

HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 1457 Searches of Cellular Phones and Other Electronic Devices

SPONSOR(S): Criminal Justice Subcommittee, Newton

TIED BILLS: **IDEN./SIM. BILLS:** CS/SB 470

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Criminal Justice Subcommittee	14 Y, 0 N, As CS	Padgett	Hall
2) Justice Appropriations Subcommittee			
3) Judiciary Committee			

SUMMARY ANALYSIS

A mobile tracking device is an electronic or mechanical device, like a GPS tracker, that tracks the movement of a person or object. Florida law currently authorizes law enforcement to install a mobile tracking device pursuant to a court order.

CS/HB 1457 requires law enforcement to obtain a warrant to conduct real-time location tracking or acquire historical location data, consistent with recent United States Supreme Court holdings. The bill defines real-time location tracking as:

- Installing and using a mobile tracking device on the object to be tracked;
- Acquiring real-time cell-site location data; or
- Acquiring real-time precise global positioning system location data.

The bill defines historical location data as:

- Historical cell-site location data in the possession of a provider; and
- Historical precise global positioning systems location data in the possession of a provider.

An officer must install a mobile tracking device within 10 days of the warrant's issuance. Additionally, the bill places time constraints on how long such a device may be used; the timeframe in which the device is used must be specified in the warrant and may not exceed 45 days from when the warrant was issued. For good cause, the court may grant one or more extensions, each of which may not exceed 45 days.

The bill imposes notice requirements for law enforcement use of a location tracking device. Within 90 days after the surveillance timeframe specified in the warrant, the officer executing the warrant must serve a copy on the person whom, or whose property, law enforcement tracked. The court may postpone notice upon a showing of good cause at the request of law enforcement.

The bill amends the definition of oral communication in the context of wiretapping and stored communications to explicitly include communication recorded by a microphone-enabled household device.

The bill has an indeterminate fiscal impact on state and local governments.

The bill provides an effective date of July 1, 2020.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Fourth Amendment

The Fourth Amendment of the United States Constitution guarantees:

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated; and
- No warrants shall issue without probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.¹

Under Fourth Amendment jurisprudence, a search occurs whenever the government intrudes upon an area in which a person has a reasonable expectation of privacy.² A warrantless search is generally per se unreasonable,³ unless an exception to the warrant requirement applies.⁴

The Florida Constitution similarly protects the people against unreasonable searches and seizures, and that right is construed in conformity with the Fourth Amendment of the U.S. Constitution.⁵ Both the Florida and federal constitutions require a warrant to be supported by probable cause, as established by oath or affirmation, and to particularly describe the place to be searched and items or people to be seized.

Advancing technology has presented law enforcement with new means of investigation and surveillance, and the courts with new questions about the Fourth Amendment implications of this technology.

Search Warrants

Chapter 933, F.S., contains grounds related to when and why a search warrant may be issued to a law enforcement officer by a judge authorizing the search and seizure of evidence, and the procedures for executing the search warrant.⁶

The issuance of a search warrant is based upon probable cause, therefore an application made under oath to a judge for a search warrant must “set forth the facts tending to establish the grounds of the application or probable cause for believing that they exist.”⁷ The application must particularly describe the place to be searched and the person and thing to be seized.⁸ If the judge finds that probable cause exists for the issuance of the search warrant, the judge must issue the search warrant.⁹

The grounds for the issuance of a search warrant include:

- When property has been stolen or embezzled in violation of law;
- When any property has been used:
 - As a means to commit any crime;
 - In connection with gambling, gambling implements and appliances; or
 - In violation of s. 847.011, F.S., or other laws in reference to obscene prints and literature;

¹ U.S. Const. amend. IV.

² *Katz v. United States*, 389 U.S. 347 (1967).

³ *United States v. Harrison*, 689 F.3d 301, 306 (3d Cir. 2012)

⁴ Examples of exceptions to the warrant requirement include exigent circumstances, searches of motor vehicles, and searches incident to arrest.

⁵ Art. 1, s. 12, Fla. Const.

⁶ Ss. 933.01–933.19, F.S.

⁷ S. 933.06, F.S.

⁸ S. 933.04, F.S.

⁹ S. 933.07, F.S.

