TEXAS CRIMINAL DEFENSE LAWYERS ASSOCIATION

Texas Criminal Defense Lawyers Association

30th Annual Rusty Duncan Advanced Criminal Law Course

June 22-24, 2017
Hyatt Regency
San Antonio, Texas

Warrantless Data Searches: Giving the Government Your Most Private Information

Speaker: Donald H. Flanary, III.
FLANARY LAW FIRM, PLLC.

Authors: Donald H. Flanary, III.
Amanda I. Hernandez
FLANARY LAW FIRM, PLLC
1005 S. Alamo St.
San Antonio, TX 78210
210.738.8383 phone
210.738.9426 fax
Don@flanarylawfirm.com
Amanda@flanarylawfirm.com
www.flanarylawfirm.com

Table of Contents

I. INTRODUCTION:

In today's society, we are used to having almost anything we want available to us in an instant. Mobile phones have become a necessary part of our everyday lives and are basically hand-held computers that enable us access the internet and communicate effortlessly. Smartphones, like IPhones and Androids, are by far the most popular versions and enable users to download countless applications (apps). In addition to allowing us to communicate with others via calls and texts, our cell phones can track where we've been and where we're going with GPS and location data. They can tell a driver to come pick us up from our home or current location with ridesharing apps, have food delivered to our door with delivery apps, play our favorite songs, and help us browse or find anything online within a matter of seconds. What we seem to forget, however, is how much detailed and personal information can be learned from accessing our phone's data. Our cell phone data can document not only our most intimate conversations, but our historical and present location, browsing history, internet habits, contact information, emails, and other private information. Even more importantly, this information can be shared with law enforcement without your consent or even knowledge under certain circumstances. This is still an issue when warrants are involved, but the problem is amplified to the highest degree when this information is being gathered and shared with the government without probable cause and, in some situations, inadvertently with no evidence of any criminal wrongdoing whatsoever.

This paper will give a basic idea of some the privacy challenges courts are facing when information is gathered by law enforcement without first securing a warrant and give you an idea of how to handle them. The paper starts with an overview of the two Supreme Court landmark cases- *United States v. Jones,* dealing with warrantless GPS tracking, and *Riley v. California,*

which dealt with warrantless cell phone searches. Following those is a summary of a case from the Texas Court of Criminal Appeals dealing with same. The basics of cell phone technology and cell site location information (CSLI) are discussed next, followed by some of the basic aspects of the Stored Communications Act (SCA) & the Third Party Doctrine. Their application to Texas and Appellate CLSI cases are then discussed. The paper then provides information about new technology now being deployed by law enforcement to not only gather information, but track suspects down. Next, two recent cases that dealt with applying the Fourth Amendment to the use of these devices are discussed. The paper touches on the privacy interests in internent protocol (IP) addresses, and notes two new bills that are before Congress that are being pushed by privacy advocates. Lastly, information on FISA 702, the government's favorite information seeker, and information on a new law signed by President Trump that takes away many internet protections.

II. THE FIRST LANDMARK GPS CASE
United States v. Jones, 132 S. Ct. 945 (2012)

It's no secret that law enforcement agents engaged in covert surveillance commonly use electronic tracking devices, or "beepers," to gather information on suspects. In applying the Fourth Amendment to these types of cases, courts have typically distinguished the device's installation from its monitoring. Thus, although the majority of published decisions address both installation and monitoring, the case law that has emerged in recent years does not resolve both issues identically.

In 2012, the Supreme Court unanimously decided a case that can be said to be one of the most important Fourth Amendment opinions since *Katz*[1]. The case, *United States v. Jones*, 565 U.S. 400 (2012), posed the question of whether the warrantless use of a tracking device on the respondent's vehicle to monitor its movements on public streets violated Jones's Fourth Amendment rights. *Id.* at 402. The majority opinion, authored by the late Justice Scalia, held that the installation of a GPS tracking device on the respondent's vehicle, without a warrant, and the subsequent use of that device to monitor the vehicle's movements on public streets constituted an unlawful search under the Fourth Amendment. *Id.* at 404.

Scalia argued that the government's physical intrusion on the defendant's car (a personal "effect") would clearly be a search within the original meaning of the Fourth Amendment, which was traditionally concerned with government trespass on private property for the purpose of a criminal investigation. *Id.* at 406. He added that the protections afforded by the Fourth Amendment "do not rise or fall with the *Katz* formulation" and that we must assure we protect basic privacy against the government as we did when the Fourth Amendment was adopted. *Id.* The majority also distinguished the *Jones* case from the *Knotts* and *Karo* beeper cases, arguing that in those cases, the electronic devices were not placed on property already possessed by the defendant so only the *Katz* test was applicable. *Id.* at 409-10. The *Jones* opinion stressed that in this case, the police physically encroached on a protected area to gather information. *Id.*

Joined by Justices Ginsburg, Breyer and Kagan, Justice Alito wrote a concurring opinion disagreeing with the majority's trespass-based reasoning and argued that the real question in the

[1] In *Katz v. United States,* 389 US 347 (1967), the Supreme Court held that Katz was entitled to Fourth Amendment protection for his conversations and that a physical intrusion into the area he occupied was unnecessary to bring the Amendment into play. The Court further established a Two-pronged privacy test used to decide whether government action is a search: (1) The subjective prong, whether the defendant had an actual expectation of privacy in the area searched; and (2) The objective prong, whether or not the expectation of privacy was reasonable (an expectation that society's prepared to recognize).

case was whether the long-term monitoring of the movement of respondent's vehicle violated his reasonable expectations of privacy. *Id.* at 419. Alito agrees that traditional privacy protections must be afforded, but noted that it is "almost impossible" to analogize the *Jones* case with those of the late 18th century. *Id.* at 420. Alito wrote:

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken…Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.

Id. at 429. Alito's argument is essentially that any technical trespass that results in the gathering of evidence amounts to search, and that the *Katz* standard should have controlled the case. He concludes by asserting while relatively short-term monitoring of an individual's movements on public streets may be reasonable, "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 430.

Justice Sotomayor also wrote a concurring opinion but expressed concern that with newer technology and modes of surveillance that do not require a physical invasion on property, the majority's opinion and trespassory test provides little guidance for future cases. *Id.* at 415. She agreed with Scalia that *Katz* supplemented rather than substituted the common-law trespassory test for whether a search has occurred for Fourth Amendment purposes, but also agreed with Alito that most long-term GPS monitoring would violate *Katz*. Notably, she also took the position that even short-term monitoring may violate an individual's reasonable expectation of privacy because of the unique nature of GPS surveillance. *Id.*

The *Jones* court stopped after ruling that the GPS tracking was a Fourth Amendment search, and made no mention about what conditions would make such a search constitutional under the Fourth Amendment nor did they set forth a presumptive warrant requirement for such

GPS searches. Because of this, substantial uncertainty continues to exist as to the conditions under which warrantless GPS searches are constitutional.

