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:	SB 210
INTRODUCER:	Senator Brandes
SUBJECT:	Searches of Cellular Phones and Other Electronic Devices
DATE:	February 8, 2019
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Cellon	Jones	CJ	**Pre-meeting**
2.			JU	
3.			RC	

I. Summary:

SB 210 amends ch. 934, F.S., relating to security of communications, to address privacy issues related to the use of communication technology and the contents of stored electronic communications.

The bill amends ch. 934, F.S., by:
- Providing legislative intent;
- Defining the terms "portable electronic communication device" and "microphone-enabled household device";
- Amending the 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 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; and
- Allowing for emergency tracking under certain circumstances.

The bill is effective July 1, 2019.

II. Present Situation:

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]

[1] U.S. CONST. AMEND. IV.

Under Fourth Amendment jurisprudence, a search occurs whenever the government intrudes upon an area in which a person has a reasonable expectation of privacy, such as one's home.[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] The Florida Constitution also explicitly protects against the "unreasonable interception of private communications by any means."[6]

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 the persons or things to be seized.[7]

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.[8]

Advancing Technology - Location Tracking

Cell phones, smartphones, laptops, and tablets are all mobile devices that can be located whenever they are turned on.[9] There are essentially three methods of locating a mobile device:

- *Network-based location*, which occurs when a mobile device communicates with nearby cell sites. The mobile device communicates through a process called registration even when the

[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. I, s. 12.
[6] "No warrant shall be issued except upon probable cause, supported by affidavit, particularly describing the place or places to be searched, the person or persons, thing or things to be seized, the communication to be intercepted, and the nature of evidence to be obtained". *Id*.
[7] *Id*. and *supra*, n. 1.
[8] *See also United States v. Jones*, 565 U.S. 400 (2012), where, in a 5-4 decision the Court found (in a narrow holding eschewing the "reasonable expectation of privacy" analysis most often used by the Court) that attaching a GPS real-time tracker on the suspect's vehicle for the purpose of tracking his whereabouts was a "trespass" upon his "effects" by the Government and therefore a warrant is required; *Smallwood v. State*, 113 So.3d 724, 741 (Fla. 2013), in which the Court, in what it called a decision "narrowly limited to the legal question and facts with which we were presented," decided that for a search incident to arrest of the contents of a suspect's cell phone, a warrant is required if there are no search incident to arrest justifications (officer protection or evidence preservation) for searching the contents; *Tracey v. State*, 152 So.3d 504 (Fla. 2014), is a case involving real-time cell site location information, where the Court determined that the use of Tracey's cell site location information to track him in real-time was a search for which probable cause was required. (Further, the Court held that the exclusionary rule was not applicable under the facts of the case therefore the evidence derived from the real-time tracking should be excluded as evidence in the case.); *Carpenter v. United States*, 138 S.Ct. 2206 (2018), found that obtaining a court order, rather than a warrant requiring a showing of probable cause, to access historical cell-site records implicates the Fourth Amendment therefore the Government will generally need a warrant.
[9] *Locational Privacy, Cell Phone Tracking Methods*, Electronic Privacy Information Center, available at https://epic.org/privacy/location (last viewed February 5, 2019).

device is idle. The service provider of the mobile device[10] 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*, which uses information transmitted by the device itself, such as global positioning system (GPS) data.
- *Third-party methods*, which facilitate real-time tracking of a mobile signal directly by using technology that mimics a wireless carrier's network.[11]

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."[12]

Florida law defines a "tracking device" as an electronic or mechanical device which permits the tracking of movement of a person or object.[13] 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."[14] If the court grants the order, the officer installs and uses the device.[15] 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; and
- 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.[16]

The court then must review the application and if it finds that the above-described 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 the information listed above.[17]

The installation and the monitoring of a mobile tracking device are governed by the standards established by the United States Supreme Court.[18]

---

[10] A service provider is the company that provides the internet to the mobile device. *Id.*
[11] *Id.*
[12] Ian Herbert, *Where We are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, Berkley J. of Crim. Law, Vol. 16, Issue 2, p. 442, n. 1 (Fall 2011), available at http://www.bjcl.org/articles/16_2%20herbert_formatted.pdf (last viewed February 5, 2019).
[13] Section 934.42(6), F.S.
[14] Section 934.42(1)-(2), F.S.
[15] Section 934.42(3), F.S.
[16] Section 934.42(2), F.S.
[17] Section 934.42(3) and (4), F.S.
[18] Section 934.42(5), F.S.

