The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Criminal Justice

BILL:	CS/SB 1256
INTRODUCER:	Criminal Justice Committee and Senator Brandes
SUBJECT:	Search of the Content, Information, and Communications of Cellular Phones, Portable Electronic Communication Devices, and Microphone-enabled Household Devices
DATE:	February 7, 2018 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Cellon	Jones	CJ	**Fav/CS**
2.			JU	
3.			RC	

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/SB 1256 amends Florida law to address privacy issues related to the use of communication technology. The bill amends ch. 934, F.S., by:

- Providing legislative intent;
- Defining the terms "portable electronic communication device" and "microphone-enabled household device";
- Changing the current definition of oral communication to include the use of a microphone-enabled household device;
- Amending the definition of a tracking device;
- Requiring a warrant for the installation and use of a tracking device;
- Setting forth time constraints under which a tracking device must be used and when notice must be provided to the person tracked;
- Allowing for emergency tracking under certain circumstances; and
- Prohibiting the intentional, unlawful access, without authorization, to a cellular phone, portable electronic communication device, or microphone-enabled household device when a person obtains wire, oral, or electronic communications stored within the device.

The bill is effective July 1, 2018.

II. Present Situation:

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 law 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.

Location Tracking

Cell phones, smartphones, laptops, and tablets are all mobile devices that can be located whenever they are turned on.[6] There are essentially three methods of locating a mobile device:

- *Network-based location* occurs when a mobile device communicates with nearby cell sites. The mobile device communicates through a process called registration even when the device is idle. The service provider of the mobile device[7] can also initiate the registration of a device. This information is stored in provider databases in order to route calls. The smaller the cell site, the more precise the location data.
- *Handset-based location* uses information transmitted by the device itself, such as global positioning system (GPS) data.
- *Third-party methods* facilitate real-time tracking of a mobile signal directly by using technology that mimics a wireless carrier's network.[8]

---

[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] Fla. Const. Art. 1, s. 12.
[6] Electronic Privacy Information Center, *Locational Privacy Issues*, available at https://epic.org/privacy/location/ (last visited January 30, 2018).
[7] A service provider is the company that provides the internet to the mobile device. *Id.*
[8] *Id.*

Mobile Tracking Devices

Mobile tracking devices can also be used to track a person's location. This broad category of devices includes radio frequency (RF)-enabled tracking devices (commonly referred to as "beepers"), satellite-based tracking devices, and cell-site tracking devices. Satellite-based tracking devices are commonly referred to as (GPS) devices.[9]

Florida law defines a "tracking device" as an electronic or mechanical device which permits the tracking of movement of a person or object.[10] Section 934.42, F.S., requires a law enforcement officer to apply to a judge for a *court order* approving the "installation and use of a mobile tracking device" and if the court grants the order, the officer installs and uses the device without the need for assistance. The application for such an order must include:

- A statement of the identity of the applicant and the identity of the law enforcement agency conducting the investigation.
- 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.
- A statement of the offense to which the information likely to be obtained relates.
- A statement whether it may be necessary to use and monitor the mobile tracking device outside the jurisdiction of the court from which authorization is being sought.[11]

The court then must review the application and if the court finds that the above requirements are met, the court will order the authorization of the installation and use of a mobile tracking device. The court is not allowed to require greater specificity or additional information then listed above.[12]

The installation and the monitoring of a mobile tracking device are governed by the standards established by the United State Supreme Court.[13]

Cellular-Site Location Data

There are currently 327.6 million cell phones in use in the United States and more than the 315 million people living in the United States.[14] As the cell phone travels, it connects to various cell phone towers, which means an electronic record of its location is created. The location record is held by the telecommunications company that services the device.[15]

Cellular-site location information (CSLI) is information that is created when a cell phone connects and identifies its location to a nearby cell tower that would process a phone call or text message made by the cell phone. CSLI can be "historic," which is the record of the phone's past

