SUPREME COURT OF THE UNITED STATES

October Term 2015

_____

Docket No. 2015-11

_____

Albert Greene,

Petitioner

v.

United States of America,

Respondent

_____

ON PETITION FOR WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE THIRTEENTH CIRCUIT

The University of San Diego School of Law
27th Annual National Criminal Procedure Tournament November 5-8, 2015
San Diego, California

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF ARCADIA

UNITED STATES OF AMERICA, Plaintiff, vs. ALBERT GREENE, Defendant	Case No.: 4:11-cr-2015-T (CVW) ORDER: ORDER GRANTING DEFENDANT'S MOTION TO SUPPRESS

On September 5, 2015, Albert Greene ("Defendant") was indicted for fifteen violations of federal law. These criminal charges arise out of Defendant's alleged illegal firearm trafficking and transportation of controlled substances. Now pending before this Court is Defendant's motion to suppress evidence seized pursuant to a search of his private computer hard-drive and subsequent motion to dismiss the indictment.

For the following reasons, the Court **GRANTS** Defendant's motion to suppress evidence obtained in violation of the Fourth Amendment.

I. STATEMENT OF FACTS

On August 10, 2015, James Tejada accessed a personal desktop computer owned by Defendant. Tejada and Defendant were co-residents in a two-bedroom apartment located in downtown Arcadia. Tejada entered Defendant's room and logged on to Defendant's computer to check his personal email. Defendant did not give Tejada permission to use his computer nor was Defendant aware that Tejada ever intended to use his computer.

In recent years, Arcadia has been a focal target area for illegal firearm and drug trafficking operations. As a result, local gangs claimed territories within the city, causing violent crime and homicide rates to skyrocket in the six months preceding the incident in question. In response, the Drug Enforcement Agency ("DEA") instituted a special initiative to encourage citizens of Arcadia to actively participate in the ongoing investigation of suspicious activity tied to the firearm and drug trafficking. Advertisements and billboards were across the city depicting the slogan: "If you see something, say something!" A television advertisement with the same slogan invited "crime stopper tips" from local citizens with the promise of financial compensation[1] for any information about illegal trafficking operations.

Tejada saw many of these television advertisements and was familiar with the $10,000 reward offered by the DEA. Tejada suspected that Defendant might be involved in some sort of illegal activity because he left their apartment at odd hours of the night and noticed that Defendant appeared to have large quantities of cash on hand regularly. Accordingly, Tejada began a personal investigation of Defendant's computer. While browsing through Defendant's

---

[1] The DEA initiative provided up to $10,000 for information that directly led to an arrest for illegal firearms and narcotics trafficking. These rewards also offer the opportunity for individuals directly involved in these operations to come forward with information with no questions asked about how the information was obtained.

computer, Tejada located a file on an external hard-drive labeled "photos." The external hard-drive was linked to the computer through a wireless router. Tejada opened the "photos" file and immediately viewed several photographs depicting large amounts of what he believed to be illegal drugs concealed in compartments of various automobiles. Defendant did not appear in any of these images. Shortly thereafter, Tejada turned off the computer and left the shared residence. Tejada contacted the police department and informed the dispatch operator about what he observed on Defendant's computer. He explained that he saw several photographs showing cars being loaded with illegal drugs.

Later that afternoon, Aaron Smith, an agent with the DEA arrived at Tejada's residence in response to his report. Agent Smith asked Tejada to show him the location of the computer. Tejada led Agent Smith to Defendant's room where the computer and external hard-drive were positioned on a desk. At that time, Tejada told Agent Smith that he found the images on the hard-drive after he entered Defendant's room without his permission or knowledge.

Agent Smith instructed Tejada to log on to Defendant's computer to show him where the images were stored. Agent Smith then asked Tejada to browse through the images. Tejada clicked on the first image and continued to scroll through the remaining images by pressing the down arrow on the keyboard. The first few photographs depicted large quantities of what Agent Smith recognized as methamphetamine, concealed inside compartments of multiple automobiles. As Tejada continued to scroll through the images, he also observed several photos of Defendant holding guns in both hands. Based on his training and experience, Agent Smith recognized the firearms as military issued automatic weapons. Based on the photographs, Agent Smith became increasingly suspicious that Defendant was involved in the illegal firearm and narcotics

trafficking plaguing the area. Agent Smith seized the external hard-drive to conduct a follow-up investigation of the images.

On August 23, 2015, as part of the ongoing investigation, the Government applied for an order from Magistrate Judge Timothy J. Thomas of this Court, pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, et seq., which ordered Verizon Wireless, Inc. to disclose to the government "the identification and address of cellular towers (cell site locations) related to the use of [Defendants' cellular telephone]." The Government sought location data for a period of 205 days (January 8, 2015 through August 1, 2015), which it argued would provide a sufficient amount of information to assess where Defendant's cell phone was primarily used and whether his conduct was consistent with an illegal trafficking operation.

On that same day, Magistrate Judge Thomas granted the Government's application. Specifically, Magistrate Judge Thomas applied the well-defined standard proscribed by the Stored Communications Act and made a factual finding that the Government "offered specific and articulable facts showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation." Magistrate Judge Thomas based his findings on the photographs discovered on Defendant's computer and Tejada's statements about Defendant's behavior.

The cell site location information ("CSLI") records resulted in over 5,000 data points for the entirety of the 205 day period. Each data point represented a signal transmission sent or received from, Defendant's cell phone and the closest cell tower at that time. Location information was created every time Defendant placed a phone call, sent a text message, or checked his personal email. Additionally, location data was created every time Defendant received a phone call or message, regardless of whether he answered the call.

The CSLI records indicated that Defendant frequently traveled to a location seventeen miles east of downtown Arcadia. Agent Smith located a warehouse in the general area that he suspected might be associated with Defendant. Agent Smith surveyed the warehouse for several days and observed Defendant traveling to and from the warehouse on multiple occasions at odd times during the night. Additionally, Agent Smith noticed numerous unmarked moving vans parked outside the warehouse during the daytime hours.

On August 30, 2015, Superior Court Judge Tanya Lopez issued a search warrant for the warehouse based on the photographs, the historical CSLI records, and Agent Smith's observations. DEA agents subsequently searched the warehouse and discovered a cache of illegal firearms and methamphetamine. By volume, the trafficking operation was one of the largest in the state. The DEA seized over 1,000 kilograms of methamphetamine and 200 illegal weapons.

On September 1, 2015, Judge Lopez issued an arrest warrant for the Defendant, Albert Greene. On September 5, 2015, a grand jury indicted Defendant on fifteen counts for illegal transportation of controlled substances and trafficking of illegal firearms.

Defendant moves to suppress the following: (1) any images Agent Smith discovered during the search of the external hard-drive that Tejada did not observe during the preceding private search; and (2) the CSLI records and any evidence gathered as a result of reviewing those records.

II. ANALYSIS

This Court finds that Agent Smith's search of Defendant's external hard-drive improperly exceeded the scope of Tejada's preceding private search and thereby violated the Fourth Amendment. Furthermore, the government's warrantless search of Defendant's CSLI records violated the Fourth Amendment.