- When any property constitutes evidence relevant to proving that a felony has been committed;
- When any property is being held or possessed:
 - In violation of any laws prohibiting the manufacture, sale, and transportation of intoxicating liquors;
 - In violation of fish and game laws;
 - In violation of laws relative to food and drug; or
 - In violation of laws relative to citrus disease pursuant to s. 581.184, F.S.; or
 - When laws in relation to cruelty to animals, as provided in ch. 828, F.S., have been or are violated in any particular building or place.¹⁰

A search warrant may also be issued for the search for and seizure of “any papers or documents used as a means of or in aid of the commission of any offense against the laws of the state.”¹¹ Section 933.18, F.S., limits the grounds for the issuance of a search warrant for a private dwelling to particular circumstances. No search warrant may be issued for a private dwelling under ch. 933, F.S., or any other law of the state unless:

- It is being used for the unlawful sale, possession, or manufacture of intoxicating liquor;
- Stolen or embezzled property is contained therein;
- It is being used to carry on gambling;
- It is being used to perpetrate frauds and swindles;
- The law relating to narcotics or drug abuse is being violated therein;
- A weapon, instrumentality, or means by which a felony has been committed, or evidence relevant to proving said felony has been committed, is contained therein;
- One or more of the following child abuse offenses is being committed there:
 - Interference with custody, in violation of s. 787.03, F.S.;
 - Commission of an unnatural and lascivious act with a child, in violation of s. 800.02, F.S.; or
 - Exposure of sexual organs to a child, in violation of s. 800.03, F.S.
- It is, in part, used for some business purpose such as a store, shop, saloon, restaurant, hotel, boardinghouse, or lodginghouse;
- It is being used for the unlawful sale, possession, or purchase of wildlife, saltwater products, or freshwater fish being unlawfully kept therein;
- The laws in relation to cruelty to animals, as provided in ch. 828, F.S., have been or are being violated therein; or
- An instrumentality or means by which sexual cyberharassment has been committed in violation of s. 784.049, F.S., or evidence relevant to proving that sexual cyberharassment has been committed, is contained therein.¹²

Upon serving a warrant, an officer must deliver a copy of the warrant to the person named in the warrant.¹³ When the officer returns the warrant to the court, he or she must attach an inventory,¹⁴ which must be delivered to the person named in the warrant upon request.¹⁵

Procedural Search Warrant Requirements

Federal Rules of Criminal Procedure

Rule 41 of the Federal Rules of Criminal Procedure (Rule) governs search warrants. In addition to requiring a warrant in certain situations, consistent with Fourth Amendment jurisprudence, the Rule imposes certain technical requirements. Under the federal Rule, a warrant for a tracking device must:

- Identify the person or property to be tracked.
- Designate the magistrate judge to whom it must be returned.

¹⁰ S. 933.02(1)–(5), F.S.

¹¹ S. 933.02, F.S.

¹² S. 933.18, F.S.

¹³ S. 933.11, F.S.

¹⁴ S. 933.12, F.S.

¹⁵ S. 933.13, F.S.

- Specify a reasonable length of time that the device may be used, not to exceed 45 days from the date of warrant issuance.
- Command the officer to:
 - Complete any installation authorized by the warrant within a 10 days.
 - Perform any installation authorized by the warrant during the daytime, unless the judge authorizes otherwise with good cause.
 - Return the warrant to the judge.¹⁶

The Rule also dictates procedures for returning and serving a tracking device warrant. Within 10 days after tracking has ended, the officer executing a tracking device warrant must:

- Return it to the judge designated in the warrant.
- Serve a copy of the warrant on the person who, or whose property, was tracked.¹⁷

A judge may delay service and notice if authorized by statute.

Florida

Law enforcement must follow certain statutory procedures for wiretapping orders under ch. 934, F.S., including notice to those whose communications were intercepted. Within a reasonable period of time, but not later than 90 days after interception terminated, a court must serve an inventory on the subject of the order and other parties to the intercepted communications.¹⁸ Such inventory must include:

- The fact of the entry of the order or the application.
- The date of entry and the period of authorized, approved, or disapproved interception, or denial of the application.
- The fact that during the period, communications were or were not intercepted.¹⁹

A party may move to inspect portions of the intercepted communications, applications, and orders.²⁰ The court may also postpone inventory service on an *ex parte* showing of good cause.²¹