---

[9] *Where We Are with Location Tracking: A look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, Ian Herbert, Issue 16.2, (Fall 2011) available at http://www.bjcl.org/articles/16_2%20herbert_formatted.pdf (last visited February 3, 2018).
[10] Section 934.42(6), F.S.
[11] Section 934.42(2), F.S.
[12] Section 934.42(3) and (4), F.S.
[13] Section 934.42(5), F.S.
[14] Center for Democracy and Technology, *Location Data: The More They Know*, Mana Azarmi, November 27, 2017, available at https://cdt.org/blog/location-data-the-more-they-know/ (last visited January 31, 2016).
[15] *Id*.

movements, or it can be "real-time" or prospective, which is the information that reveals the phone's current location.[16] Historic CSLI enables law enforcement to piece together past events by connecting a suspect to the location of a past crime.[17] Prospective location information helps law enforcement trace the current whereabouts of a suspect.[18]

GPS Location Data

A cell phone's GPS capabilities allow it to be tracked to within 5 to 10 feet.[19] GPS provides users with positioning, navigation, and timing services based on data available from satellites orbiting the earth.[20] If a mobile device is equipped with GPS technology, significantly more precise location information is then sent from the handset to the carrier.[21]

Microphone-Enabled Household Devices

Smart speakers are devices that use voice-activated artificial intelligence technology to respond to commands. They are designed as virtual home assistants and intended to be used in as many different ways as possible. [22]

Although the term "always on" is often used to describe smart speakers, this is not entirely accurate. Speech activated devices use the power of energy efficient processors to remain in an inert state of passive processing, or "listening," for the "wake words." The device buffers and re-records locally, without transmitting or storing any information, until it detects the word or phrase that triggers the device to begin actively recording and transmitting audio outside of the device to the service provider. [23]

Chapter 934, F.S., Security of Communications Definitions

Florida law governing security of communications is found in ch. 934, F.S. Among the subjects covered in the chapter are procedures related to, and limitations upon, the government's use of

---

[16] *Id*.
[17] National Association of Criminal Defense Lawyers, *Cell Phone Location Tracking*, available at https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf (last visited January 30, 2018).
[18] *Id*.
[19] *Id*.
[20] GPS.gov, *GPS Location Privacy*, last modified August 22, 2017, available at https://www.gps.gov/policy/privacy (last visited January 30, 2018).
[21] EE Times, *How does a GPS tracking system work?*, Patrick Bertagna, October 26, 2010 available at https://www.eetimes.com/document.asp?doc_id=1278363&page_number=2 (last visited January 30, 2018). Note that cell phone service providers were required by the Federal Communications Commission in 1996 to begin providing location data to 911 operators for a program called Enhanced 911 (E911) which ultimately required a high level of handset location accuracy. As a result, many cell service providers began putting GPS chips inside the handsets. *See* Herbert, *Where We are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, Berkeley Journal of Criminal Law, Volume 16, Issue 2, (2011).
[22] NextAdvisor, *Smart Speakers and Voice Recognition: Is Your Privacy at Risk?*, Jocelyn Baird, April 4, 2017, available at https://www.nextadvisor.com/blog/2017/04/04/smart-speakers-and-voice-recognition-is-your-privacy-at-risk/ (last visited February 1, 2018).
[23] *Id*.; *See also* The Future of Privacy Forum, *Always On: Privacy Implications Of Microphone-Enabled Devices*, Stacey Gray, April 2016, available at https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf (last visited February 1, 2018).

wiretapping or interception, and tracking devices. This chapter closely mirrors the federal statutory law found in the Electronic Communications Privacy Act of 1986.[24]

Definitions provided in the chapter that are pertinent to the bill are as follows:

- "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications or communications affecting intrastate, interstate, or foreign commerce.[25]
- "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, interstate, or foreign commerce, but does not include:
  - Any wire or oral communication;
  - Any communication made though a tone paging device;
  - Any communication from an electronic or mechanical device which permits the tracking of the movement of a person or an object; or
  - Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.[26]
- "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation does not mean any public oral communication uttered at a public meeting or any electronic communication.[27]
- "Intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.[28]
- "Contents" when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.[29]
- "Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, electronic, or oral communication other than any telephone or telegraph instrument, equipment, or facility, or any component thereof:
  - Furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or
  - Being used by a provider of wire or electronic communications service in the ordinary course of its business or by an investigative or law enforcement officer in the ordinary course of her or his duties.[30]
- "Investigative or law enforcement officer" means any officer of the State of Florida or political subdivision thereof, of the United States, or of any other state or political