1. THE PRIVATE SEARCH DOCTRINE

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. As the Supreme Court has explained, a "search" for Fourth Amendment purposes exists when the Government obtains evidence as a result of a physical intrusion on persons, houses, papers, or effects. Florida v. Jardines, 133 S.Ct. 1409, 1414 (2013). In circumstances where a physical trespass is not present, a "search" occurs where (1) a person has a subjective expectation of privacy in the information obtained, and (2) society is willing to recognize the person's expectation of privacy as objectively reasonable. See Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); see also Kyllo v. United States, 533 U.S. 27, 33 (2001). Further, searches conducted without a warrant are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." Arizona v. Gant, 556 U.S. 332, 338 (2009) (quoting Katz, 389 U.S. at 357) (internal quotation marks omitted).

The Fourth Amendment only protects against governmental action. United States v. Lichtenberger, 786 F.3d 478, 482 (6th Cir. 2015). It does not apply "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." Id. (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)); see also United States v. Jacobsen, 466 U.S. 109 (1984). The Fourth Amendment applies to a search conducted subsequent to a private search only where the government's search exceeds the scope of the private search. Walter, 447 U.S. at 657. Accordingly, no matter how unreasonable Tejada's original search of his roommate's computer might have been, this is not the search that is properly addressed under

the law. Instead, we must determine whether Agent Smith's subsequent search remained within the scope of Tejada's private one.

The Supreme Court of the United States has not yet addressed the issue of how to define the scope of the private search doctrine within the context of computers and electronic storage devices. Because this is a novel issue, we look to our sister circuits for guidance in determining the proper scope to apply. Several circuits have addressed the issue with conflicting results. Upon surveying the circuit decisions that address this issue, the majority appears to find the scope of the private search doctrine limited to the specific items that the private party actually observed prior to any government involvement.

By way of example, the Sixth Circuit held that a search exceeded the scope of the initial private search, and thus violated the Fourth Amendment, where the officer viewed photographs that were not observed during the prior, private search. Lichtenberger, 786 F.3d at 485. The court focused on the "extensive privacy interests at stake in modern electronic device[s]" and the amount of "information the government stands to gain when it re-examines the evidence. Id. at 485-86.

Here, the record clearly establishes that Agent Smith observed images that Tejada did not observe in the preceding private search. Up until the point Tejada showed Agent Smith the additional photographs depicting the illegal firearms, Agent Smith's search did not violate Defendant's Fourth Amendment rights. Therefore, all subsequently viewed images violated the Defendant's Fourth Amendment rights. Furthermore, just as in Lichtenberger, there are significant privacy interests at stake. The amount of information stored on Defendant's personal computer was significant. This Court is not prepared to expand the private search doctrine to information that goes beyond that uncovered in the preceding private search.

The Government has asked us to adopt the "separate closed container" analysis as set forth in United States v. Runyan, 275 F.3d 449 (5th Cir. 2001). In Runyan, the Fifth Circuit held that the government did not exceed the scope of the preceding private search where it examined photographs on a computer disk that the private party did not observe. Id. at 465; see also Rann v. Atchison, 689 F.3d 832, 837 (7th Cir. 2012). Runyan, and its progeny, fail to appreciate the nature of modern electronic storage devices and the privacy interests involved. There is a fundamental difference between the CD's in Runyan and the essentially unlimited storage capacity of modern computers and external hard-drives. The government's position is untenable in the digital age and to include all information that might be stored on a computer hard-drive would render the protections of the Fourth Amendment meaningless in many circumstances.

If this Court were to follow the Government's position to its logical conclusion, we would be obligated to allow a search of the entire computer hard-drive based on Tejada's original, limited search of that computer. Tejada viewed only a portion of the photographs that were eventually searched by Agent Smith. A computer hard-drive should not be considered a "separate closed container" for the purposes of the private search doctrine. When Agent Smith viewed images beyond what Tejada initially observed, he exceeded the scope of the initial private search.

Accordingly, the additional images discovered by Agent Smith must be suppressed.

2. CELL SITE LOCATION INFORMATION AND THE THIRD-PARTY DOCTRINE

Even if a portion of the initial search was illegal, the Government contends that the photographs properly found pursuant to the private search doctrine would have supported their request for Defendant's CSLI records. Therefore, the Court must consider whether the CSLI records were properly searched.

Defendant argues that the warrantless search of his historical CSLI records violated his Fourth Amendment rights and, therefore, any items found in the warehouse as the result of the CSLI should be suppressed. In response, the Government argues that the third-party doctrine applies to historical CSLI records and therefore, no Fourth Amendment violation occurred.

Under the third-party doctrine, "[a] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743-744 (1979). "It is that voluntary conveyance—not the mere fact that the information winds up in the third party's records—that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of privacy." United States v. Graham, No. 12-4659, 2015 WL 4637931, at *15 (4th Cir. 2015).

Here, the historic CSLI must be suppressed because Defendant did not voluntarily convey his CSLI and therefore did not assume the risk that Verizon would disclose the information to law enforcement. While there is disagreement among the circuits as to whether the third-party doctrine applies to CSLI, this Court finds the reasoning in Graham particularly persuasive.

In Graham, the government sought to obtain historical CSLI from the defendant's phone over a 221 day period. Graham, 2015 WL 4637931 at *3. The court held that the third-party doctrine did not apply to the CSLI because cell phone users do not voluntarily convey CSLI. Id. at *15. The service provider automatically generates historical CSLI whenever the phone connects to the provider's network. See Com. v. Augustine, 4 N.E.3d 846, 862 (Mass. 2014). Of importance to the analysis, historical CSLI includes information about phone calls made by the user, as well as incoming phone calls received but not answered by the user. See In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to

Disclose Records to the Government (In re Application (Third Circuit)), 620 F.3d 304, 317 (3rd Cir. 2010). Information contained in historical CSLI records therefore necessarily includes information that is not "actively disclosed" by the user. Graham, 2015 WL 4637931 at *15.

Here, the Government searched 205 days of Defendant's historic CSLI records. Equipped with that information, the Government located a warehouse that Defendant traveled to on several occasions. Defendant could not have known Verizon was tracking his location with such specificity. Nor was Defendant aware of what cell towers his phone was transmitting information to or where those cell towers were located.

Furthermore, a large portion of the data location entries contained in the CSLI records related to unanswered calls received by Defendant's cell phone and unsolicited email communications sent to Defendant. It cannot be said that Defendant "voluntarily conveyed" that location information to Verizon Wireless if he did not actively submit the transmission. These processes are automatic and completed without notice to the user.

The Fifth Circuit, in In re Application of U.S. for Historical Cell Site Data (In re Application (Fifth Circuit)), 724 F.3d 600 (5th Cir. 2013), and the en banc Eleventh Circuit in United States v. (Quartavious) Davis, 785 F.3d 498 (11th Cir. 2015), extended the third-party doctrine to historic CSLI records. Those cases held that, because cell phone users voluntarily use their cell phones and are generally aware that their cell phones transmit a signal to a cell tower, they voluntarily provide this information to a third-party, namely, a cellular provider. In re Application (Fifth Circuit), 724 F.3d at 613. Here, the Government asks us to accept this position.

This Court cannot accept that proposition. Cell phone use is integral to participating in modern society. See Graham, 2015 WL 4637931 at *16. "People cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society

through use of their cell phones." Id. If this Court were to extend the third-party doctrine to the CSLI records in question, it would undoubtedly result in a substantial reduction in the protections afforded by the Fourth Amendment.

For the forgoing reasons, this Court holds that the Government violated Defendant's Fourth Amendment rights when it searched his historical CSLI over a period of 205 days.

CONCLUSION & ORDER

In light of the forgoing reasons, the Court GRANTS Defendant's motion to suppress the images and CSLI records.