III. "DATA IS DIFFERENT"

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

In *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court was faced with the question of whether law enforcement may, without a warrant, search a cell phone for digital information after it seized from an individual who has been arrested. *Id.* at 2480. Chief Justice Roberts wrote the opinion of the unanimous Court and held that a warrant is generally required before searching a cell phone, even when it is seized incident to arrest. *Id.* at 2493.

In so holding, Chief Justice Roberts stressed the fact that privacy concerns in regards modern cell phones are generally much higher than those implicated by the searching of a cigarette pack, a wallet, or a purse. *Id* at 2488-89. He wrote:

> "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."

Id. at 2489.

In addition to being quantitatively different, the *Riley* opinion made it clear that cell phone data can also be qualitatively different from traditional physical records. The Court explained that searching this type of data can reveal significant and intimate details about a person's life, from possible diseases or addictions to GPS monitoring of previous locations. Chief Justice Roberts even went as far as saying that searching a cell phone can typically expose to the government "far more than the most exhaustive search of a house." *Id.* at 2491. Justice Alito wrote separately, concurring in part and concurring in the judgement, but expressed doubt

that the search incident to arrest exception exists for primary purposes of protecting officer safety and preserving evidence. *Id.* at 2495. Justice Alito recognized the heightened privacy interests in cell phone technology, and suggested that legislatures should be the ones to answer the question of what information law enforcement may reasonably search for within a phone incident to arrest. *Id.* at 2497-98.

B. *State v. Granville*, 423 S.W.3d 399 (Tex. Crim. App. 2014)

The Court of Criminal Appeals addressed a similar question in *State v. Granville,* after an officer, who took no part in the arrest, searched a cell phone for evidence pertaining to an allegation unrelated to the crime for which the defendant was arrested. *State v. Granville*, 423 S.W. 3d 399 (Tex. Crim. App. 2014). The Court abruptly stated, "we reject [the State's] argument that a modern-day cell phone is like a pair of pants or a bag of groceries, for which a person loses all privacy protection once it is checked into a jail property room." *Id.* at 402. The Court went on to note that "[a] cell phone is unlike other containers as it can receive, store, and transmit an almost unlimited amount of private information." *Id.* at 408. Further, "[t]he potential for invasion of privacy, identify theft, or at a minimum, public embarrassment is enormous." *Id.* at 408–09. "Searching a person's cell phone is like searching his home desk, computer, bank vault, and medicine cabinet all at once. There is no doubt that the Fourth Amendment protects the subjective and reasonable privacy interest of citizens in their homes and in their personal 'papers and effects.'" *Id*. at 415. The *Granville* Court held that citizens do not lose their "expectation of privacy in the contents of [their] cell phone merely because [they have] been arrested and [their] cell phone is in the custody of police for safekeeping." *Id*. at 404. The majority opinion closed by stating, the officer "could have seized appellant's phone and held it while he sought a search warrant, but, **even with probable cause**, he could not 'activate and

search the contents of an inventoried cellular phone' without one." *Id*. at 417 (emphasis supplied).

IV. THE BASICS OF CELL PHONES & LOCATION DATA

In the most basic form, cell phones work like walkie-talkies. When you use your phone to call someone, your phone first converts your voice into an electrical signal and then transmits it via radio waves to the nearest cellular base station or "cell site". Wireless carriers use a network of these towers to relay the wave to the other person's phone, which converts it to an electrical signal and then back to sound again. In order to properly work, this two-way communication device requires the inbound signal (reception) and the outbound signal (transmission). The signal strength on your phone, usually represented by bars, indicates the magnitude of the of the received signal from the cell site. The regular communication between phone and cell sites enables the carrier not only to route calls, but to route text messages and internet data to and from the mobile phone. In order to keep this constant communication, mobile phones regularly register themselves with the nearest cell site so that the network can connect the mobile phone to incoming calls and text messages. In addition to using your mobile phone to make a call, send a text, or use the internet, your phone's process of continuously registering to the nearest cell site automatically generates location data that can be traced back to your device. This data, commonly known as cell site location information (CSLI), has been the subject of controversy in recent years, and its precision can be said to have varying degrees.[2] Law enforcement agencies have the power to compel network providers to disclose this location data, regardless of whether it was automatically generated by the wireless carrier in the normal course of business or

[2] See Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 Berkeley Tech. L.J. 117, 126 (2012).

specifically created in response to a "ping," or surveillance request from law enforcement. This "carrier-assisted surveillance" can reveal intimate details about the mobile phone user's life, including real-time location tracking, a list of numbers dialed, the addresses of web pages viewed, and other types of data.[3]

V. The Basics of the Stored Communications Act (SCA) & The Third Party Doctrine

In 1986, the Stored Communications Act (SCA) was enacted. Pub. L. No. 99-508, 100 Stat. 1860 (codified as amended at 18 U.S.C. §§ 2701–2712 (2012)). The SCA allowed for the collection of basic subscriber information, such as their name, address, phone number, and payment information. While the government was certainly aware of the possibility of location data collection, the congressional intent in 1986 was to "provide a reasonable level of Federal privacy protection" in a world with rapidly-evolving technology in hopes of spurring "continued innovation" and building "customer confidence." 132 CONG. REC. 14,600 (1986) (statement of Sen. Patrick Leahy); *Id.* at 14,609 (statement of Sen. Charles Mathias Jr.).

Another factor silencing the call for location data was the lack of reliability due to the few cell sites in existence. OFFICE OF TECH. ASSESSMENT, U.S. CONG., ELEC. SURVEILLANCE & CIVIL LIBERTIES 39 (1985). But the government was well aware that as cell phones became "more popular, cell sizes [would] be reduced allowing more precise tracking." *Id.* This proved true, as today's CSLI can be more accurate than global positioning systems (GPS) data—depending on various factors, such as the number of cell sites in the vicinity, and how advanced the cell site technology. *See* Susan Freiwald, *Cell Phone Location*

[3] Stephanie K. Pell & Christopher Soghoian, *A Lot More Than A Pen Register, and Less Than A Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities* (Fn2), 16 Yale J.L. & Tech. 134, 145 (2014)

Data and the Fourth Amendment: A Question of Law, Not Fact, 70 MD. L. REV. 681, 712 (2011) (acknowledging that when multiple sources are available for triangulation, the location area could be significantly reduced achieving GPS-like accuracy); *see also ECPA Reform & the Revolution in Location Based Techs. & Servs.: Hearing Before the Subcomm. on the Const., Civil Rights, & Civil Liberties of the H. Comm. of the Judiciary*, 111th Cong. 29–30 (2010) (attributing advancement in cell site technology as one reason for GPS being comparable to cell site data) (prepared statement of Matt Blaze, Professor, Univ. of Pa.); *Id.* at 40–41 (noting GPS could be less reliable than cell site data because satellite signals are affected when the cell phone is indoors) (statement of Michael Amarosa, Vice President, TruePosition, Inc.).