Exclusionary Rule

Under the exclusionary rule, evidence collected in violation of a defendant's constitutional rights may not be used against him or her at trial.²² However, violations of certain ministerial rules related to, but not implicating, constitutional protections do not necessarily invoke the exclusionary rule. These violations include failure to serve a copy of the warrant on the person searched or to return the warrant. Courts have typically held that a ministerial or technical violation requires suppression of evidence only if:

- There was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the rule had been followed; or
- There is evidence of intentional and deliberate disregard of the rule.²³

In Florida, an appellate court has held that properly returning a warrant is ministerial in nature and failure to do so does not void the warrant, absent a showing of prejudice.²⁴

Searches of Cell Phones

¹⁶ Fed. R. Crim. P. 41(e)(2)(C).

¹⁷ Fed. R. Crim. P. 41(f)(2).

¹⁸ S. 934.09(8)(e), F.S.

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

²² *Weeks v. United States*, 232 U.S. 383 (1914); *Mapp v. Ohio*, 367 U.S. 643 (1961).

²³ *United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988).

²⁴ *Nofs v. State*, 295 So.2d 308 (Fla. 2d DCA1974).

An exception to the warrant requirement is a search incident to arrest, allowing law enforcement to perform a warrantless search of an arrested person, and the area within the arrestee's immediate control, in the interest of officer safety and to prevent escape or the destruction of evidence.²⁵

In *Riley v. California*,²⁶ the United States Supreme Court held that law enforcement must obtain a search warrant to search the digital contents of a cell phone seized incident to arrest. The Court considered the advanced capabilities of modern cell phones, noting that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."²⁷ The Court reasoned that a modern smartphone's immense storage capacity allows it to carry a tremendous quantity and variety of records regarding a person's private life, such as photographs, prescriptions, bank records, contacts, and videos.²⁸

Wiretapping and Stored Communications

By Law Enforcement

Wiretapping generally refers to electronic or mechanical eavesdropping on communications.²⁹ Law enforcement use of a wiretap is subject to Fourth Amendment protections under the United States Constitution.³⁰

In Florida, a law enforcement officer may apply for an order authorizing the interception of wire, oral, or electronic communication.³¹ In addition to the standard requirements of probable cause, oath or affirmation, and particularity, as required for a search warrant, an interception order application must include:

- The identity of the officer making and authorizing the application.
- A full and complete statement of the facts and circumstances justifying the order, including:
 - Details of the offense.
 - A description of the nature and location where the communications will be intercepted, with exceptions.
- A particular description of the type of communications to be intercepted.
- The identity of the person, if known, committing the offense and whose communications are to be intercepted.
- Whether or not law enforcement has tried other investigative procedures that have failed, or why other procedures are reasonably unlikely to succeed or too dangerous.
- The time period for interception.
- All previous applications involving any of the same persons, facilities, or places specified in the application.
- If applying for an extension, the results obtained thus far from the interception or a reasonable explanation of the failure to obtain such results.³²

A court may require additional testimony or documentary evidence in support of an interception order application. Only the Governor, the Attorney General, the statewide prosecutor, or any state attorney may authorize an interception order application, and the order must pertain to certain enumerated crimes.³³ Upon receiving such an order, a communication service provider, landlord, custodian, or any other person may not disclose the existence of any interception or the device used to accomplish the interception.³⁴

By the General Public

²⁵ *Chimel v. California*, 395 U.S. 752 (1969).

²⁶ 134 S.Ct. 2473 (2014).

²⁷ *Id.* at 2484.

²⁸ *Id.* at 2489.

²⁹ Black's Law Dictionary (10th ed. 2014), wiretapping.

³⁰ *Katz v. United States*, 389 U.S. 347 (1967).

³¹ S. 934.09, F.S.

³² *Id.*

³³ S. 934.07, F.S.

³⁴ S. 934.03(2)(a)3., F.S.