IT IS SO ORDERED.

_____
George M. Williams
United States District Judge

UNITED STATES COURT OF APPEALS FOR THE THIRTEENTH CIRCUIT

UNITED STATES OF AMERICA, *Petitioner*, v. ALBERT GREENE, *Respondent*.	No. 13-2015 D.C. No. 4:11-cr-2015-T (CVW) OPINION

Appeal from the United States
District Court for the Southern
District of Arcadia
George M. Williams, District Judge,
Presiding

Argued and
Submitted
September 8, 2015—Casadena,
Arcadia

Filed
September
7, 2015

Before: William P. Draber, Susan K. Stiles, and John J. Jackson, Circuit Judges

Opinion by Judge
Jackson

OPINION

JACKSON, J. Circuit Judge:

I. BACKGROUND

Because the facts of the case are not disputed, this Court hereby adopts and incorporates by reference the facts from the opinion below. The parties' standing on their respective claims is not in dispute.

II. ANALYSIS

This appeal arises from the serendipitous discovery of a large-scale drug and firearm trafficking operation that went undetected for several years. After Respondent's roommate stumbled across several photographs of the operation on his home computer hard-drive, DEA agents were able to successfully locate one of the largest illegal trafficking operations in the state. On September 5, 2015, a grand jury indicted Respondent on fifteen counts for illegal transportation of controlled substances and trafficking of illegal firearms.

Before trial, Respondent successfully moved to suppress certain evidence. After a lengthy oral argument and supplemental briefing by both parties, the District Court granted both motions. Petitioner, the Government, timely appealed both motions.

We disagree with Respondent and overrule the District Court's rulings on both motions. First, we find that the scope of Agent Smith's search did not exceed Tejada's preceding private search. Second, we find that the third-party doctrine applies to historic CSLI records, therefore, the Government's search of Respondent's CSLI records did not violate his Fourth Amendment rights.

1. THE SCOPE OF THE PRIVATE SEARCH DOCTRINE

On appeal, Petitioner argues that Agent Smith's review of the images was valid under the private search doctrine, which permits a government agent to verify the illegality of evidence discovered during a private search. Respondent argues that Agent Smith's warrantless examination of his external hard-drive was a search that violated the Fourth Amendment because it exceeded the scope of Tejada's previous search.

In *Katz v. United States*, 389 U.S. 347 (1967), the Supreme Court established that a "search" occurs for Fourth Amendment purposes when the Government violates a subjective expectation of privacy that society considers objectively reasonable. *See id*. at 360-61 (Harlan, J., concurring). The Fourth Amendment protects not only tangible goods, but also privacy interests. *Id*. at 352-353. If a person has a reasonable expectation of privacy in any information, it is protected by the Fourth Amendment. People have a reasonable expectation of privacy in their personal computers. *United States v. Ziegler*, 474 F.3d 1184, 1191-92 (9th Cir. 2007). However, the Fourth Amendment does not apply to private individuals, not acting as agents of the Government or on behalf of the Government. *Walter v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting). Even where the initial invasion by the private party is unreasonable or deliberate, the Fourth Amendment is not implicated. *United States v. Jacobsen*, 466 U.S. 109, 109 (1984). Then, a warrantless follow-up search by a government agent falls within the "private search doctrine." *Walter*, 447 U.S. at 657.

At the outset, we recognize a significant division among federal appellate courts on this issue. An inquiry into the proper scope to apply for the private search doctrine necessarily requires a fact specific analysis. We hold that Agent Smith's search did not

violate Respondent's Fourth Amendment rights. In so doing, we apply the "closed container" approach as articulated in *United States v. Runyan*, 275 F.3d 449, 464 (5th Cir. 2001).

"[P]olice do not exceed the private search when they examine more items within a closed container than did the private searchers." *Id*. Additionally, "police do not exceed the scope of a prior private search when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties." *Id*.; *see also Rann v. Atchison*, 689 F.3d 832, 838 (7th Cir. 2012) (upholding a search where the private party did not observe the images on a memory card.); *compare United States v. Lichtenberger*, 786 F.3d 478, 485 (6th Cir. 2015) (finding that the private search exceeded the scope where the officer viewed images that were not observed during the previous private search.)

First, Petitioner argues that the external hard-drive is a closed container for purposes of the private search doctrine. We agree. The external hard-drive was wirelessly connected to the desktop computer. The images contained on the external hard-drive were only accessible through a folder on the desktop computer labeled "photos." Furthermore, the sole function of the hard-drive was data storage. For Fourth Amendment purposes, the hard-drive is similar to a CD, albeit capable of storing larger quantities of information. It is unlike the laptop computer in *Lichtenberger* because it does not function like a personal computer. The hard-drive does not have any computational abilities, nor can it access the Internet or run software.

Moreover, many of the privacy issues presented by cell phones do not exist in the context of external hard-drive devices. Although an external hard-drive may contain

many kinds of data, in vast amounts, and corresponding to a long swath of time, it does not include call logs, detailed accounts of texts messages, or location information.

Second, Petitioner argues that because the external hard-drive is a closed container, Agent Smith's search fell within the scope of Tejada's initial search. Like the CDs in *Runyan*, as long as Tejada viewed at least one image on the hard-drive, Agent Smith could lawfully search the entire hard-drive. On these facts, we agree as well.

We find the court's reasoning in *Runyan* persuasive on this issue. If this Court were to hold that the search exceeded the scope, "police would exceed the scope of a private investigation and commit a warrantless 'search' in violation of the Fourth Amendment each time they happened to find an item within a container that the private searchers did not happen to find." *Runyan*, 275 F.3d at 465. This approach would deter police from properly conducting their investigations and frustrate the investigation of containers where no expectation of privacy exists. *Id*.

We hold that the external hard-drive at issue is a closed container for the purpose of the private search doctrine. Because the hard-drive is a closed container, Agent Smith's search did not exceed the scope of Tejeda's private search.

2. CSLI RECORDS AND THE THIRD PARTY DOCTRINE

On appeal, Petitioner argues the trial court erred in granting Respondent's motion to suppress the historic cell site location information ("CSLI") records because a cell phone user has no expectation of privacy in business records conveyed to a third party. Respondent argues that the Government's warrantless acquisition of his historical cell site location information violated his Fourth Amendment rights and must be suppressed. We agree with Petitioner. The third-party doctrine applies to historical CSLI, therefore,

Respondent does not have a legitimate expectation of privacy in the historical CSLI obtained by the Government.

The third-party doctrine establishes 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 (1979) (citations omitted), *See also*, *United States v. Miller*, 425 U.S. 435, 443 (1976) (finding that the third-party doctrine applies to bank records.) By "revealing his affairs to another" an individual "takes the risk…that the information will be conveyed by that person to the Government." *Id.* at 443.

Defendant did not have a reasonable expectation of privacy in the CSLI recorded by Verizon Wireless. In *Smith v. Maryland*, the Supreme Court held that the third-party doctrine applied to dialed telephone numbers. *Smith*, 422 U.S. at 745-46. A telephone company installed a pen register on a suspect's home telephone line at the request of the police. *Id.* at 737. The Court determined that under the third-party doctrine, the pen register did not violate the suspect's Fourth Amendment rights because he "voluntarily conveyed numerical information to the telephone company" and "assumed the risk" that the company would provide that information to the government. *Id*. at 744.