Cellular-Site Location Data

In the United States, it has been reported that there are 327.6 million cell phones in use, which is more than the current U.S. population (315 million people).[19] "As the cell phone travels, it connects to various cell phone towers, which means an electronic record of its location is created[.]"[20] The cell phone's location record is held by the telecommunications company that services the device.[21]

Cellular-site location information (CSLI) is information generated when a cell phone connects and identifies its location to a nearby cell tower that, in turn, processes the phone call or text message made by the cell phone. "CSLI can be 'historic,' in which case the record is of a cell phone's past movements, or it can be 'real-time' or prospective, in which case the information reveals the phone's current location."[22] Historic CSLI enables law enforcement to piece together past events by connecting a suspect to the location of a past crime.[23] Real-time location information helps law enforcement trace the current whereabouts of a suspect.[24]

GPS Location Data

A cell phone's GPS capabilities allow it to be tracked to within 5 to 10 feet.[25] GPS provides users with positioning, navigation, and timing services based on data available from satellites orbiting the earth.[26] If a mobile device is equipped with GPS technology, significantly more precise location information is then sent from the handset to the carrier.[27]

Microphone-Enabled Household Devices

Another emerging technology raising privacy concerns is the smart speaker. Smart speakers, like the Google Home[28] or Amazon Echo,[29] are devices that use voice-activated artificial intelligence

---

[19] Mana Azarmi, *Location Data: The More They Know*, Center for Democracy and Technology (November 27, 2017), available at https://cdt.org/blog/location-data-the-more-they-know/ (last viewed February 5, 2019).
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Cell Phone Location Tracking*, National Association of Criminal Defense Lawyers, available at https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf (last viewed February 5, 2019).
[24] *Id.*
[25] *Id.*
[26] *GPS Location Privacy*, GPS.gov (October 31, 2018), available at https://www.gps.gov/policy/privacy (last viewed February 5, 2019).
[27] Patrick Bertagna, *How does a GPS tracking system work?* (October 26, 2010), EE Times, available at https://www.eetimes.com/document.asp?doc_id=1278363&page_number=2 (last viewed February 5, 2019). 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. *Supra*, n. 11.
[28] *Google Home*, Google Store, available at https://store.google.com/product/google_home (last viewed February 5, 2019).
[29] *Echo & Alexa*, Amazon, available at https://www.amazon.com/all-new-amazon-echo-speaker-with-wifi-alexa-dark-charcoal/dp/B06XCM9LJ4 (last viewed February 5, 2019).

technology to respond to commands. They are designed as virtual home assistants and intended to be used in as many different ways as possible.[30]

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.[31]

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

Several definitions in ch. 934, F.S., are pertinent to the bill:

- "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.[32]
- "Electronic communication" means the 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. The definition does not include: any wire or oral communication; any communication made through a tone-only 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.[33]
- "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.[34]
- "Electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.[35]
- "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

[30] Jocelyn Baird, *Smart Speakers and Voice Recognition: Is Your Privacy at Risk?*, NextAdvisor (April 4, 2017), available at https://www.nextadvisor.com/blog/2017/04/04/smart-speakers-and-voice-recognition-is-your-privacy-at-risk/ (last viewed February 5, 2019).
[31] *Id*. *See also* Stacey Gray, *Always On: Privacy Implications Of Microphone-Enabled Devices*, The Future of Privacy Forum (April 2016), available at https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf (last viewed February 5, 2019).
[32] Section 934.02(7), F.S.
[33] Section 934.02(12), F.S.
[34] Section 934.02(15), F.S.
[35] Section 934.02(14), F.S.

    - 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.[36]
- "Electronic storage" means any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, and any storage of a wire or electronic communication by an electronic communication service for purposes of backup protection of such communication.[37]
- "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.[38]
- "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 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 or political subdivision thereof in any civil, regulatory, disciplinary, or forfeiture action relating to, based upon, or derived from such offenses.[39]
- "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 and does not mean any public oral communication uttered at a public meeting or any electronic communication.[40]
- "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.[41]
- "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.[42]

Prohibited Access to 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.[43]

[36] Section 934.02(4), F.S.
[37] Section 934.02(17), F.S.
[38] Section 934.02(3), F.S.
[39] Section 934.02(6), F.S.
[40] Section 934.02(2), F.S.
[41] Section 934.02(19), F.S.
[42] Section 934.02(1), F.S.
[43] Section 934.21(1), F.S.

The penalties for this offense vary based on the specific intent and the number of offenses.[44] It is a first degree misdemeanor[45] if the above described offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain.[46] Any subsequent offense with this intent is a third degree felony.[47] If the person did not have the above-described intent then the above-described offense is a second degree misdemeanor.[48]

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 real-time cell-site location data, real-time precise GPS location data, and historical precise GPS location data. As such, the law enforcement collection of the precise location of a person, cellular phone, or portable electronic communication device[49] 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.
- 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[50] 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.