A. The Current SCA

In its current form, the SCA states "[a] provider of electronic communication service . . . shall disclose to a governmental entity the . . . local and long distance telephone connection records . . . of a subscriber to or customer of such service . . . [with a] court order . . . [issued upon] specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . or the records or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. §§ 2703(c)–(d) (2012).

A court order meeting the "specific and articulable facts" standard under the SCA is referred to as a 2703(d) order. 2703(d) states:

> **(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.A. § 2703 (West) (emphasis supplied).

2703(d) orders have a lower threshold than a warrant based upon probable cause. *See In re U.S. for Historical Cell Cite Data*, 724 F.3d 600, 606 (5th Cir. 2013) ("The 'specific and articulable facts' standard is a lesser showing than the probable cause standard that is required by the Fourth Amendment to obtain a warrant."); *In re Order Directing a Provider of Elec. Commc'n Serv*., 620 F.3d 304, 313 (3d Cir. 2010) (noting the standard required for a 2703(d) order "is a lesser one than probable cause"). For this reason, 2703(d) orders are the preferred choice for federal investigators. *See* ELEC. SURVEILLANCE UNIT, U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 44–45 (2005), http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf (advising "2703(d) orders are an appropriate tool to compel a provider" to disclose CSLI).

The scope and amount of information law enforcement could seek under the SCA has dramatically expanded since original enactment. *See* The Elec. Commc'ns Privacy Act: Promoting Sec. & Protecting Privacy in the Digital Age: Hearing Before the S. Comm. of the Judiciary, 111th Cong. 16 (2010) (Statement of James Dempsey, Vice President, Ctr. for Democracy & Tech.) (noting the SCA has been amended eighteen times since 1986; all at the request of the Department of Justice). The most damaging amendment, in terms of privacy interests, was in 2001.

The SCA was significantly impacted by the quick enactment of the sweeping Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). Pub. L. No. 107-56, 115 Stat. 272 (2001). With this amendment, the SCA allowed for law enforcement access to "connection records." 18

U.S.C. § 2703(c)(2)(c). The original purpose of only permitting law enforcement access to basic subscriber information was officially extinct.

B. The SCA Fails to Define "Connection Records"

Surprisingly, there are no direct references to CSLI records in the text of the SCA. There is a close alternative in the 2001 addition of "connection records," but Congress never defines this category. Today, there is no legislative history or discussion for a court to turn to understand its textual meaning of these words. "The legislative history does not comment on the intent of this change nor did this topic arise in any of the negotiations surrounding the passage of the Act."[4] Regardless, the DOJ believes CSLI records are included and accessible through the SCA.[5]

It is unclear whether the Justice Department sought CSLI under the SCA prior to the 2001 amendment, and the constitutionality of obtaining CSLI with a 2703(d) order was not addressed by a until 2005. *See generally In re U.S.,* 384 F.Supp.2d 562 (E.D.N.Y. 2005) (considering a 2703(d) application to obtain historical cell site data as one of first impression). Additionally, it would be five more years before this process reached an appellate court. *See In re Order Directing a Provider of Elec. Commc'n Serv.*, 620 F.3d 304, 306 (3d Cir. 2010) (noting this task "has not been performed by any other court of appeals"). While it remains probable that the Justice Department has utilized this process for more than a decade, they are only now being scrutinized.

---

[4] Elect. Surveillance Unit, US. Dep't of Justice, Electronic Surveillance Manual: Procedures and Case Law Forms 49 (2005), http: //www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

[5] Computer Crime & Intellectual Prop., Section, U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 160 (3d ed.2009), http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf ("In most districts, investigators may obtain [CSLI] through [2703(d) orders].")

While the DOJ seems complacent with its interpretation of the SCA, judges are forced to resolve issues without any statutory guidance or legislative history defining the meaning of connection records and whether CSLI is included. Even if they do, should law enforcement be required to obtain a warrant? Unfortunately, courts can avoid this discussion altogether by classifying CSLI as a business record and therefore allowing a broad reclassification of the issue as to whether business records can be accessed without a warrant. Additionally, the government repeatedly argues that subscribes do not have a privacy interest in a service provider's business records, citing the Third-Party Doctrine.

C. The Basics of the Third Party Doctrine

By using the Third-Party Doctrine, the government suggests individuals do not have a reasonable expectation of privacy in their CSLI records, because the subscriber voluntarily conveys location information to the service provider. The Third-Party Doctrine was recognized by the Supreme Court over forty years ago; first in *United States v. Miller*, 425 U.S. 435 (1976) and then in *Smith v. Maryland*. 442 U.S. 735 (1979).

i. *United States v. Miller,* 425 U.S. 435 (1976)

The 1976 *Miller* decision originated from an investigation into a warehouse fire where police discovered "175-gallons of nontax-whiskey." *Miller*, 425 U.S. 437. The investigation revealed Miller may have committed other crimes, to include tax fraud. *Id.* at 436. Through the course of the investigation, law enforcement obtained Miller's bank transaction records with defective subpoenas. *Id.* at 436–37. The Court held Miller did not have a reasonable expectation of privacy in the bank records, because the documents "contain[ed] only information [he] voluntarily conveyed" to the banks. *Id*. at 442. The Court applied this same standard to telephone numbers three years later.

ii. *Smith v. Maryland*, 442 U.S. 735 (1979)

In 1979, the Court in *Smith* considered for the first time whether the use of a pen register without a warrant amounted to a Fourth Amendment search. *Smith*, 442 U.S. 736–37. The Court held Smith did not have any "actual expectation of privacy in the phone numbers he dialed, and even if he did, his expectation was not 'legitimate.'" *Id*. at 745. Society could not recognize Smith's expectation of privacy as reasonable, because in 1979, "[a]ll telephone users realize[d] that they must 'convey' phone numbers to the telephone company." *Id*. As in Miller, the Court considered the information (dialing of a number) to be voluntary conveyed to a third party (phone company), thus waiving any reasonable expectation of privacy. *Id.* at 744.

VI. CSLI CASES IN TEXAS & FEDERAL COURTS OF APPEAL

Numerous Texas and Federal Courts of Appeal have faced and continue to face the issue of whether the Fourth Amendment requires a warrant based upon probable cause before the government can acquire a subscriber's CSLI from a network provider. The following cases are summarized because they are the most recent. The first are 5th Cirucit precedent cases that relate to CSLI and a warrantless cell phone search at the border. The following are other recent important appellate decisions regarding same. Lastly, a case from the Texas Court of Criminal Appeals is discussed.

A. No Probable Cause Required - *In re Application of the U.S.A. for Historical Cell Site Data* (5th Circuit 2013)

The 5th Circuit has not meaningfully addressed CSLI issues since they decided *In re Application of the USA for Historical Cell Site Data,* 724 F.3d 600 (5th Cir. 2013), and upheld the government's ability to obtain CSLI without a finding of probable cause. There, the court was faced with the issue of whether the Stored Communications Act (SCA) violated the Fourth

Amendment with its policy of allowing the government to obtain court orders compelling mobile phone service providers to release subscribers' historical CSLI without a showing of probable cause. *Id.* at 602.