[24] 18 U.S.C. 2510-3127.
[25] Section 934.02(1), F.S.
[26] Section 934.02(12), F.S.
[27] Section 934.02(2), F.S.
[28] Section 934.02(3), F.S.
[29] Section 934.02(7), F.S.
[30] Section 934.02 (4), F.S.

subdivision thereof, who is empowered by law to conduct on behalf of the Government investigations of, or to make arrests for, offenses enumerated in this chapter or similar federal offenses, any attorney authorized by law to prosecute or participate in the prosecution of such offenses, or any other attorney representing the State of Florida or political subdivision thereof in any civil, regulatory, disciplinary, or forfeiture action relating to, based upon, or derived from such offenses.[31]

Stored Communications

Florida law also prohibits accessing stored communications. It is unlawful for a person to:
- Intentionally access a facility through which an electronic communication service is provided; or
- Intentionally exceed an authorization to access; and
- Obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system.[32]

The penalties for this offense vary based on the specific intent and the number of offenses.[33] It is a first degree misdemeanor[34] if the above described offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain.[35] Any subsequent offense with this intent is a third degree felony.[36]

If the person did not have the above described intent then the above described offense is a second degree misdemeanor.[37]

III. Effect of Proposed Changes:

Legislative Findings for Chapter 934, F.S. (Section 1)

The bill amends s. 934.01, F.S., by adding the term "electronic" to the current terminology of "wire and oral" communications in the legislative findings.

The bill also creates new legislative findings:
- Recognizing a subjective and objectively reasonable expectation of privacy in precise location data. As such, the law enforcement collection of the precise location of a person, cellular phone, or portable electronic communication device[38] without the consent of the device owner should be allowed only when authorized by a warrant issued by a court and should remain under the control and supervision of the authorizing court.

[31] Section 934.02(6), F.S.
[32] Section 934.21(1), F.S.
[33] *See* s. 934.21(2), F.S.
[34] A first degree misdemeanor is punishable by up to one year in jail and up to a $1,000 fine. Sections 775.082 and 775.083, F.S.
[35] Section 934.21(2), F.S.
[36] A third degree felony is punishable by up to five years imprisonment and up to a $5,000 fine. Sections 775.082, 775.083, and 775.084, F.S.
[37] A second degree misdemeanor is punishable by up to 60 days in county jail and up to a $500 fine. Sections 775.082 and 775.083, F.S.
[38] The term "portable electronic communication device" is defined in Section 3 of the bill.

- Recognizing that the use of portable electronic devices is growing at a rapidly increasing rate. These devices can store, and encourage the storage of, an almost limitless amount of personal and private information. Further recognizing that these devices are commonly used to access personal and business information and other data stored in computers and servers that can be located anywhere in the world. Recognizing a person who uses a portable electronic device has a reasonable and justifiable expectation of privacy in the information contained in the portable electronic device.
- Recognizing that microphone-enabled household devices[39] often contain microphones that listen for and respond to environmental triggers. Further recognizing that these devices are generally connected to and communicate through the Internet, resulting in the storage of and accessibility of daily household information in a device itself or in a remote computing service. Finding that an individual should not have to choose between using household technological enhancements and conveniences or preserving the right to privacy in one's home.

Chapter 934, F.S., Security of Communications Definitions (Section 2)

The bill amends s. 934.02, F.S., by amending a current definition, and creating new definitions:

- The current definition of "oral communication" is amended to include the use of a *microphone-enabled device*.
- The definition of "microphone-enabled household device" is created and is defined 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;
  - Which communicates with, by any means, another device, entity, or individual; and
  - Which contains a microphone designed to listen for and respond to environmental cues.
- The definition of "portable electronic communication device" is created and is defined as an object capable of being easily transported or conveyed by a person which is capable of creating, receiving, accessing, or storing electronic data or communications and which communicates with, by any means, another device, entity, or individual.

