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 210
INTRODUCER:	Criminal Justice Committee and Senator Brandes
SUBJECT:	Searches of Cellular Phones and Other Electronic Devices
DATE:	February 13, 2019 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 210 amends chs. 933 and 934, F.S., relating to search warrants and the 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. 933, F.S., by:

- Codifying the Constitutional provision that extends the security against unreasonable searches or seizures to the interception of private communications by any means; and
- Expanding the reasons for law enforcement to obtain a search warrant to include the content within certain communication devices.

The bill amends ch. 934, F.S., by:

- Providing legislative intent;
- Defining the terms "portable electronic communication device," "microphone-enabled household device," "mobile tracking device," "real-time location tracking," and "historical location data";
- Amending the definition of oral communication to include the use of a microphone-enabled household device;
- Requiring a search warrant for the interception of wire, oral, or electronic communications, or 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;

- Allowing for emergency tracking or the interception of oral communications under certain circumstances; and
- Clarifying that certain conduct relating to access to stored communications is not a criminal offense.

The bill also reenacts certain sections in ch. 934, F.S.

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]

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 search 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]

---

[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. 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

Chapter 933, F.S., 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.[9]

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."[10] The application must particularly describe the place to be searched and the person and thing to be seized.[11] If the judge finds that probable cause exists for the issuance of the search warrant the judge must issue the search warrant.[12]

The grounds for the issuance of a search warrant include:
- When the 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;
- 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 of the laws prohibiting the manufacture, sale, and transportation of intoxicating liquors;
  - In violation of the fish and game laws;
  - In violation of the laws relative to food and drug; or
  - In violation of the laws relative to citrus disease pursuant to s. 581.184, F.S.; or
- When the 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.[13]

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."[14] Section 933.18, F.S., limits the grounds for the issuance of a search warrant for a private

---

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] Sections 933.01- 933.19, F.S.

[10] Section 933.06, F.S.

[11] Section 933.04, F.S.

[12] Section 933.07, F.S.

[13] Section 933.02(1)-(5), F.S.

[14] Section 933.02, F.S.

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 in violation of s. 784.049, F.S., is contained therein.[15]

After a law enforcement officer executes a search warrant, he or she must then bring the property seized and any person arrested in connection with the property before the judge or another court having jurisdiction of the offense.[16] A copy of the search warrant and an inventory of any property seized during the execution of the warrant must either be delivered to the person whose property is the subject of the search warrant, or may be left upon the premises if no one is there.[17] The search warrant and a sworn copy of any required inventory must be returned to the judge.[18]

Chapter 934 - Security of Communications – Interception of Wire, Oral, or Electronic Communications

Sections 934.03-934.09, F.S., govern the interception of wire, oral, or electronic communications. “Intercept” is defined as 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.[19] These sections of law are patterned after federal law, and address the relationships

[15] Section 933.18, F.S.
[16] Section 933.07(1), F.S.
[17] Section 933.11, F.S.
[18] Section 933.12, F.S.
[19] Section 934.02(3), F.S.

between citizens, communications service providers, and investigative and law enforcement officers with respect to the obtainment and use of wire, oral, or electronic communications.[20]

Intentionally intercepting another person's wire, oral, or electronic communication is generally prohibited under s. 934.03, F.S. However, under circumstances where a communications service provider is served with a court order, the service provider is allowed to provide information, facilities, or technical assistance to a person who is authorized to intercept wire, oral, or electronic communications.[21] If a person's wire or oral communications are intercepted under circumstances not permitted in ss. 934.03-934.09, F.S., none of the content or evidence derived from the content may be used as evidence.[22]

The Governor, Attorney General, statewide prosecutor, or any state attorney can authorize a law enforcement agency to apply to a judge for a court order permitting the interception of wire, oral, or electronic communications.[23] Intercepting the communication is authorized when the interception may provide or has provided evidence of the commission of the crimes enumerated in s. 934.07(1), F.S.[24]

Section 934.09, F.S., contains the procedures related to the interception of wire, oral, or electronic communications. The procedures include what the application for a court order for the interception must contain, the time limitations for the interception, extensions of time, notice to the person whose communication has been intercepted, and special procedures in emergency situations.

To issue an order authorizing the interception, a court must determine that there is probable cause for belief that an individual is committing, has committed, or is about to commit an offense as listed in s. 934.07, F.S., and that there is probable cause for belief that particular communications concerning that offense will be obtained through such interception.[25]

---

[20] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. s. 2510-22. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications. *See* U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Justice Information Sharing, Privacy & Civil Liberties*, available at https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285 (last viewed February 12, 2019).

[21] Section 934.03(2)(a), F.S.

[22] The content of the wire or oral communications or evidence derived from the content may not be admitted as evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the state, or a political subdivision thereof. Section 934.06, F.S.

[23] Section 934.07(1), F.S.