Here, as in *Smith*, Defendant voluntarily conveyed location information to Verizon each time he made a phone call or sent a text message. Verizon recorded the location of the cell tower in order to route Defendant's cell phone calls and messages. By conveying this information, Defendant "exposed" the CSLI to Verizon and "assumed the risk" that the information would be disclosed to the Government. *Id*. For those reasons, the Government's acquisition of Defendant's historical CSLI did not violate the Fourth Amendment.

Several courts have recently held that the government's acquisition of historical CSLI does not violate the Fourth Amendment. *See e.g*., *In re U.S. for Historical Cell Site Data*, 724 F.3d 600, 614 (5th Cir. 2013) (finding that cell phone users voluntarily convey CSLI to service providers through general use of their phones.)

In contrast, the Fourth Circuit held that the government's inspection of historic CSLI violated the Fourth Amendment. *United States v. Graham*, No. 12-4659, 2015 WL 4637931, *21 (4th Cir. 2015). In that case, the Court stated that cell phone users do not "volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person." *Id*. at *16. Cell phone users do not generally know "what cell sites transmit their communications or where those cell sites are located." *Id*. at *17.

Similarly, Respondent argues that much of the information conveyed by his cell phone was not voluntarily conveyed. Respondent states that even if the phone calls or text messages that he sent could be considered "voluntarily conveyed," the incriminating information here was obtained from pieces of information that he did not voluntarily convey such as unsolicited emails or unanswered phone calls. We do not agree with this narrow interpretation of the rule. Cell phone users voluntarily convey CSLI to their service providers when they connect to the provider's network, whether they are making a call or sending an email. Every time the user activates his phone, the cell phone provider must establish a connection with the nearest cell tower. It makes no difference if the user remains ignorant of the technical workings or is unaware of the exact location of the nearest cell tower.

For the foregoing reasons, the judgment of the district court is

REVERSED and REMANDED.

STILES, J., Circuit Judge Dissenting:

I disagree with the majority's holding that the private search doctrine applies to Mr. Tejada's search of Respondent's computer and external hard-drive. Tejada was acting as a government agent when he conducted the search with the intent of discovering evidence relating to illegal firearms and narcotics trafficking. Furthermore, although I agree the third-party doctrine applies to Respondent's historical CSLI records, it only applies to transmissions that he "actively submitted." Therefore, the historical CSLI records should be limited to phone calls and messages he sent, rather than any phone calls or messages he received.

1. THE PRIVATE SEARCH DOCTRINE AND GOVERNMENT AGENTS

Although slight variation among the circuits that have addressed the issue exists, I would adopt the Sixth Circuit's two-part test to determine whether Tejada was a government agent when he conducted the search. In order to show that a person is acting as a government agent, two facts must be shown: 1) "the police instigated, encouraged, or participated in the search," and 2) "the individual must have engaged in the search with the intent of assisting the police in their investigative efforts." *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985).

The Drug Enforcement Agency and the Arcadia Police Department had a year long campaign that saturated the local airwaves and billboards. Tejada testified that he had seen many advertisements on local television channels asking local citizens to become more proactive in their community. Tejada also testified that he had been suspicious of Respondent's behavior for several months and searched the external hard-

drive with the express purpose of confirming those suspicions and providing that information to the Government.

Thus, the Government instigated and encouraged Tejada to conduct the search of the external hard-drive when it guaranteed him $10,000 in return for any information leading to an arrest for illegal gun or narcotics trafficking. Furthermore, Tejada engaged in the search with the intent to assist the DEA and the Arcadia Police Department in their investigation by providing them any information he might find.

2. THE THIRD-PARTY DOCTRINE AND HISTORICAL CSLI RECORDS

The majority relies on *Smith v. Maryland* to establish that the third-party doctrine applies to historic CSLI records. However, the majority's analysis fails to distinguish some of the major differences presented by the historic CSLI records in question.

In *Smith v. Maryland*, the Supreme Court held that a phone call "voluntarily convey[s] numerical information to the telephone company and 'expose[s]' that information to its equipment in the ordinary course of business." *Smith v. Maryland*, 442 U.S. 735, 744 (1979). *Smith* only dealt with "the numbers dialed from the telephone at [a person's] home." *Id.* at 737. The Court in *Smith* did not intend to extend the third-party doctrine to all information that might be *received* by an individual through a cellular network.

Here, Respondent's historic CSLI records were comprised of telephone calls he sent and received, text messages he sent and received, and email communications he sent and received. At least half of the data points correspond to location information collected from unsolicited communications to Respondent's cell phone. Respondent never responded to a significant portion of those unsolicited communications, therefore, there is

no indication that he was aware of their existence. To say that Respondent "voluntarily conveyed" that information to a third-party by virtue of the fact that he agreed to use a cell phone is illogical and bad law.

I respectfully dissent.

SUPREME COURT OF THE UNITED STATES

October Term 2015

———

Docket No. 2015-12

Albert Greene,

Petitioner,

v.

United States of America,

Respondent.

Petition for certiorari is granted. The Court grants cert limited to the following questions:

1. **What is the proper scope of a search under the private search doctrine as it applies to electronic data storage devices?**

2. **Whether the third-party doctrine applies to historic cell site location information records.**

Exhibit A

Excerpt of James Tejada's Suppression Hearing Testimony

DIRECT EXAMINATION

Q. Good morning Sir.

A. Good morning.

Q. Please state and spell your name for the record.

A. James Tejada. T-E-J-A-D-A.

Q. Thank you. Now, do you recall anything about the day of August 10, 2015?

A. Mhmm yeah.

Q. Okay, and what do you recall from that day?

A. I used my roommate's computer in our apartment and saw a bunch of pictures of illegal stuff.

Q. Let's back up a bit. First of all, who is your roommate?

A. Albert Greene.

Q. And why were you using Mr. Greene's computer?

A. Well, I didn't have one and I needed to check on some of my emails.

Q. Was Mr. Greene aware that you were using his computer that day?

A. No. Al was outta town for the weekend. I mean, yeah, I thought about asking him, but I noticed the door to his room was unlocked. I figured it would

be cool to just go in because I just needed to use it for a second to check my emails.

Q. What, if anything, did you see when you logged on to his computer to check your email?

A. Well…First I checked my email. But then after a few minutes, I decided to browse around on his computer. I saw he'd just bought an external hard-drive for his computer and so I was kinda curious about why he needed so much extra storage so I…

Q. Let me stop you right there. Can you please describe the external hard-drive that you were just referencing?

A. Yeah its just a small black box that sits on top of the computer desk. I think it has a wireless connection or something to the computer. It could hold like 2 terabytes of data.

Q. Were you able to access anything on that external hard-drive?

A. Yes.

Q. How were you able to do that?

A. There was a file folder on the desktop that I clicked on. It just opened the external hard-drive folder from there.

Q. What, if anything, did you specifically see in that folder?

A. There was a folder labeled “photos.” I clicked on that one and then a whole bunch of pictures popped up. I couldn't really tell what the photos were at first, but after I scrolled through a few of them, I realized some photos were showing some type of drugs and then other photos showed those drugs inside cars in little hidden compartments.

Q. What did you do next?

A. I immediately shut off the computer. I always suspected that Al might be up to something sketchy, but I didn’t know it was so serious. That day, I called the Arcadia Police and told them what I saw. Then, a few hours later, Agent Smith showed up at my door.