The government in that case sought orders for sixty days of cell site data from cell phone network providers under the SCA for three separate investigations. *Id.* The U.S. District Court for the Southern District of Texas denied the applications, holding that the Fourth Amendment was violated because there was no finding of probable cause. On appeal, the 5th Circuit vacated the district court's decision and remanded it back to the trial court, instructing them to grant the government's applications. The Court reasoned that cell site data are maintained by the providers as "**business records**," and that users voluntarily use their phone, **knowing** that they convey information about their location to their networks when making calls. *Id.* at 613. Thus, the court concluded, no showing of probable cause, as is usually required for a search warrant, is necessary.

The Court wrote:

> "Cell site data are business records and should be analyzed under that line of Supreme Court precedent. Because the magistrate judge and district court treated the data as tracking information, they applied the wrong legal standard. Using the proper framework, the SCA's authorization of § 2703(d) orders for historical cell site information if an application meets the lesser 'specific and articulable facts' standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional. Moreover, as long as the Government meets the statutory requirements, the SCA does not give the magistrate judge discretion to deny the Government's application for such an order."

Id. at 615.

B. Using a State Subpoena – *United States v. Guerrero* (5th Circuit 2014)

The Fifth Circuit did take another CSLI case to address whether suppression was warranted since the government collected CSLI with a state subpoena rather than a 2703(d) order

in *United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014). There, the Court held that "The violation of the Act is clear," but also held that the SCA does not provide for suppression. *Id.* Thus, appellant was required to show a Fourth Amendment violation, but since Fifth Circuit precedent already decided the warrantless collection of CSLI did not implicate the Fourth Amendment, the evidence was held to be properly admitted. *Id.* at 361.

C. No warrant required – Border exception: *United States v. Escarcega* (5th Circuit 2017)

In *United States v. Escarcega,* 15-51090, 2017 WL 1380555, (5th Cir. Apr. 17, 2017), the Fifth Circuit, in a per curiam decision, affirmed Escarcega's denial of a motion to suppress evidence of the warrantless search of his cell phone. *Id.* at *1. There, Escarcega turned over his cell phone to Border Patrol agents when attempting to cross the border into America. *Id.* The Court explained that "[t]he defendant in this routine crossing of the border could expect **no privacy of articles in his possession,"** and affirmed the lower court's denial of suppression.

D. No warrant required because of Exigent Circumstances: *United States v. Caraballo* (2nd Circuit 2016)

On August 01, 2016, the Second Circuit decided *United States v. Caraballo.* In that case, Caraballo was appealing his conviction for conspiring to distribute cocaine base, possessing a firearm causing death, and possessing a firearm in furtherance of a drug trafficking crime. *United States v. Caraballo*, 831 F.3d 95 (2d Cir. 2016), *cert. denied*, 137 S. Ct. 654, 196 L. Ed. 2d 546 (2017). In Caraballo's case, police officers were investigating the death of an associate of Caraballo's and asked Sprint, his network provider, to track the GPS coordinates of Caraballo's cell phone for a period of two hours. *Id.* at 97. Sprint complied with the request and the defendant was tracked down and arrested later that day. *Id.* Caraballo argued to the trial court should have suppressed the evidence collected upon his arrest because the "pinging" of his

cell phone violated his Fourth Amendment rights. The Second Circuit held that the exigent circumstances presented in the case justified the officers' warrantless identification of the GPS coordinates of Caraballo's phone and affirmed the conviction. *Id.*

The government in *Caraballo* argued that there were two possible sources of exigency to justify the search: (1) the officers reasonably believed that the defendant posed an exigent threat to the undercover officers and confidential informants involved in his drug operation; and (2) the time lapse associated with obtaining a warrant could result in the imminent destruction or dissipation of evidence. *Id.* at 104. The Court ruled that the first source sufficed to support the officers' "limited intrusion" in Caraballo's privacy from the pinging, and discussed the *Dorman/MacDonald* factors in their reasoning. The Second Circuit pointed out that the first two prongs indicated the officers were reasonable because the killing of the victim was brutal and the officers had reason to believe Caraballo was armed. They acknowledged that the third factor was not exactly met, but although they lacked probable cause to arrest, he was their "primary suspect." *Id.* The court stressed the fact that the officers had specific reasons to think that the suspect would commit acts of violence against undercover agents and confidential informants because, before her death, Caraballo had allegedly told the victim he would "kill her" if she spoke to the police. The Second Circuit ultimately concluded that:

> "The officers reasonably believed that Caraballo posed an exigent threat to the undercover officers and confidential informants involved in his drug operation. This threat justified the pinging of Caraballo's phone, a) which at most constituted a limited intrusion into his privacy interests, b) which objectively could be viewed as plausibly consistent with existing law and c) which the officers used in the most limited way to achieve their necessary aim."

Id. at 106.

E. "The Fourth Amendment in Retreat" – *United States v. Graham* (4th Circuit 2016)

Also in 2016, the Court of Appeals, en banc, decided *United States v. Graham,* 824 F.3d 421 (4th Cir. 2016). In that case, the defendants were convicted of being felons in possession of firearm, Hobbs Act robbery, conspiracy to commit Hobbs Act robbery, and brandishing a firearm after their denial of their motion to suppress. *Id.* There, law enforcement sought court orders through the Stored Communications Act (SCA), under which the government may compel disclosure of certain records under a standard lower than probable cause. They demanded that the defendants' phone carrier (Sprint/Nextel) provide the historical CSLI associated with the defendants' phones for a total of 221 days over seven months, collecting over 28,000 CSLI data points for each defendant. The government used this CSLI to place the defendants at most of the crime scenes. Denying their motion to suppress, the district court concluded that the defendants could not legitimately expect privacy in their historical CSLI records as they voluntarily conveyed that information to Sprint/Nextel; the third-party doctrine thus applied[6].

Although the Court of Appeals for the Fourth Circuit affirmed the convictions[7], they held that defendants' Fourth Amendment rights were violated when the government obtained historical cell-site location information from their cell phone provider without a warrant. The government moved for rehearing en banc, which was granted.