Stored Communications (Section 3)

The bill creates new misdemeanor offenses by prohibiting a person who intentionally and unlawfully accesses, without authorization, a cellular phone, portable electronic communication device, or microphone-enabled household device and thereby obtains wire, oral, or electronic communications stored within them. The bill provides that the penalties for these offenses are the same as the other offenses for unlawfully accessing stored communications. These penalties also vary based on the specific intent and the number of offenses committed.

It is a first degree misdemeanor if the above described offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain. Any subsequent offense with this intent is a third degree felony.

[39] The term "microphone-enabled household device" is defined in Section 3 of the bill.

If the person did not have the above described intent then the above described offense is a second degree misdemeanor.

Location Tracking (Section 4)

The bill expands the scope of s. 934.42, F.S., to include the cellular-site location data, precise global positioning satellite location data, and historical global positioning satellite location data.

Specifically, s. 934.42, F.S., amends the definition for a "tracking device" to create a definition of a "mobile tracking device" or "tracking device." A "mobile tracking device" or "tracking device" is defined to mean any electronic or mechanical device, including a cellular phone or a portable electronic communication device, which allows the tracking of the movement of a person or object and may be used to access cellular-site location data, precise global positioning satellite location data, and historical global positioning satellite data.

The bill also amends s. 934.42, F.S., to require a *warrant* rather than a *court order* for the law enforcement officer to install and use a mobile tracking device or to acquire cellular-site location data, precise global positioning satellite location data, or historical global positioning satellite data.

The bill requires that the application for a *warrant* must set forth a reasonable length of time that the mobile tracking device may be used. The time may not exceed 45 days after the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each.

The bill requires the court to find probable cause in the required application statements in granting of a warrant for the use of a mobile tracking device or tracking device. The warrant must also require the officer to complete any authorized installation within a specified timeframe after the warrant is issued, to be no longer than 10 days. Within 10 days after the use of the tracking device has ended, the officer executing the warrant must return the warrant to the judge.

Also, within 10 days after the use of the tracking device has ended, the officer executing the warrant must serve a copy of it on the person who was tracked or whose property was tracked. Upon request by the law enforcement agency, the court may delay notice for a period of 90 days.

The bill requires that, in addition to the United States Supreme Court, standards established by Florida courts apply to the installation, use, or monitoring of any mobile tracking device as authorized by s. 934.42, F.S.

The bill also allows for the installation of a mobile tracking device without 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;
- 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 such installation or use.[40]

Within 48 hours after the installation or use has occurred or begins to occur, a warrant approving the installation or use must be issued in accordance with s. 934.42, F.S. If an application for the warrant is denied, or when 48 hours have lapsed since the installation or use of the mobile tracking device began, whichever is earlier a law enforcement officer must immediately terminate the installation or use of a mobile tracking device.

The bill is effective July 1, 2018.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The Florida Department of Law Enforcement does not expect any fiscal impact from this bill.[41]

VI. Technical Deficiencies:

None.

[40] This exception is similar to that found in s. 934.09(7), F.S.
[41] The Florida Department of Law Enforcement, *2018 Legislative Bill Analysis*, January 4, 2018 (on file with the Senate Committee on Criminal Justice).

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 934.01, 934.02, 934.21, and 934.42.

IX. Additional Information:

A. Committee Substitute – Statement of Substantial Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS by Criminal Justice on February 6, 2018:
The committee substitute:

- Defines the terms "portable electronic communication device" and "microphone-enabled household device";
- Changes the current definition of oral communication to include the use of a microphone-enabled household device;
- Amends the definition of a tracking device;
- Requires a warrant for the installation and use of a tracking device;
- Sets forth time constraints under which a tracking device must be used and when notice must be provided to the person tracked;
- Allows for emergency tracking under certain circumstances;
- Removes the requirement of a warrant instead of a court order for the interception of a wire, oral, or electronic communication; and
- Removes the misdemeanor the bill created for a person intentionally and unlawfully accessing a cell phone, portable electronic communication device, or microphone-enabled household device.

B. Amendments:

None.