Q. What exactly did you tell Agent Smith about the photos?

A. I said that I saw some drug photos.

Q. Okay, then what happened when Agent Smith arrived? Did you show him the photos?

A. Yes. I took Agent Smith into Al’s room where the computer was. I opened the photos folder and

started scrolling through the photos I had seen. At some point, I saw a some photos with guns too. Agent Smith asked me why I didn't mention those photos and I told him that I didn't notice them the first time.

Q. No further questions.

CROSS EXAMINATION

Q. Mr. Tejada, at the time you used Mr. Greene's computer, you were familiar with the "If you see something, say something!" Crime Stopper campaign advertised on local television in Arcadia, weren't you?

A. Uh… Yes. I've seen the commercials and advertisements at the bus station.

Q. And you were aware that there was a $10,000 reward for any information leading to the arrest of anyone dealing in illegal narcotics or firearms, correct?

A. Yes…

Q. In fact, that is the real reason you were using Mr. Greene's computer, right?

A. Well.. no… I mean, I was using his computer to check my email…I guess the thought had crossed my mind. I was curious…Al had been doing some odd things

for a while. He always had a lot of cash on him. He never really had a steady job. He always left at weird times during the night. I'll admit, I was kinda suspicious of his behavior. The commercials on TV really make you want to fight crime… I mean, I felt like I was doing my civic duty. I didn't really think I would find anything, but once I did, I knew I had to call the police. These pictures were exactly the type of evidence…I mean information that the police department was looking for to stop these illegal trafficking operations.

Q. Nothing further.

Exhibit B

Excerpt of Aaron Smith's Suppression Hearing Testimony

DIRECT EXAMINATION

Q. Good morning Agent.

A. Mornin’.

Q. Please state your name for the record.

A. Aaron Smith.

Q. What do you do for a living?

A. I am Federal Agent with the Drug Enforcement Agency.

Q. What is your assignment?

A. I am currently assigned to the Southwest District of Arcadia. I primarily conduct my work in the city limits of Arcadia.

Q. Were you working on August 10, 2015?

A. Yes.

Q. Do you recall the events that took place that day?

A. Yes. I received information from an individual named James Tejada. He contacted our office to report some photographs he had seen on a roommate’s computer. He spoke with the dispatch operator.

Q. What did you do next?

A. I asked him to provide me the location of his residence. He told me his address and I let him know I would be coming by later that afternoon to investigate

the photos.

Q. Did he tell you how many pictures he saw?

A. I don't really remember. I think he said something like 3 or 4 photographs.

Q. Were these photos concerning to you?

A. Yes. I have been specially assigned to the southern district of Arcadia to investigate narcotics and firearm trafficking in the region. Arcadia is near an international border and has been targeted for illegal trafficking in recent years.

Q. Did you follow-up on the report?

A. Yes. I went to Mr. Tejada's residence that afternoon and had him show me the images.

Q. What happened when you arrived?

A. Mr. Tejada let me in the front door of his apartment. I asked him to show me where the computer was located. He brought me into one of the bedrooms.

Q. Did Mr. Tejada tell you who the computer belonged to?

A. Yes. He told me his roommate, Albert Greene, lived in the apartment with him. He also told me that Mr. Greene was out of town for the weekend and did not know that he was using his computer.

Q. What did you do next?

A. I prompted Tejada to show me the images that he had viewed earlier that day. Tejada logged in to the computer and clicked on a general file on the desktop labeled "photos." When he clicked on the folder, it opened a photo browsing application. The first image depicted a substance, which I believe, based on my training and experience to be methamphetamine. It was covered in plastic wrap and placed in a compartment of a vehicle. Tejada continued to scroll through the images. The next three images were very similar to the first one. Tejada continued on to the next photograph, which contained an individual holding two firearms. Tejada told me that the individual in those photos was his roommate, Albert Greene. Tejada scrolled through two more photos.

Q. What did you do next?

A. I collected the external hard-drive that the photos were stored on and went back to my headquarters. Based on the photos, I suspected that Mr. Greene might be involved in an illegal trafficking operation.

Q. Did you continue to investigate the matter?

A. Yes. I conducted a records search for Albert Greene and was able to find his personal cell phone number. With that information and the photos from the hard-drive, we applied for and obtained an order compelling Verizon Wireless, Inc. to hand over the Cell Site Location Information records for Mr. Greene's cell phone.

Q. What did that information reveal?

A. The CSLI showed that Mr. Greene used his cell phone in two areas…at or near his residence and in a rural area about 17 miles or so east of downtown Arcadia.

Q. Why was that significant?

A. Generally, in my experience, these trafficking operations take place in rural areas. Also, the phone records showed a significant amount of use during nighttime hours. This is also consistent with an illegal trafficking operation because the operators traditionally conduct their business at that time.

Q. What did you do next?

A. Well… I am familiar with the area. There is

really only one road out in that area. When I looked at the CSLI, the only cell tower in that area was near that road. The next day, I drove to that general location and observed a fairly large warehouse building about 3.5 miles of the main road. I believed that this was the location Mr. Greene had been using his cell phone.

Q. What did you do next?

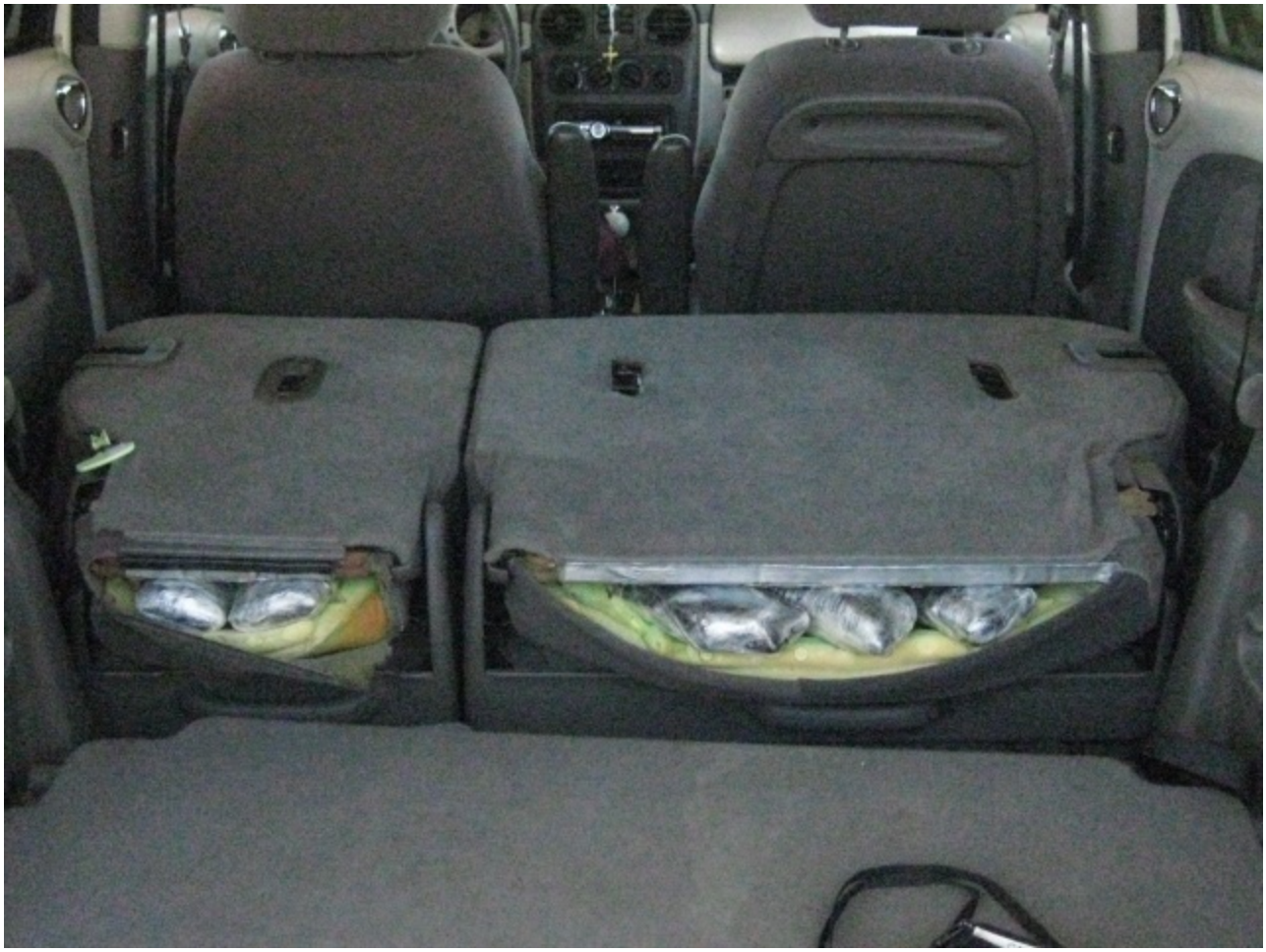
A. I conducted surveillance on the area over the course of several days. I saw Defendant traveling to and from the warehouse on multiple occasions. Every time Defendant went to the warehouse, it was basically in the middle of the night. Also, I saw quite a few unmarked moving vans entering and leaving the warehouse during the nighttime hours. All of the vans were normally parked out front of the warehouse during the day. Based on all of that information, I applied for and obtained a search warrant for the warehouse.