On rehearing, the Court held that government did **not** violate Fourth Amendment by obtaining historical CSLI from cell phone provider without warrant. *United States v. Graham,* 824 F.3d 421 (4th Cir. 2016). Diana Gribbon Motz, Circuit Judge writing for the majority, reasoned that by using their phones, the defendants "assumed the risk" that the carrier would transmit that information to the government. *Id.* at 427-28. She rejected the defendants' argument

[6] *See: United States v. Graham,* 796 F.3d 332, 350 (4th Cir. 2015), *reh'g en banc granted*, 624 Fed. Appx. 75 (4th Cir. 2015) *and adhered to in part on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016).
[7] *Id.*

that the information was not "voluntarily conveyed" because mobile phone users are aware that location matters because location determines reception. *Id.* Therefore, she argued, choosing to use cell phones despite that knowledge equates to users voluntarily conveying to carriers their location information. *Id.*

Circuit Judge Wynn wrote separately in *Graham*, joined by Circuit Judges Floyd and Thacker, dissenting in part and concurring in the judgement, but the opinion could be considered just a dissent. Wynn disagreed with the majority that the defendants voluntarily conveyed the CSLI. Wynn argued that binding precedent regarding "voluntary conveyance" means two things: (1) that the defendant **knew** he was communicating the particular information; and (2) that the defendant had **acted in some way** to submit the particular information he knew. *Id.* at 443. Wynn noted:

> "[T]here is no reason to think that a cell phone user is aware of his CSLI, or that he is conveying it. He does not write it down on a piece of paper, like the dollar amount on a deposit slip, or enter it into a device, as he does a phone number before placing a call. Nor does CSLI subsequently appear on a cell phone customer's statement, as the relevant information did for the banking customer in *Miller* and the phone caller in *Smith*."

Id. at 445. Wynn ends by adding:

> "What [the majority's reasoning] elucidates is the extraordinary breadth of the majority's decision today. It is not bounded by the relative precision of location data, by the frequency with which it is collected, or by the statutory safeguards Congress has thought it prudent to enact. The majority's holding, under the guise of humble service to Supreme Court precedent, markedly advances the frontlines of the third-party doctrine. **The Fourth Amendment, necessarily, is in retreat."**

Id. at 449 (emphasis supplied).

Although the defendants in *Graham* could seek Supreme Court review of the 4th Circuit en banc opinion, but it is unclear if the justices will be willing to hear the case, considering the current split in the Circuits.

F. No Search Involved – *United States v. Carpenter* (6th Circuit 2016)

In 2011, the government obtained several months' worth of cell phone location records for suspects in a criminal investigation in Detroit without getting a warrant. For one suspect, Timothy Carpenter, the records revealed 12,898 separate points of location data, and for Timothy Sanders, another suspect, the government got 23,034 separate location points—an average of 261 each day. After being convicted at trial, partly because of the introduced CSLI, they appealed to the Sixth Circuit Court in *United States v. Carpenter,* 819 F.3d 880 (6th Cir. 2016). There, a divided Sixth Circuit held that the government did not conduct a "search" for Fourth Amendment purposes when it obtained business records from defendants' wireless carriers for cell phone service, containing cell tower locational data. The court reasoned:

> "[Cell phone records] say nothing about the content of any calls. Instead the records include routing information, which the wireless providers gathered in the ordinary course of business. Carriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls. And carriers keep records of these data to find weak spots in their network and to determine whether roaming charges apply, among other purposes. Thus, the cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves. **The government's collection of business records containing these data therefore is not a search**."

Id. at 887 (emphasis supplied).

G. Texas Case – *Ford v. State*, 477 S.W.3d 321 (Tex. Crim. App. 2015)

On December 16, 2015, the Texas Court of Criminal Appeals released its opinion in *Ford v. State*, 477 S.W.3d 321 (Tex. Crim. App. 2015). While noting the apparent circuit split, it sided with the Fifth and Eleventh Circuits application of the Third-Party Doctrine to hold CSLI is "a record that the 'provider has already created'—[and therefore] is not subject to a reasonable expectation of privacy that implicates the Fourth Amendment." *Id.* at 322.

The court attempted to distinguish the case from previous cases like *Graham*[8] by arguing the circuit "took pains to repeatedly note that it was only addressing long-term [CSLI]." *Id.* at 333. Accordingly, a viable Fourth Amendment claim may escape the Third-Party Doctrine "if long-term location information were acquired." *Id.* at 334. The court did not explain what long-term meant, because the case at bar only involved four days. Interestingly, the concerns addressed by *Graham* were ignored in the Texas opinion; specifically, the government's lack of advance knowledge about how revealing the CSLI will be or whether it details movements in private spaces. *Graham*, 796 F.3d at 350. Regardless, the court felt confident "the Supreme Court is primed to take up this issue." *Ford*, 477 S.W.3d at 335.

H. Putting it all together – CLSI Texas & Fifth Circuit Precedent and what it all means

With the lack of Supreme Court guidance, Texas courts, among those in other states, are left to decide these issues on their own. The Fifth Circuit in *In re Application of the USA for Historical Cell Site Data, supra,* held that the government could avoid getting a warrant if they obtain court orders under the SCA. Then, in *United States v. Guerrero, supra,* the Fifth Circuit clarified that State subpoenas for CSLI information violated the SCA, but the violation did not require suppression. The Fifth Circuit has yet to address the constitutionality of other warrantless CSLI collection issues, including what exigent circumstances can satisfy an exception to the warrant requirement. Additionally, they make no mention of the real-time (as opposed to the historic cell site data discussed in *In Re Application of the USA for Historical Cell Site Data)* location data that can be obtained through CSLI, their privacy implications and

[8] In *United States v. Graham,* 796 F.3d 332 (4th Cir. 2015), reh'g en banc granted, 624 Fed. Appx. 75 (4th Cir. 2015)and adhered to in part on reh'g en banc, 824 F.3d 421 (4th Cir. 2016), the Fourth Circuit held that the government's warrantless procurement of cell site location information (CSLI) recorded by defendants' cell phone service provider violated Fourth Amendment. This case is also discussed *supra* at p 18-20.

whether these types of records require a warrant. It is important not to assume that all CSLI records are referring to historic data and remember this when dealing with a CSLI case.

VII. STINGRAY TECHNOLOGY

What the government continuously tries to hide, though, is the fact that they can receive all of this carrier-assisted surveillance data in other ways besides compelling carriers to disclose the information. Today, law enforcement agencies all over the country possess "StingRay" devices, though their use is typically cloaked in secrecy. StingRays are the most common device manufactured by the Harris Corporation, but the technology is also known as "TriggerFishes," International Mobile Subscriber Identity ("IMSI") catchers, digital analyzers, "KingFishes," "Hailstorms," and cell-site simulators. In essence, a StingRay device is an invasive cell phone surveillance tool that mimics cell phone towers and sends out signals to trick nearby cell phones into transmitting location data and other identifying information. When law enforcement uses these devices to track a suspect's cell phone, they also gather information from the mobile phones of countless bystanders who just happen to be in the same area, which can span several kilometers. This means that potentially thousands of people have their right to privacy violated every time a StingRay-like device is activated.

