyers-now-opting-for-smartphones.html
[35] *Id*.
[36] http://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/
[37] http://www.census.gov/population/projections/data/national/2012/summarytables.html
[38] http://www.nielsen.com/us/en/newswire/2012/two-thirds-of-new-mobile-buyers-now-opting-for-smartphones.html
[39] https://www.privacyrights.org/fs/fs2b-cellprivacy.htm
[40] *Id*.
[41] *Id*.
[42] *Id*.
[43] *Id*.
[44] *Id*.
[45] *Id*.

[46] Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, THE NEW YORK TIMES (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&_r=0.
[47] *Id.*
[48] *Id.*
[49] Cory Janssen, *Carnivore*, TECHOPEDIA (last visited Apr. 26, 2013), http://www.techopedia.com/definition/10243/carnivore.
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] Kim Zetter, *U.S. Declassifies Part of Secret Cybersecurity Plan,* Wired.com (Mar. 2, 2010, 4:19PM), http://www.wired.com/threatlevel/2010/03/us-declassifies-part-of-secret-cybersecurity-plan/.
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] Stingrays: The Biggest Unknown Technological Threat to Cell Phone Privacy You Don't Know About https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy
[76] 'Stingray' Phone Tracker Fuels Constitutional Clash http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] When Secretive Stingray Cell Phone Tracking "Warrant" Isn't A Warrant https://www.eff.org/deeplinks/2013/03/when-stingray-warrant-isnt-warrant
[81] https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html
[88] Judge Questions Tools That Grab Cellphone Data on Innocent People http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people/
[89] http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html
[90] *Id.*
[91] *Id.*
[92] *Id.*

[93] Zack Shlachter, *KinFish-ing for Info*, Fort Worth Weekly (May 30, 2012), http://www.fwweekly.com/2012/05/30/kingfishing-info/.
[94] *Id*.
[95] *Id*.
[96] *Id*.
[97] Andy Greenberg, *Here's How Often AT&T, Sprint, and Verizon Each Hand Over Users' Data to the Government*, FORBES (July 7, 2012, 11:00AM), http://www.forbes.com/sites/andygreenberg/2012/07/09/by-the-numbers-heres-how-often-att-sprint-and-verizon-hand-over-users-data-to-the-government/.
[98] *Id*.
[99] *Id*.
[100] *Id*.

[101] *Id*.
[102] *Id*.
[103] *Id*.
[104] *Id*.
[105] *Id*.
[106] *Id*.
[107] *Id*.
[108] *Id*.
[109] *Id*.
[110] *Id*.
[111] *Id*.
[112] Zack Whittaker, *How Much Data Can Police Swipe From Suspects' Phones Without a Warrant*, ZD.NET (Feb. 27, 2013, 12:58 GMT), http://www.zdnet.com/how-much-data-can-police-swipe-from-suspects-phones-without-a-warrant-hint-a-lot-7000011891/.
[113] Id.
[114] Id.
[115] Id.
[116] Id.
[117] Id.
[118] Id.
[119] Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, THE NEW YORK TIMES (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&_r=0.
[120] Id.
[121] Id.
[122] Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, THE NEW YORK TIMES (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&_r=0.
[123] Id.
[124] Id.
[125] Id.
[126] Id.
[127] Id.
[128] Id.
[129] Id.
[130] Id.
[131] Id.
[132] Id.