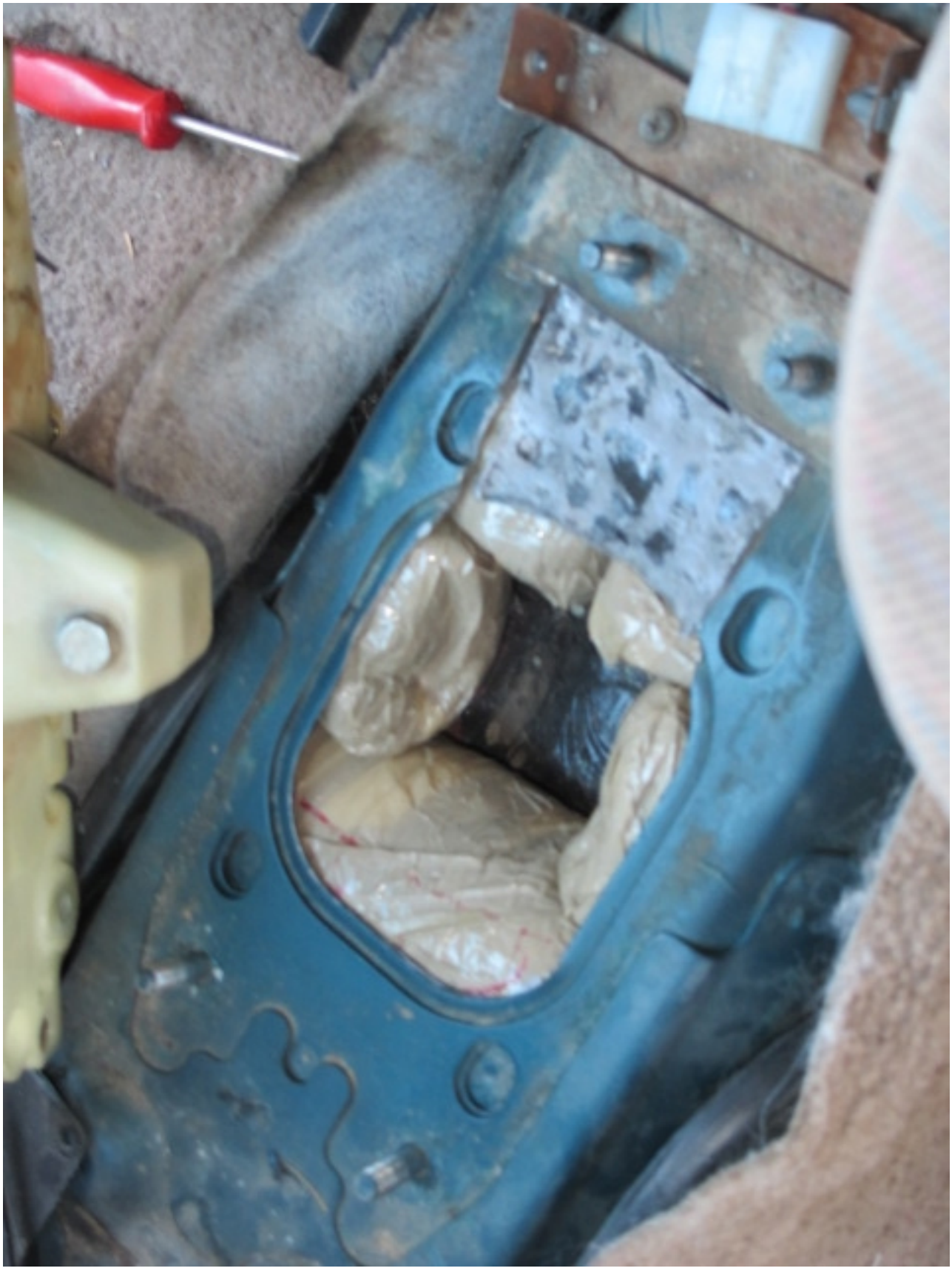
Q. What did you find during the search?

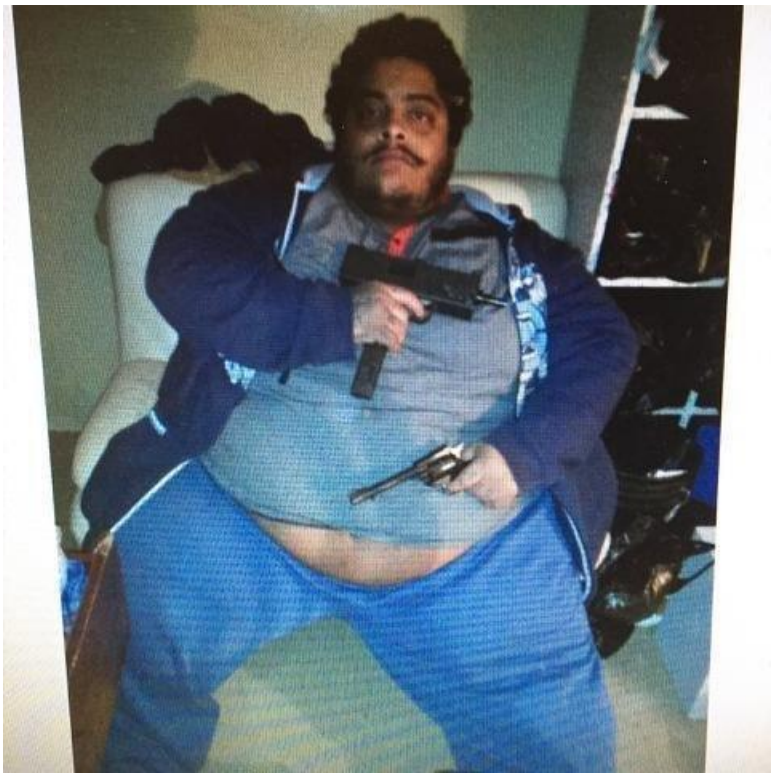
A. Guns and drugs. A lot of guns and drugs. Over 1,000 kilograms of methamphetamine and 200 illegal weapons ranging from automatic machine guns to rocket launchers.