Although the underlying technology is complex and impressive, the device itself is simple in design and can be easily carried by hand, mounted on a drone, or installed on a vehicle.[9] If configured to do so, Stingrays can intercept the same data traditionally received from carrier-assisted surveillance, including the numbers dialed, historical and current location data,

[9] *Id.* at 145-46.

web pages visited from the mobile phone, and other similar data.[10] However, unlike with traditional carrier-assisted surveillance, the third-party provider will not necessarily have any knowledge of the surveillance performed or what records were disclosed to law enforcement. This means that when a StingRay device is utilized, it leaves no visual indication to the target that she is under surveillance and does not require the help of the third-party carrier whose network the device is impersonating. This technological design ensures that only the operator of the device (i) will have knowledge that an interception ever took place and (ii) has access to the intercepted information.[11] Using a StingRay device eliminates the problem law enforcement encounters when third-party network providers interfere with surveillance requests in the interest of their customers' privacy, and allows them to conduct this surveillance invisibly.

VIII. RECENT STINGRAY CASES

A. *State of Maryland v Andrews*, 134 A. 3d 324 (2016)

As of today, only one appellate court decision in the country has directly addressed the Fourth Amendment limits on police use of Stingrays. On March 30, 2016, the Maryland Court of Special Appeals decided *State of Maryland v. Andrews,* 134 A. 3d 324 (2016), and held that police are required to obtain a warrant in order to track cell phones. In *Andrews,* Baltimore Police used the "Hailstorm" (a cell site stimulator manufactured by the same company that makes StingRays) to locate the defendant, who was wanted on charges of attempted murder. *Id.* at 326. The Hailstorm device allowed law enforcement to track the defendant's cell phone to a precise location inside a residence. Officers arrested Andrews pursuant to a valid arrest warrant and found the cell phone in his pocket. The Circuit Court for Baltimore City agreed with

[10] See Harris Corp, Price List 4 (2008), https:// info.publicintelligence.net/Harris-SurveillancePriceList.pdf (listing an optional "GSM Intercept Software package" for the StingRay).
[11] Stephanie K. Pell & Christoper Soghoian, *supra*, at 146-47.

Andrews that the warrantless use of the Hailstorm device violated his Fourth Amendment rights and suppressed all evidence obtained from the defendant's home as fruit of the poisonous tree, and the State appealed. *Id.* Justice Leahy agreed with Andrews and wrote for the three judge panel on appeal, holding:

> "We conclude that **people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement**, and—recognizing that the Fourth Amendment protects people and not simply areas—that people have an objectively reasonable expectation of privacy in real-time cell phone location information. Thus, we hold that **the use of a cell site simulator requires a valid search warrant**, or an order satisfying the constitutional requisites of a warrant, unless an established exception to the warrant requirement applies."

Id. at 350 (emphasis supplied).

Most privacy advocates hailed the opinion as a landmark decision, hoping that other courts would look to this decision with upcoming cell site simulator cases. In addition to the holding, the case shed light on just how common the use of StingRay devices is becoming, as Baltimore police testified during the case that they had used the technology 4,300 times since 2007.[12] By 2014, Baltimore had become a hot spot for the debate over the use of StingRay technology, which had been used by law enforcement for years but always kept secret from the public. Then, in 2015, the Baltimore Sun published a non-disclosure agreement that purported to be between the FBI and the Baltimore Police and State's Attorney's Office, in which local authorities agreed to "never disclose the use of a StingRay device."[13] The State agreed to drop cases if they presented a risk that the StingRay technology might be revealed, and although

[12] Spencer S. Hsu, *A Maryland court is the first to require a warrant for covert cellphone tracking,* The Washington Post, March 31, 2016, available at: https://www.washingtonpost.com/world/national-security/a-maryland-court-is-the-first-to-require-a-warrant-for-covert-cellphone-tracking/2016/03/31/472d9b0a-f74d-11e5-8b23-538270a1ca31_story.html?utm_term=.cabfd945d986

[13] Justin Fenton, *Maryland appellate court: warrant required for 'stingray' phone tracking,* The Baltimore Sun, March 31, 2016, 4:04 p.m., *available at: http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-stingray-court-decision-20160331-story.html*

similar agreements were being made around the country, this was one of the first agreements to be unveiled to the public.[14] In their brief to the court, the Maryland Attorney General's Office argued that cell phone users have the option of turning off their mobile phones if they do not wish to be tracked by the government. Although the *Andrews* opinion addressed some Fourth Amendment concerns, it is still unclear what types of exceptions to the warrant requirement and surrounding circumstances will justify the warrantless use of StingRay devices.

B. *Prince Jones v. United States of America*, No. 15-CF-322, DC Court of Appeals

As of the date of this publication, a three-judge panel of the highest local appeals court in Washington, D.C., is grappling over the limits of privacy expectations in a case involving the warrantless use of a StingRay device to locate a suspect. The challenge before the court comes from the appeal of Prince Jones, who was convicted in November of 2014 of robbing three women and raping two of them.[15] During the 2013 attacks, Jones stole a cell phone from one of the victims. Assuming the suspect would use the stolen mobile phone, D.C. police officers employed the use of a StingRay device, without a warrant, to track down the phone's location. The D.C. officers believed that no warrant should be required because of an exigent circumstance, namely, that the suspect would use the stolen cell phone for only a short period of time then abandon it.[16] Using the StingRay, the law enforcement officers were able to precisely locate the suspect, Prince Jones, who was sitting in his car with the stolen phone. Jones's defense challenged the warrantless use of the StingRay before the trial court, and the lower court found that even if the police actions violated the Fourth Amendment, the evidence found in the

[14] *Id.*
[15] No. 15-CF-322, DC Court of Appeals.
[16] Howard W. Cox, *StingRay Technology and Reasonable Expectations of Privacy in the Internet of Everything,* Federalist Society Review, Volume 17, Issue 1, March 31, 2016, *available at: http://www.fed-soc.org/publications/detail/stingray-technology-and-reasonable-expectations-of-privacy-in-the-internet-of-everything*

car could still be used under the "inevitable discovery" doctrine.[17] Now on appeal, the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) have filed an amicus brief in support of Jones, arguing that warrants should be required before law enforcement uses a StingRay device. The brief points out that (1) the device can locate people's cell phones with great precision, including inside of homes and other private spaces protected by the Fourth Amendment, and (2) they can sweep in information about not just a suspect's cell phone but numerous bystanders' phones as well.[18] The ACLU and EFF also reported that an investigation revealed that in D.C., the city spent more than $200,000 in 2002 and 2003 to purchase Triggerfish and StingRay cell-site simulators from the Harris Corp., although grants to train officers were not approved until 2009, as first reported in late 2014 by a Vice News journalist.[19]

Regardless of what the D.C. Court of Appeals holds, it is easy to see that light is finally being shed on law enforcement's extensive use of StingRay devices. In recent years, law enforcement agencies around the country have reported using cell-site simulators in hundreds of cases, including police in the cities of Charlotte, Milwaukee, Tacoma, and Tallahassee. It has also been reported that numerous federal law enforcement agencies in Department of Justice (DOJ), the Department of Homeland Security (DHS), and the Department of the Treasury are currently using some form of StingRay technology. Additionally, New York City recently disclosed using the technology more than 1,000 times over seven years, and Baltimore City and county police about 5,000 times over five years.[20] In other instances, law enforcement have said

[17] *U.S. v. Price Jones – Challenge to Police's Warrantless Use of 'Stingray' Cell Phone Tracker,* ACLU, Updated April 12, 2017, available at: https://www.aclu.org/cases/us-v-prince-jones-challenge-polices-warrantless-use-stingray-cell-phone-tracker
[18] *Id.*
[19] *Id.*
[20] *Id.*

that they used cell-site simulators after obtaining court orders for pen registers from service providers, even though such orders were traditionally used to record incoming and outgoing numbers dialed to or from a particular phone, and are held to a lower standard of proof than required for search warrants.