Florida law prohibits wiretapping by the general public.³⁵ Subject to exceptions, it is a third degree felony³⁶ to intentionally:

- Intercept any wire, oral, or electronic communication;
- Use any electronic, mechanical, or other device to intercept any oral communication when:
 - Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
 - Such device transmits communications by radio or interferes with the transmission of such communication;
- Disclose to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through illegal interception;
- Use the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through illegal interception; or
- Disclose to any other person the contents of any wire, oral, or electronic communication intercepted by authorized means when that person:
 - Knows or has reason to know that the information was obtained through the interception in connection with a criminal investigation;
 - Has obtained or received the information in connection with a criminal investigation; and
 - Intends to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.³⁷

The penalty for wiretapping may be decreased to a misdemeanor³⁸ under the following circumstances:

- The person has no prior wiretapping offenses;
- The conduct was not done for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; and
- The intercepted communication was a radio communication that was not scrambled, encrypted, or transmitted using modulation techniques intended to preserve the privacy of such communication.³⁹

Stored Communications

Separate from wiretapping, Florida law also criminalizes unlawfully accessing stored communications by intentionally:

- Accessing without authorization an electronic communication service provider facility; or
- Exceeding authorization to access such facility.⁴⁰

The penalties for unlawfully accessing stored communications vary based on specific intent and the number of offenses. If the offense is committed for the purpose of commercial advantage, malicious destruction or damage, or private commercial gain, it is a first degree misdemeanor for a first offense and a third degree felony for a second or subsequent offense.⁴¹ If the offense was not committed for commercial advantage, malicious destruction or damage, or private commercial gain, it is a second degree misdemeanor.⁴²

New Technologies

Several technologies now use microphone-enabled features, which may be activated in different ways. Some, such as many Smart TVs, require the user to manually activate the microphone by pressing a

³⁵ S. 934.03, F.S.

³⁶ A third degree felony is punishable by up to five years in prison and a \$5,000 fine. Ss. 775.082 and 775.083, F.S.

³⁷ S. 934.03(1), F.S.

³⁸ Misdemeanors are classified as either first- or second-degree. A first degree misdemeanor is punishable by up to one year in county jail and a \$1,000 fine. A second degree misdemeanor is punishable by up to 60 days in county jail and a \$500 fine. Ss. 775.082 and 775.083, F.S. Under s. 934.03(4), F.S., wiretapping may be either a first- or second-degree misdemeanor, depending on the specific type of communication intercepted.

³⁹ S. 934.03(4), F.S.

⁴⁰ S. 934.21(1), F.S.

⁴¹ S. 934.21(2)(a), F.S.

⁴² S. 934.21(2)(b), F.S.

button.⁴³ Some respond to a trigger phrase, activating the device to begin transmitting information. These devices, which include many home assistant devices such as the Google Home and Amazon Echo, constantly “listen” for the trigger phrase.⁴⁴ The service provider remotely stores recordings from the devices for quality control.⁴⁵ Other devices, such as baby-monitors and home security systems, are always recording.⁴⁶

As these microphone-enabled devices grow in popularity, privacy concerns mount. A security expert recently demonstrated how an Amazon Echo might be hacked.⁴⁷ Additionally, prosecutors in Arkansas requested recordings possibly made by an Amazon Echo in a murder case.⁴⁸

Pen Registers and Trap and Trace Devices

Pen registers and trap and trace devices can track incoming and outgoing phone calls in real time. Historically, a pen register was understood to record the telephone numbers dialed from a target telephone, and a trap and trace device to record the telephone numbers from incoming calls to a target telephone.⁴⁹

Florida law defines a pen register as a device or process that records or decodes dialing, routing, addressing, or signaling information, not including the contents of any communication.⁵⁰ A trap and trace device means a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication; a trap and trace also does not intercept the contents of any communication.⁵¹ Florida’s definition of these terms are substantially similar to the definitions in the federal Pen Register Act.⁵² The broader statutory definitions draw more types of information, other than content, under the purview of a pen register or trap and trace device order.⁵³

Law enforcement may only install a pen register or trap and trace device pursuant to an order under s. 934.33, F.S. The application for such an order must include:

- The identity of the applicant and the law enforcement agency conducting the investigation; and
- A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the investigating agency.⁵⁴

The statutory requirement of relevancy to an ongoing criminal investigation falls short of the probable cause standard, as required for the issuance of a search warrant.

In *Smith v. Maryland*,⁵⁵ the United States Supreme Court considered whether Fourth Amendment protections applied where the government warrantlessly installed and used a pen register at a telephone company's offices to record the telephone numbers a target phone dialed. Through the pen register, law enforcement discovered that a telephone in Smith's home had been used to place a call to

⁴³ Future of Privacy Forum, *Microphones and the Internet of Things* (Aug. 2017), <https://fpf.org/wp-content/uploads/2017/08/Microphones-Infographic-Final.pdf> (last visited Feb. 3, 2020).