[44] *See* s. 934.21(2), F.S.
[45] A first degree misdemeanor is punishable by up to one year in jail, a fine of up $1,000, or both. Sections 775.082 and 775.083, F.S.
[46] Section 934.21(2), F.S.
[47] A third degree felony is punishable by up to 5 years in state prison, a fine of up to $5,000, or both. Sections 775.082 and 775.083, F.S.
[48] A second degree misdemeanor is punishable by up to 60 days in county jail, a fine of up to $500, or both. Sections 775.082 and 775.083, F.S.
[49] The term "portable electronic communication device" is defined in Section 2 of the bill.
[50] The term "microphone-enabled household device" is defined in Section 2 of the bill.

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 household 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.

Penalties for Accessing Stored Communications (Section 3)

The bill amends s. 934.21, F.S., to make conforming changes and clarifies that the penalty for accessing a facility through which an electronic communication service is provided without authorization to obtain, alter, or prevent authorized access to a wire or electronic communication does not apply to conduct authorized:

- By the provider[51] or user[52] of wire, oral, or electronic communications services through cellular phones, portable electronic communication devices, or microphone-enabled household devices;
- Under ch. 933, F.S.;[53] or
- For legitimate business purposes that do not identify the user.

Location Tracking (Section 4)

The bill creates new definitions related to location tracking in s. 934.42, F.S. The bill provides that:

- "Mobile tracking device" means an electronic or mechanical device that permits the tracking of a person's or an object's movements.
- "Real-time location tracking" means the:
  - Installation and use of a mobile tracking device on the object to be tracked;
  - Acquisition of real-time cell-site location data; or
  - Acquisition of real-time precise GPS location data.
- "Historical location data" means historical precise GPS location data in the possession of a provider.

[51] Section 934.21(3)(a), F.S.
[52] Section 934.21(3)(b), F.S.
[53] Chapter 933, F.S., authorizes search and inspection warrants.

The bill also amends s. 934.42, F.S., to require a *warrant* rather than a *court order* for the law enforcement officer to engage in real-time location tracking or to acquire historical location data in the possession of a provider. This means that law enforcement must meet the higher standard of having probable cause for purposes of a warrant rather than the lower standard of having a reasonable, articulable suspicion.

The bill requires that the application for a warrant set forth a reasonable length of time that the mobile tracking device may be used or the location data may be obtained in real-time. This time period may not exceed 45 days from the date the warrant is issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. When seeking historical location data the applicant must specify a date range for the data sought.

If the court issues a warrant, the warrant must also require the officer to complete any authorized installation within a specified timeframe no longer than 10 days. A warrant that permits the use of a mobile tracking device must be returned to the issuing judge within 10 days of the time period specified in the warrant ending. Additionally, a warrant authorizing the collection of historical GPS data must be returned to the issuing judge within 10 days after receiving the records.

Also, within 10 days after the use of the tracking device has ended or the historical location has been received from the service provider, the officer executing the warrant must serve a copy of the warrant on the person who was tracked, whose property was tracked, or whose historical location data was received.[54] Upon a showing of good cause for postponement, the court may grant a postponement of this notice in 90 day increments.

The bill requires that, in addition to the United States Supreme Court standards, 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 real-time tracking 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 real-time tracking before a warrant authorizing such tracking can, with due diligence, be obtained; and if
- There are grounds upon which a warrant could be issued to authorize the real-time tracking.[55]

Within 48 hours after the tracking has occurred or begins to occur, a warrant approving the real-time tracking must be issued in accordance with s. 934.42, F.S. When an application for a warrant is denied, when the information sought has been obtained, or when 48 hours have lapsed since the tracking began, whichever is earlier, the tracking must be terminated immediately.

The bill is effective July 1, 2019.

[54] Service may be accomplished by delivering a copy to the person who, or whose property, was tracked or data obtained; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address.
[55] This exception is similar to that found in s. 934.09(7), F.S., related to intercepting wire, oral, or electronic communication.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The Florida Department of Law Enforcement anticipates no fiscal impact to the department resulting from the bill.[56]

It is unknown at this time whether local law enforcement agencies will experience a fiscal impact resulting from this bill.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

[56] The Florida Department of Law Enforcement, *2019 Legislative Bill Analysis, SB 210* (January 7, 2019) (on file with the Senate Committee on Criminal Justice).

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

None.

B. Amendments:

None.