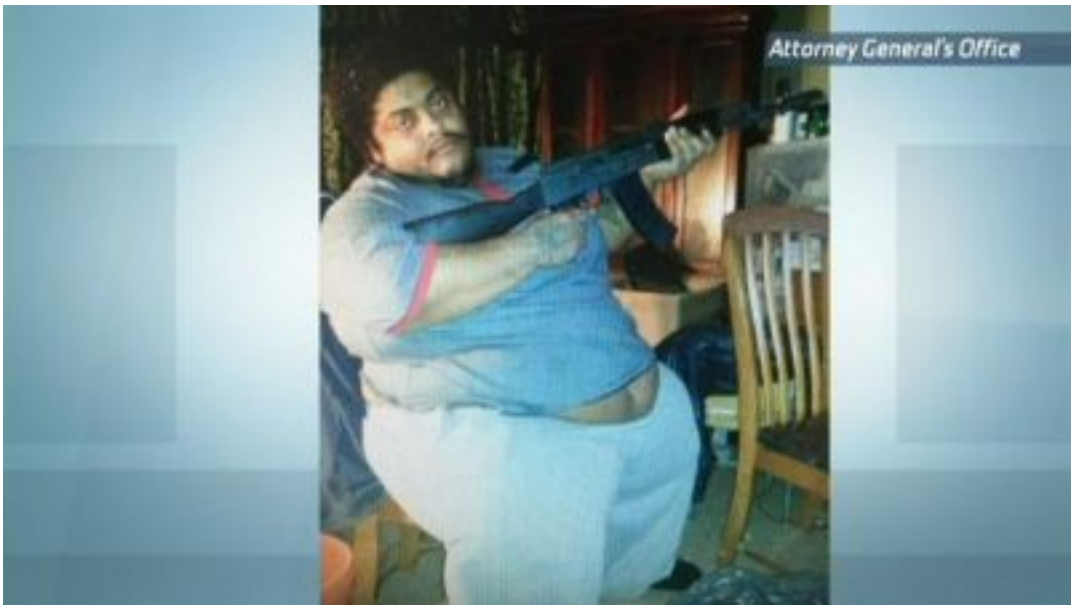
Exhibit C

Photographs Contained on External Hard-drive








Attorney General's Office

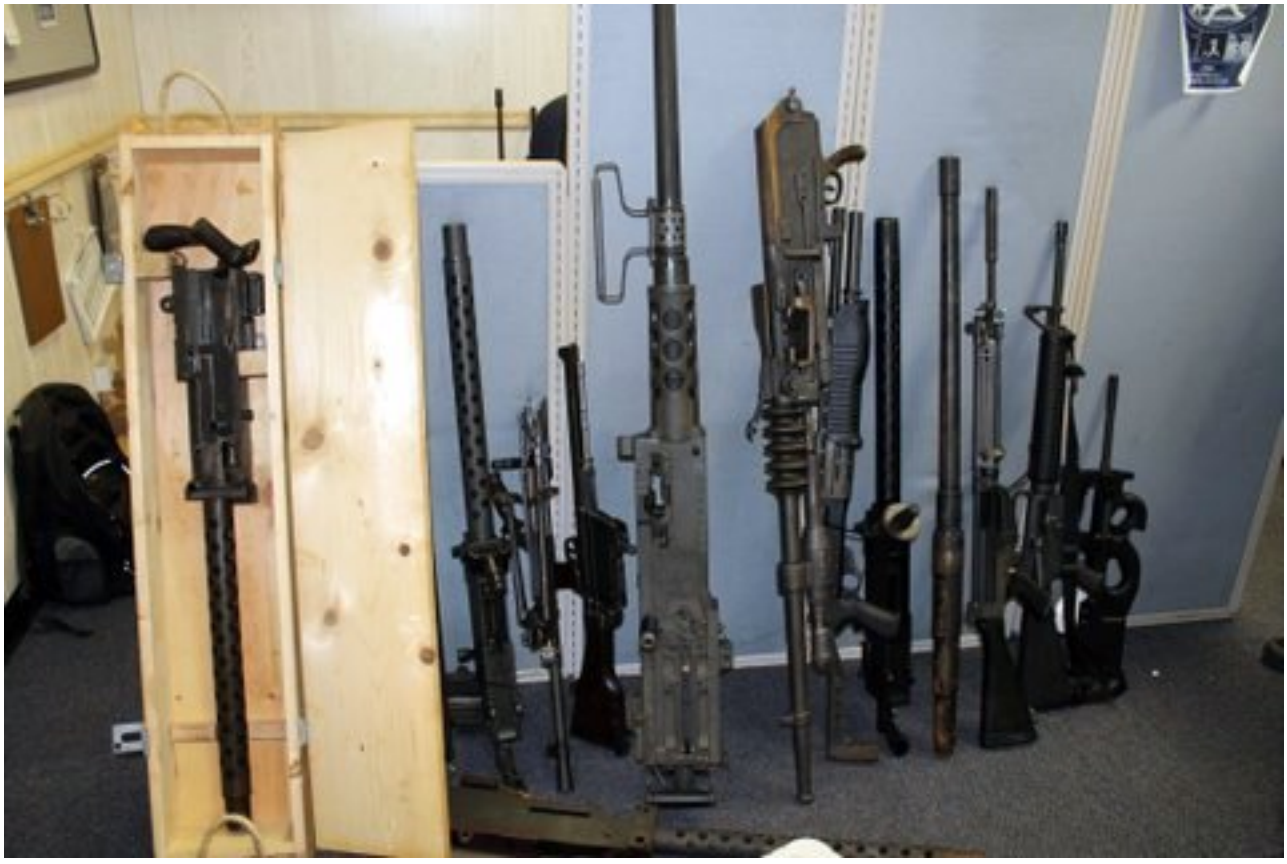
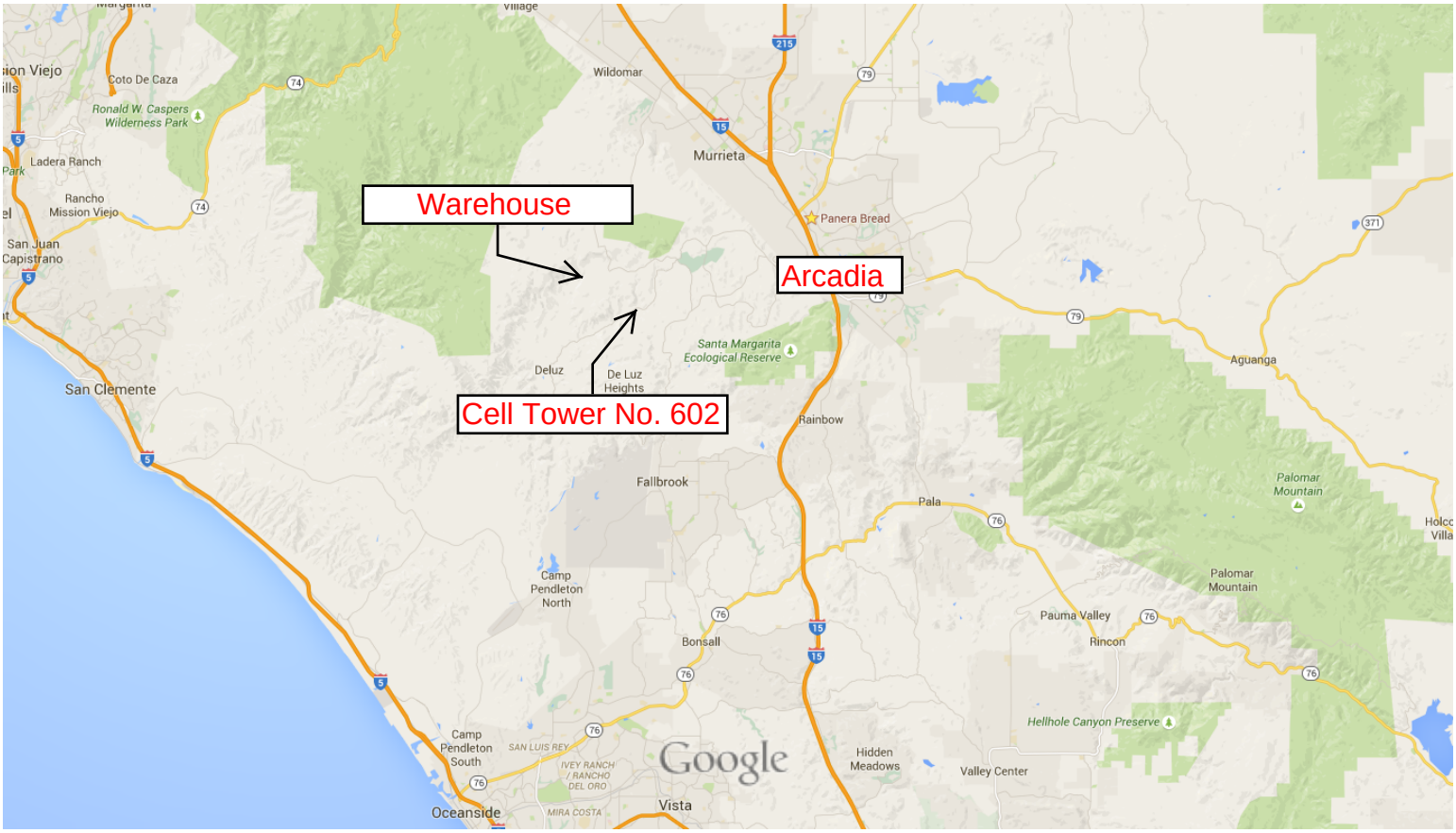