⁴⁴ *Id.*

⁴⁵ Nicole Chavez, *Arkansas judge drops murder charge in Amazon Echo case*, CNN (Dec. 2, 2017), <http://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html> (last visited Feb. 3, 2020).

⁴⁶ Future of Privacy Forum, *supra* note 43.

⁴⁷ Jay McGregor, *Listening-in on a Hacked Amazon Echo is Terrifying*, Forbes (Sep. 7, 2017), <https://www.forbes.com/sites/jaymcgregor/2017/09/07/listening-in-on-a-hacked-amazon-echo-is-terrifying/#32744f415c7f> (last visited Feb. 3, 2020).

⁴⁸ Chavez, *supra* note 45.

⁴⁹ *Tracey v. State*, 152 So.3d 504, 506 (Fla. 2014).

⁵⁰ S. 934.02(20), F.S.

⁵¹ S. 934.02(21), F.S.

⁵² 18 U.S.C. § 3127.

⁵³ For example, the U.S. Department of Justice used pen register orders to track real-time locations of a cell-phone using a cell-site simulator until September 2015. U.S. Department of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* (Sep. 3, 2015), <https://www.justice.gov/opa/file/767321/download> (last visited Feb. 3, 2020).

⁵⁴ S. 934.32(2), F.S.

⁵⁵ 442 U.S. 735 (1979).

a robbery victim. The Court held that there was no expectation of privacy in dialed telephone numbers, as they were voluntarily transmitted to the telephone company.⁵⁶

The Florida Supreme Court (FSC) considered a pen register and trap and trace order in *Tracey v. State*,⁵⁷ in which law enforcement obtained not only dialed numbers but real-time location information. Officers in *Tracey* applied for the numbers associated with incoming and outgoing calls; however, the phone company also provided real-time cell-site location information, which officers used to track Tracey's location and movements.⁵⁸ The FSC held that the real-time location tracking of Tracey through his cell phone was a search under the Fourth Amendment and therefore required either a warrant or an exception to the warrant requirement.

Mobile Tracking Devices

A mobile tracking device is an electronic or mechanical device, such as a GPS tracker, that tracks a person's or object's movement.⁵⁹ A court order issued under s. 934.42(2), F.S., authorizes a law enforcement officer to install a mobile tracking device to collect tracking and location information. Law enforcement must provide a statement to the court that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the investigating agency.⁶⁰ A certification of relevance is a lower standard than the probable cause standard required to obtain a warrant.

In 2012, the United States Supreme Court addressed mobile tracking devices in *United States v. Jones*.⁶¹ The Court held that installing a GPS tracking device on a vehicle without a warrant violated the Fourth Amendment as an unlawful search.⁶² Prior to the *Jones* decision, installation of a mobile tracking device was not considered a search when used to track a person's public movements.⁶³ As searches are generally per se unreasonable absent a warrant, the *Jones* decision requires a warrant, supported by probable cause, for installation of a mobile tracking unit.

Historical Cell Site Data

Cell phones connect to cell sites or base towers in order to make calls, send text messages, use data, and perform other functions.⁶⁴ These cell sites are located at fixed geographic locations. A phone connects to the cell site with the strongest available signal and may connect to different cell sites as it moves through a coverage area.⁶⁵ A phone company keeps a record of a phone's cell site connections for certain actions.⁶⁶ The data in these records can approximate a person's location, although it is possible for a cell site to have a coverage area of approximately 2,700 miles⁶⁷ and for a phone to connect to a tower other than the one closest to it.⁶⁸

In its 2018 *Carpenter v. United States*⁶⁹ decision, the United States Supreme Court held that law enforcement must secure a warrant, supported by probable cause, to access historical cell site data. In finding a reasonable expectation of privacy in these records, the Court noted:

⁵⁶ *Id.* at 742-44.

⁵⁷ 152 So.3d 504 (Fla. 2014).

⁵⁸ *Id.* at 507-508.

⁵⁹ S. 934.42, F.S.

⁶⁰ S. 934.42(2)(b), F.S.

⁶¹ 565 U.S. 400 (2012).

⁶² *Id.*

⁶³ *United States v. Knotts*, 460 U.S. 276 (1983).

