HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 1405 Searches of Cellular Phones and Other Electronic Devices
SPONSOR(S): Criminal Justice Subcommittee, Toledo
TIED BILLS: **IDEN./SIM. BILLS:**

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Criminal Justice Subcommittee	13 Y, 0 N, As CS	Bruno	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 1405 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; or
- Historical precise global positioning 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 10 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 grant one or more extensions of the notice requirement for up to 90 days upon law enforcement request.

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 does not appear to have a fiscal impact on state or local government.

The bill provides an effective date of July 1, 2019.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

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.

Searches of Cell Phones

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.[6]

In *Riley v. California*,[7] 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."[8] The Court reasoned that a modern smartphone's immense storage capacity allows it to carry tremendous quantity and variety of records regarding a person's private life, such as photographs, prescriptions, bank records, contacts, and videos.[9]

[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] *Chimel v. California*, 395 U.S. 752 (1969).
[7] 134 S.Ct. 2473 (2014).
[8] *Id.* at 2484.
[9] *Id.* at 2489.

Wiretapping and Stored Communications

By Law Enforcement

Wiretapping generally refers to electronic or mechanical eavesdropping on communications.[10] Law enforcement use of a wiretap is subject to Fourth Amendment protections under the United States Constitution.[11]

In Florida, a law enforcement officer may apply for an order authorizing the interception of wire, oral, or electronic communication.[12] 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 reasonably are 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.[13]

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.[14] 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.[15]

By the General Public

Florida law prohibits wiretapping by the general public.[16] Subject to exceptions, it is a third degree felony[17] 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;

[10] Black's Law Dictionary (10th ed. 2014), wiretapping.
[11] *Katz v. United States*, 389 U.S. 347 (1967).
[12] S. 934.09, F.S.
[13] *Id.*
[14] S. 934.07, F.S.
[15] S. 934.03(2)(a)3., F.S.
[16] S. 934.03, F.S.
[17] 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.

- 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.[18]

The penalty for wiretapping may be decreased to a misdemeanor[19] under the following circumstances:

- The person has no prior wiretapping offenses;
- The conduct was not done for 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.[20]

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.[21]

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.[22] If the offense was not committed for commercial advantage, malicious destruction or damage, or private commercial gain, it is a second degree misdemeanor.[23]

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 button.[24] 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.[25] The service provider remotely stores recordings from the devices for quality control.[26] Other devices, such as baby-monitors and home security systems, are always recording.[27]

---

[18] S. 934.03(1), F.S.
[19] 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.
[20] S. 934.03(4), F.S.
[21] S. 934.21(1), F.S.
[22] S. 934.21(2)(a), F.S.
[23] S. 934.21(2)(b), F.S.
[24] 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 Mar. 13, 2019).
[25] *Id.*
[26] 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 Mar. 13, 2019).
[27] Future of Privacy Forum, *supra.*

As these microphone-enabled devices grow in popularity, privacy concerns mount. A security expert recently demonstrated how an Amazon Echo might be hacked.[28] Additionally, prosecutors in Arkansas requested recordings possibly made by an Amazon Echo in a murder case.[29]

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.[30]

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.[31] 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.[32] Florida's definition of these terms are substantially similar to the definitions in the federal Pen Register Act.[33] 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.[34]

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.[35]

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*,[36] 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 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.[37]

The Florida Supreme Court (FSC) considered a pen register and trap and trace order in *Tracey v. State*,[38] 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

[28] 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 Mar. 13, 2019).
[29] Chavez, *supra.*
[30] *Tracey v. State*, 152 So.3d 504, 506 (Fla. 2014).
[31] S. 934.02(20), F.S.
[32] S. 934.02(21), F.S.
[33] 18 U.S.C. § 3127.
[34] 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 Mar. 13, 2019).
[35] S. 934.32(2), F.S.
[36] 442 U.S. 735 (1979).
[37] *Id.* at 742-44.
[38] 152 So.3d 504 (Fla. 2014).

phone company also provided real-time cell-site location information, which officers used to track Tracey's location and movements.[39] 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.[40] 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.[41] 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*.[42] The Court held that installing a GPS tracking device on a vehicle without a warrant violated the Fourth Amendment as an unlawful search.[43] 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.[44] 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.[45] 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.[46] A phone company keeps a record of a phone's cell site connections for certain actions.[47] 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 miles[48] and for a phone to connect to a tower other than the one closest to it.[49]

In its 2018 *Carpenter v. United States*[50] 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 these records, the Court noted:

> [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

[39] *Id.* at 507-508.
[40] S. 934.42, F.S.
[41] S. 934.42(2)(b), F.S.
[42] 565 U.S. 400 (2012).
[43] *Id.*
[44] *United States v. Knotts*, 460 U.S. 276 (1983).
[45] 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 Mar. 13, 2019).
[46] *Id.*
[47] *Id.*
[48] 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 Mar. 13, 2019).
[49] Center for the Advancement of Public Integrity, *supra.*
[50] 138 S.Ct. 2206 (2018).

> neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible.[51]

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 investigation[52] – a lower standard than probable cause.

Cell-Site Simulators

A cell-site simulator functions like a cellular tower.[53] The simulator causes each cellular device within a certain radius to connect and transmit its standard unique identifying number to the simulator.[54] 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.[55] 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.[56]

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.[57] The District of Columbia Court of Appeals,[58] U.S. District Court for Northern California,[59] and U.S. District Court for Southern New York[60] 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 1405 amends the definition of oral communication to explicitly include communication 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 communication 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.

---

[51] *Id.* at 2219.
[52] S. 934.23(5), F.S.
[53] 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 Mar. 13, 2019).
[54] *Id.* at 2.
[55] *Id.*
[56] *Id.*
[57] *Id.* at 3.
[58] *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 Mar. 13, 2019).
[59] *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 Mar. 13, 2019).
[60] *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 Mar. 13, 2019).

The bill provides an additional exception to unlawfully accessing stored communications when the access is:

- For a legitimate business purpose, and
- Of information that is not personally identifiable or that has been collected in such a way that prevents identification of the user of the device.

It 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.

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; or
- Historical precise global positioning 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 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 bill imposes notice requirements for law enforcement real-time location tracking and acquisition of historical location data. Within 10 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 10 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 good cause shown, the court may grant one or more 90-day postponements of the notice requirement upon law enforcement request.

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

- Involves immediate danger of death or serious physical injury to any person or the danger of escape of a prisoner; and
- 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 without 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, 2019.

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, 2019.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   None.

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 municipal or county governments.

2. Other:

   None.

B. RULE-MAKING AUTHORITY:

Not applicable.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On March 26, 2019, the Criminal Justice Subcommittee adopted one amendment and reported the bill favorably as a committee substitute. The amendment:

- Added a requirement that law enforcement obtain a warrant to acquire historical cell site location data.
- Separated statutory sections discussing real-time location tracking and acquiring historical location data for clarity.

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