Exhibit D

Map of Arcadia

Google Maps



Map data ©2015 Google 2 mi

Exhibit E

CSLI Application and Order

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ARCADIA

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	))))))	MISC. NO. 1653 **Filed Under Seal**

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703 (d)

SUSAN JOHNSON, an Assistant United States Attorney for the Southern District of Arcadia, hereby files under seal this ex parte application for an order pursuant to 18 U.S.C. § 2703(d) to require VERIZON WIRELESS, INC., a telecommunications company located in the Southern District of Arcadia, which functions as cellular service provider to provide records. The records and other information requested are set forth as an Attachment to the Application and to the proposed Order. In support of this Application, the United States asserts:

LEGAL AND FACTUAL BACKGROUND

1. The United States Government, including the Drug Enforcement Agency, are investigating an individual named ALBERT GREENE for his involvement in an illegal firearms and narcotics trafficking operation taking place within the Southern District of Arcadia.

2. Investigation to date of these incidents provides reasonable grounds to believe that VERIZON WIRELESS, INC, has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation. Because VERIZON WIRELESS, INC. functions as an electronic communications service provider (provides its subscribers access to electronic communication services, including e-mail and the Internet), 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information it is seeking.

3. Here, the government seeks to obtain subscriber ALBERT GREENE's historic cell site location information for a period of 205 days (January 8, 2015 through August 1, 2015).

4. A subpoena allows the government to obtain subscriber name, address, length and type of service, connection and session records, telephone or instrument number including any temporarily assigned network address, and means and source of payment information. 18 U.S.C. § 2703(c)(2). The government may also compel such

information through an order issued pursuant to 18 U.S.C. § 2703(d). 18 U.S.C. §§ 2703(c)(1)(B), (c)(2).

5. To obtain records and other information pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with 18 U.S.C. § 2703(c)(1), which provides, in pertinent part:

> 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- . . .
> (B) obtains a court order for such disclosure under subsection (d) of this section.

6. Section 2703(d), in turn, provides in pertinent part:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction (fn2) 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. . . . 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.

Accordingly, this application sets forth the specific and articulable facts showing that there are reasonable grounds to believe that the materials sought are relevant and material to the ongoing criminal investigation.

THE RELEVANT FACTS

7. On August 10, 2015, JAMES TEJADA accessed a personal desktop computer owned by ALBERT GREENE. TEJADA and GREENE were co-residents in a two-bedroom apartment located in downtown Arcadia. TEJADA entered GREENE's room and logged on to his computer to check his personal email. TEJADA located a file on an external hard-drive labeled "photos." TEJADA opened the "photos" file and immediately viewed several photographs depicting large amounts of what he believed to be illegal drugs concealed in compartments of various automobiles.

8. TEJADA reported his observations to DEA Agent AARON SMITH. Agent SMITH conducted a follow-up investigation later that afternoon, wherein, he discovered several more photographs on the hard-drive. The additional images depicted

GREENE possessing illegal firearms consistent with firearms trafficking. TEJADA told Agent SMITH that he suspected GREENE might be involved in some sort of illegal activity based on his behavior. GREENE would leave his apartment in the middle of the night and appeared to have large quantities of cash on hand regularly.

9. Arcadia has been a focal target area for illegal firearm and drug trafficking operations. As a result, local gangs claimed territories within the city, causing violent crime and homicide rates to skyrocket in the six months preceding the incident in question.

10. The conduct described above provides reasonable grounds to believe that a number of federal statutes may have been violated.

11. Records of customer and subscriber information relating to ALBERT GREENE that are available from VERIZON WIRELESS, INC., will help government investigators identify the the location(s) of the illegal trafficking operations GREENE is associated with. Accordingly, the government requests that VERIZON WIRELESS INC. be directed to produce all records described in Attachment A to this Application.

WHEREFORE, it is respectfully requested that the Court grant the attached Order.

Executed on August 23, 2015

SUSAN JOHNSON
Assistant United States Attorney

ATTACHMENT A

You are to provide the following information as printouts and as ASCII data files, if available:

A. The cell site location information for any accounts registered to ALBERT GREENE for a period of 205 days (January 8, 2015 through August 1, 2015).

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ARCADIA

IN RE APPLICATION OF THE	)	
UNITED STATES OF AMERICA FOR	)	MISC. NO. 1653
AN ORDER PURSUANT TO	)	
18 U.S.C. § 2703(d)	)	**Filed Under Seal**

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703(b) and (c), which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing VERIZON WIRELESS, INC., an electronic communications service provider located in the Southern District of Arcadia, to disclose certain records and other information, as set forth in Attachment A to the Application, the court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that VERIZON WIRELESS, INC. will, within three days of the date of this Order, turn over to agents of the Drug Enforcement Agency the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this Application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that VERIZON WIRELESS, INC., shall not disclose the existence of the Application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

TIMOTHY J. THOMAS
United States Magistrate Judge

August 23, 2015