⁶⁴ Center for the Advancement of Public Integrity, *Does Seeking Cell Site Location Information Require a Warrant? The Current State of Law in a Rapidly Changing Field* (August 1, 2016), http://www.law.columbia.edu/sites/default/files/microsites/public-integrity/files/does_seeking_cell_site_location_information_require_a_search_warrant_-_wesley_cheng_-_august_2016_update_0.pdf (last visited Feb. 3, 2020).

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 Richmond J.L. & Tech. 3 (2011), <http://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1354&context=jolt> (last visited Feb. 3, 2020).

⁶⁸ Center for the Advancement of Public Integrity, *supra* note 64.

⁶⁹ 138 S.Ct. 2206 (2018).

[There have been] seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.⁷⁰

However, current Florida statutes authorize law enforcement to obtain historical cell site data pursuant to a court order based only on specific and articulable facts showing that there are reasonable grounds to believe the records are relevant and material to an ongoing criminal investigation⁷¹ – a lower standard than probable cause.

Cell-Site Simulators

A cell-site simulator functions like a cellular tower.⁷² The simulator causes each cellular device within a certain radius to connect and transmit its standard unique identifying number to the simulator.⁷³ Law enforcement can use this capability to help locate a cell phone whose unique identifying number is known or to determine the unique identifier of a cell phone in the simulator's proximity.⁷⁴ A cell-site simulator provides only the relative signal strength and general direction of a target phone; it does not have the same capabilities as a GPS locator.⁷⁵

In 2015, the U.S. Department of Justice (USDOJ) issued written guidance on the use of a cell-site simulator. In this memorandum, USDOJ began requiring federal agencies to obtain a search warrant supported by probable cause in order to use a cell-site simulator.⁷⁶ The District of Columbia Court of Appeals,⁷⁷ U.S. District Court for Northern California,⁷⁸ and U.S. District Court for Southern New York⁷⁹ have held that use of a cell-site simulator constitutes a search under the Fourth Amendment, requiring either probable cause and a warrant or an exception to the warrant requirement.

Effect of Proposed Changes

Wiretapping and Stored Communications

CS/HB 1457 amends the definition of "oral communication" to explicitly include communications recorded by a "microphone-enabled device." The bill defines microphone-enabled device as a device, sensor, or other physical object within a residence:

- Capable of connecting to the Internet, directly or indirectly, or to another connected device;
- Capable of creating, receiving, accessing, processing, or storing electronic data or communications;
- That communicates with, by any means, another entity or individual; and
- That contains a microphone designed to listen for and respond to environmental cues.

By including communications recorded by a microphone-enabled device in the definition of oral communication, the bill ensures that communication intercepted through a microphone-enabled device is subject to Florida's wiretapping protections, including criminal penalties for those who violate the wiretapping statute and stringent requirements for law enforcement interception of such communication.

⁷⁰ *Id.* at 2219.

⁷¹ S. 934.23(5), F.S.

⁷² U.S. Department of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, at 1 (Sep. 3, 2015), <https://www.justice.gov/opa/file/767321/download> (last visited Feb. 3, 2020).

⁷³ *Id.* at 2.

⁷⁴ *Id.*

⁷⁵ *Id.*

⁷⁶ *Id.* at 3.

⁷⁷ *Jones v. U.S.*, Case No. 15-CF-322 (Sep. 21, 2017), <https://www.dccourts.gov/sites/default/files/2017-09/15-CF-322.pdf> (last visited Feb. 3, 2020).

⁷⁸ *U.S. v. Ellis*, Case No. 13-CR-00818, Pretrial Order No. 3 Denying Motions to Suppress (Aug. 24, 2017), <https://www.documentcloud.org/documents/3962321-Gov-UScourts-Cand-273044-337-0.html> (last visited Feb. 3, 2020).

⁷⁹ *U.S. v. Lambis*, Case No. 15cr734, Opinion and Order (Jul. 12, 2016), <https://www.documentcloud.org/documents/2992109-Pauley-Stingray-Opinion-7-12-16.html#document/p6/a307678> (last visited Feb. 3, 2020).

The bill provides an additional exception to unlawfully accessing stored communications when the access is for a legitimate business purpose and does not include personal information. The bill also clarifies that exceptions existing in current law for conduct authorized by the provider or user of a communications service may include services through cellular telephones, portable electronic communication devices, or microphone-enabled household devices.