Some members of the United States Congress are also seeking to pressure federal government agencies to adopt a policy of obtaining warrants before using a StingRay device. In 2014, the FBI instituted an internal policy that **most** FBI StingRay applications would be based upon a search warrant standard. Even more recently, the DOJ announced a policy guidance seeking to submit **most** federal law enforcement StingRay applications to a warrant standard.[21] Although these are steps in the right direction, policy statements like these do not typically apply to the operation of non-DOJ law enforcement agencies.

IX. OTHER WARRANTLESS DATA CONCERNS

A. United States v. Weast (5th Circuit 2016)

In *U.S. v. Weast,* the Fifth Circuit held that the defendant did not have reasonable expectation of privacy in internet protocol (IP) address or file shared on peer-to-peer network. *United States v. Weast,* 811 F.3d 743 (5th Cir. 2016), *cert. denied*, 137 S. Ct. 126, 196 L. Ed. 2d 99 (2016). There, police officers used a peer-to-peer file sharing software to search for computer users sharing child pornography. *Id.* at 746. Law enforcement then located an IP address whose corresponding user appeared to be sharing child pornography and subsequently downloaded six files shared by the user. *Id.* Officers then used a publicly accessible website to determine the internet service provider (ISP) associated with the IP address from his search, and served a subpoena on them. *Id.* The response to the subpoena revealed that the IP address was

[21] *Id.* at n.16

registered to the defendant and the officers executed a search warrant at his residence, where they found him. *Id.* On appeal, Weast argued that his Fourth Amendment rights were violated by the use of the peer-to-peer software, without a warrant, to identify his IP address as possibly linked to child pornography and to download data that the defendant had made available for sharing. *Id.* at 747. The *Weast* court wrote:

> **We have never explicitly stated whether IP addresses or files shared through peer-to-peer networks are subject to a reasonable expectation of privacy**. However, other circuits have concluded that they are not. As the Third Circuit has explained, "[f]ederal courts have uniformly held that 'subscriber information provided to an internet provider,' " including IP addresses, " 'is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties."10 Similarly, other courts have consistently held that Fourth Amendment protections do not extend to data shared through peer-to-peer networks…
>
> The reasoning of Guerrero easily extends to the facts now before us; **IP addresses and peer-to-peer-shared files are widely and voluntarily disseminated in the course of normal use of networked devices and peer-to-peer software, just as cell phone location data are disseminated in the course of normal cell phone use.** For this reason, Weast's Fourth Amendment rights were not violated when Officer Watkins accessed his IP address and shared files.

Id (emphasis supplied).

B. United States v. Caira, (7th Circuit 2016)

Similarly, In *United States v. Caira,* the Sixth Circuit ruled that the defendant had no reasonable expectation of privacy in his Internet Protocol addresses. *United States v. Caira*, 833 F.3d 803 (7th Cir. 2016). There, the Court reasoned that the defendant shared the information with a third party, namely, Microsoft, who was the owner of the web-based e-mail service he was using. Because he shared this information, the Drug Enforcement Administration (DEA) committed no Fourth Amendment search when it subpoenaed that information, despite contention that such subpoena was equivalent to placing tracking device on him. *Id.* at 806. They stated that the defendant sent address to the owner every time he logged in to his e-mail

service, and the government received much less information than tracking device would have provided. *Id.* at 807.

X. POSSIBLE NEW LEGISLATION

A. Warrant before StingRay Use – The GPS Act

On February 15, 2017, a bipartisan group of House and Senate lawmakers introduced the Geolocation Privacy and Surveillance (GPS) Act for the 115th Congress. This new legislation would require police agencies to obtain a search warrant before they can deploy StingRay devices. The Act (S.395, H.R. 1062) would also prohibit businesses from disclosing geographical tracking data about its customers to others without the customers' permission.[22] Only time will tell if Congress will take action, but for now, the GPS Act is just a bill on Capitol Hill.

B. Warrant before border search – Protecting Data at the Border Act

Recently, four members of Congress introduced a bill (the Protecting Data at the Border Act) that would make it illegal to access the contents of a device belonging to a U.S. citizen or permanent resident without first obtaining a warrant.[23] Traditionally, law enforcement shields itself by claiming broad authority to search because of the border exception, but this bill even specifies that border agents can't hold people for more than four hours in attempts to compel them to give up information or unlock their phone. These privacy concerns are now more important than ever before, especially considering the dramatic rise in the number of cell phone searches conducted near the border in the past few years. The number of cell phone border

[22] *See: Geolocation Privacy*, available at: http://www.gps.gov/policy/legislation/gps-act/
[23] Cora Currier, *Lawmakers Move to Stop Warrantless Cellphone Searches at the U.S. Border,* The Intercept, April 04, 2017, available at: https://interc.pt/2oyZePi

searches spiked from 5,000 in 2015 to 25,000 in 2016, and reports show that there were 5,000 in February of 2017 alone.[24] The proposed bill allows emergency exceptions and unfortunately does not protect non-U.S. citizens, but the legislation overall would be a huge win for privacy advocates if passed into law.

XI. FISA 702 – The government's #1 Spy

"Section 702 is probably one of the most if not the most valuable surveillance authority for the national security community today." *–Raj De; Former general counsel for the NSA*

Congress first enacted the Foreign Intelligence Surveillance Act of 1978 ("FISA"), which created the Foreign Intelligence Surveillance Court ("FISA Court") and gave it the power to grant or deny government applications for surveillance orders in foreign intelligence investigations. *See:* 50 U.S.C. § 1803(a). In July of 2008, President Bush signed into law the FISA Amendments Act of 2008 ("FAA"),[25] which includes the new Section 702. Under this statute, the U.S. Attorney General and the Director of National Intelligence (DNI) may jointly authorize surveillance of people who are not "U.S. persons."[26] Essentially, FISA Section 702 currently grants the government authority to acquire foreign intelligence by targeting non-U.S. persons "reasonably believed" to be outside U.S. borders, but this isn't how it plays out. While not directly aimed at targeting U.S. persons, this change invested the government with far-reaching new authority to collect Americans' international communications from numerous facilities inside the United States.

A critical difference between traditional FISA and the FAA is that under the latter, surveillance can be authorized despite not being predicated on probable cause or even individualized suspicion. Under section 1881a, the government does not have to demonstrate to

[24] *Id.*
[25] *See:* FISA Amendments Act of 2008, P.L. 110–261, July 10, 2008, 122 Stat 2436.
[26] *See: Id.*

the FISA Court that the intended surveillance targets are even suspected criminals, much less terrorists, because the section does not require them to identify the surveillance targets at all.[27] The FAA does not limit government surveillance to particular persons reasonably believed to be outside the country, but instead allows bulk collection of content within the topics certified for collection for surveillance and eventual data mining.

Although much is still unknown about the interworking of these programs, the public was made aware of additional details after Edward Snowden's leaks in 2013, including the fact that a FISA Court Judge approves the program features, which include the targeting procedures.[28] The targeting procedures remain classified information, but new leaks in 2009 revealed that foreignness and location determinations are made based on the "totality of the circumstances," including information from leads, agency databases that may be relevant to location, and the "technical analyses" of the facility from which it expects to acquire intelligence.[29]

The NSA receives Section 702 content from network providers through two alarming programs, "Prism," (the larger program) and "Upstream." Prism involves the government relying on information about a particular e-mail address, phone number, or other information about a person, linking it or him to a foreign intelligence objective. The address or name is then made a "selector" and the government can then order internet companies (like Google, Apple, and Facebook) to search all information in their possession and copy whatever data is tied to a "selector."[30] These selectors can be very broad in scope and are connected to massive amounts

---

[27] See: David Kris & J. Douglas Wilson, National Security Investigations & Prosecutions § 17.3, 602 (2012) ("For non-U.S. person targets, there is no probable-cause requirement; the only thing that matters is the government's reasonable belief about the target's location" (internal parentheses omitted).
[28] William C. Banks, *Next Generation Foreign Intelligence Surveillance Law*: Renewing 702, 51 U. Rich. L. Rev. 671, 678–79 (2017)(footnote omitted)
[29] *Id.*
[30] Daniel Schuman and Sean Vitka, *Drawing a Line on Mass Surveillance: How Congress must Reform Section 702,* Just Security, Thursday, March 23, 2017 at 8:34 a.m., *available at:* https://www.justsecurity.org/39142/drawing-line-mass-surveillance-congress-reform-section-702/

of information which is all turned over to the government. A Washington Post analysis found 9 out of 10 people whose account information was collected were not intended targets of government surveillance and half of them were American citizens.[31] Similarly, the Washington post evaluated 160,000 texts and emails gathered by the NSA and found that 90% of the account holders were not foreign targets, and most of them were Americans.[32]

Upstream works backwards and allows the government to compel entities like AT&T to scan the information flowing through the underlying infrastructure that links continents and enables the internet's global activity. This search is again done using "selectors," but allows agencies to receive the information in real-time.[33] Upstream's information scanning has no regard for privacy or sensitivity and affects all information traveling across the cables.[34] The information connected with these broad "selectors" can contain our most private communications, yet are collected and turned over to the government without our knowledge.

Whether generated through Prism or Upstream, the data collected from these programs can then be subjected to warrantless FBI "backdoor searches," even if no suspicion of wrongdoing is present.[35] The FBI also has broad power to distribute these data to virtually any law enforcement body , including data that may contain evidence of serious or minor crimes.[36]

Now utilized as a key surveillance program, the current form of FISA 702 is set to expire on at the end of this year unless Congress renews it, and the topic is sparking debate between current lawmakers. NPR reported that at a recent House Judiciary Committee hearing on reauthorizing the section, testimony was given that despite the requirement to hide the names of

---

[31] *Id.*
[32] Sarah St. Vincent, *Broad Warrantless Surveillance Threatens to Undermine the Criminal Justice System,* Just Security, April 26, 2017, at 9:20 am, *available at: https://www.justsecurity.org/40292/broad-warrantless-surveillance-threatens-undermine-criminal-justice-system/*
[33] *Id.*at n.26.
[34] *Id.*
[35] *Id.* at n.28
[36] *Id.*

American persons or entities in surveillance records, Americans' emails and phone conversations collected under the statute can be used against them in a criminal case.[37] According to NPR, this upset some current lawmakers, including Republican Ted Poe, who argued that this was a clear Fourth Amendment violation. They also reported that Idaho Republican Raul Labrador similarly provided recent examples of such abuse by pointing out recent news leaks about Michael Flynn's phone conversations with the Russian ambassador, which ultimately ended Flynn's short career as President Trump's national security adviser.[38] Other Republican and Democrat lawmakers have also expressed concern over the amount of Americans' communications that are incidentally collected under the statute. In today's day and age, communication has never been easier and privacy concerns have never been greater, and it is clear to see that lawmakers on both sides of the political system are starting to see this.

XII. NEW TRUMP LAW

Bye bye, Internet Privacy & Hello, new spies:

On Monday, April 03, 2017, President Trump signed a congressional resolution that completed the overturning of the internet privacy protections put in place by the Obama-era FCC. The new resolution makes it easier for broadband internet service suppliers (like AT&T and Spectrum) to track and even sell a customer's online information, including browsing history, like internet companies like Facebook and Google can.[39] Had they not been repealed, the Obama-era FCC rules would have required these broadband suppliers to receive permission before collecting customer's data. Privacy experts point out that the repeal offers no substitute,

[37] See: *Intelligence Leaks Complicate Efforts To Renew Key Surveillance Program* Transcript, National Public Radio, April 17, 2017, 4:30 p.m., available at: http://www.npr.org/templates/transcript/transcript.php?storyId=524393106

[38] *Id.*

[39] Todd Heisler, *Trump Completes Repeal of Online Privacy Protections From Obama Era,* The New York Times, April 3, 2017, *available at:* https://nyti.ms/2nDJW7V

despite the fact that broadband companies offer a different position than internet companies because they are a fundamental tool in accessing the internet.[40] With the new lack of regulations, it will be interesting to see how courts will respond when a broadband internet provider discloses law enforcement the content and details of a customer's internet activity without first obtaining a warrant, regardless of whether law enforcement complied with the SCA, and whether they will require warrants even when the SCA does not.

XIII. CONCLUSION

As cell phones and other technologies continue to advance and make our everyday lives easier, they become integrated into our daily lives and are usually available at all times and places. Law enforcement has now found ways to take advantage of our everyday reliance on these devices and have developed their own tools to get an inside look on who we are and what our daily lives consist of. As this paper has discussed, courts are struggling to apply the Fourth Amendment to these types of cases and have received little guidance from the Supreme Court. Additionally, not even 100 days into his presidency, Trump has already signed new law banishing internet privacy restrictions announced by the FCC during the Obama-era. Only time will tell how the courts will handle these privacy concerns in the future, and until Congress steps in, it is anyone's best guess. Until then, we're facing a new day and age where some of our most valuable private information is being collected, stored, and distributed to the government without our or knowledge, much less our consent.

[40] *Id.*