The bill defines a portable communication device as an object:

- That may be easily transported or conveyed by a person;
- Is capable of creating, receiving, accessing, processing, or storing electronic data or communications; and
- Communicates with, by any means, another device, entity, or individual.

Location Tracking

The bill requires law enforcement to obtain a warrant to conduct real-time location tracking or acquire historical location data. The bill defines “real-time location tracking” as:

- Installing and using a mobile tracking device on the object to be tracked;
- Acquiring real-time cell-site location data; or
- Acquiring real-time precise global positioning system location data.

The bill defines historical location data as:

- Historical cell-site location data in the possession of a provider; and
- Historical precise global positioning systems location data in the possession of a provider.

If using a mobile tracking device, an officer must install the device within 10 days of the warrant’s issuance. Additionally, the bill places time constraints on how long a device may be used or real-time location data may be obtained, which must be specified in the warrant and may not exceed 45 days from the date of the warrant’s issuance. Upon a showing of good cause a court may grant one or more extensions, not to exceed 45 days. For real-time tracking methods, an officer must return the warrant to the issuing judge within 10 days of the specified tracking timeframe expiring. For historical location data, the warrant must specify a date range for the data sought, and the officer must return the warrant within 10 days of receiving the records. The court may seal the warrant upon a showing of good cause.

The bill imposes notice requirements for law enforcement real-time location tracking and acquisition of historical location data. Within 90 days after the surveillance timeframe specified in the warrant for real-time location tracking, the officer executing the warrant must serve a copy on the person whom, or whose property, law enforcement tracked. For acquisition of historical location data, the executing officer must serve a copy on the person within 90 days of receiving the records. An officer may serve this notice by delivering a copy to the person or leaving a copy at the person’s residence or usual place of abode with an individual of suitable age and discretion who lives there or by mailing a copy to the person’s last known address. Upon a showing a good cause by law enforcement, the court may postpone notice. Failure to timely return or serve the warrant would likely be considered a ministerial deficiency, requiring suppression of evidence only upon a showing of prejudice or deliberate disregard.

The bill allows for real-time location tracking before a warrant is issued if an emergency exists which:

- Involves immediate danger of death or serious physical injury to any person, the danger of escape of a prisoner, a missing person at risk of death or serious physical injury, or a call for emergency services from a cellular telephone;
- Requires the installation or use of a mobile tracking device before a warrant authorizing such installation or use can, with due diligence, be obtained; and
- There are grounds upon which a warrant could be issued to authorize the installation and use.

When tracking someone prior to a obtaining a warrant under this provision of the bill, law enforcement must terminate the surveillance when:

- The information sought is obtained;
- The application for the warrant is denied; or

- 48 hours have lapsed since the installation or use of the mobile tracking device began, whichever is earlier.

The bill provides an effective date of July 1, 2020.

B. SECTION DIRECTORY:

Section 1: Amends s. 934.01, F.S., relating to legislative findings.

Section 2: Amends s. 934.02, F.S., relating to definitions.

Section 3: Amends s. 934.21, F.S., relating to unlawful access to stored communications; penalties.

Section 4: Amends s. 934.42, F.S., relating to mobile tracking device authorization.

Section 5: Creates s. 934.44, F.S., relating to historical location data acquisition.

Section 6: Provides an effective date of July 1, 2020.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

None.

2. Expenditures:

None.⁸⁰

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

None.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. The bill does not appear to affect county or municipal governments.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

Not applicable.

⁸⁰ Florida Department of Law Enforcement, Agency Analysis of House Bill 1457, p. 3 (Nov. 13, 2019).
STORAGE NAME: h1457a.CRJ
DATE: 2/4/2020

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On February 3, 2020, the Criminal Justice Subcommittee adopted an amendment and reported the bill favorably as a committee substitute. The strike-all amendment:

- Retained current law requiring law enforcement obtain a court order, rather than a search warrant, prior to performing a wiretap.
- Added additional emergency circumstances where a real-time tracking device can be installed without first obtaining a warrant.
- Increased the time limit for law enforcement to notify a person who was tracked or whose historical location data was obtained from 10 days to 90 days.

This analysis is drafted to the committee substitute as passed by the Criminal Justice Subcommittee.