[24] The crimes are murder, kidnapping, aircraft piracy, arson, gambling, robbery, burglary, theft, dealing in stolen property, criminal usury, bribery, or extortion; any felony violation of ss. 790.161-790.166, F.S. (offenses for destructive devices); inclusive; any violation of s. 787.06, F.S. (human trafficking); any violation of ch. 893, F.S. (drug abuse prevention and control); any violation of the provisions of the Florida Anti-Fencing Act; any violation of ch. 895, F.S., (offenses concerning racketeering and illegal debts); any violation of ch. 896, F.S. (offenses related to financial transactions); any violation of ch. 815, F.S. (computer-related crimes); any violation of ch. 847, F.S. (offenses related to obscenity); any violation of s. 827.071. F.S. (sexual performance by a child); any violation of s. 944.40, F.S. (offenses related to escape); or any conspiracy or solicitation to commit any violation of the laws of this state relating to the crimes listed.

[25] Section 934.09(3), F.S.

Section 934.10, F.S., contains the civil remedies available to a person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of ss. 934.03-934.09, F.S.

Advancing Technology - Location Tracking

Cell phones, smartphones, laptops, and tablets are all mobile devices that can be located whenever they are turned on.[26] 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 device is idle. The service provider of the mobile device[27] 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.[28]

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."[29]

Florida law defines a "tracking device" as an electronic or mechanical device which permits the tracking of movement of a person or object.[30] 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."[31] If the court grants the order, the officer installs and uses the device.[32] 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.[33]

---

[26] *Locational Privacy, Cell Phone Tracking Methods*, Electronic Privacy Information Center, available at https://epic.org/privacy/location (last viewed February 5, 2019).
[27] A service provider is the company that provides the internet to the mobile device. *Id.*
[28] *Id.*
[29] 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).
[30] Section 934.42(6), F.S.
[31] Section 934.42(1)-(2), F.S.
[32] Section 934.42(3), F.S.
[33] Section 934.42(2), F.S.

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.[34]

The installation and the monitoring of a mobile tracking device are governed by the standards established by the United States Supreme Court.[35]

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).[36] "As the cell phone travels, it connects to various cell phone towers, which means an electronic record of its location is created[.]"[37] The cell phone's location record is held by the telecommunications company that services the device.[38]

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."[39] Historic CSLI enables law enforcement to piece together past events by connecting a suspect to the location of a past crime.[40] Real-time location information helps law enforcement trace the current whereabouts of a suspect.[41]

GPS Location Data

A cell phone's GPS capabilities allow it to be tracked to within 5 to 10 feet.[42] GPS provides users with positioning, navigation, and timing services based on data available from satellites orbiting the earth.[43] If a mobile device is equipped with GPS technology, significantly more precise location information is then sent from the handset to the carrier.[44]

---

[34] Section 934.42(3) and (4), F.S.
[35] Section 934.42(5), F.S.
[36] 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).
[37] *Id*.
[38] *Id*.
[39] *Id*.
[40] *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).
[41] *Id*.
[42] *Id*.
[43] *GPS Location Privacy*, GPS.gov (October 31, 2018), available at https://www.gps.gov/policy/privacy (last viewed February 5, 2019).
[44] 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.

Microphone-Enabled Household Devices

Another emerging technology raising privacy concerns is the smart speaker. Smart speakers, like the Google Home[45] or Amazon Echo,[46] 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.[47]

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.[48]

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.[49]
- "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.[50]
- "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.[51]
- "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.[52]

---

[45] *Google Home*, Google Store, available at https://store.google.com/product/google_home (last viewed February 5, 2019).
[46] *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).
[47] 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).
[48] *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).
[49] Section 934.02(7), F.S.
[50] Section 934.02(12), F.S.
[51] Section 934.02(15), F.S.
[52] Section 934.02(14), F.S.

- "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.[53]
- "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.[54]
- "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.[55]
- "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.[56]
- "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.[57]
- "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.[58]
- "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.[59]

[53] Section 934.02(4), F.S.
[54] Section 934.02(17), F.S.
[55] Section 934.02(3), F.S.
[56] Section 934.02(6), F.S.
[57] Section 934.02(2), F.S.
[58] Section 934.02(19), F.S.
[59] Section 934.02(1), F.S.

Prohibited Access to Stored Communications

Under certain circumstances, Florida law 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.[60]

The penalties for this offense vary based on the specific intent and the number of offenses.[61] It is a first degree misdemeanor[62] if the above described offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain.[63] Any subsequent offense with this intent is a third degree felony.[64] If the person did not have the above-described intent then the above-described offense is a second degree misdemeanor.[65]

III. Effect of Proposed Changes:

Chapter 933, F.S., Search Warrants (Sections 1 and 2)

The bill amends s. 933.02, F.S., to incorporate content held within a cellular phone, portable electronic communication device, or microphone-enabled household device as among the grounds upon which a search warrant may be issued by a judge, if the content constitutes evidence relevant to proving that a felony has been committed.

Section 933.04, F.S., is amended to add the constitutional provision found in Article I, section 12 of the Constitution of Florida that protects private communications from unreasonable interception just as persons, houses, and effects are protected from unreasonable searches and seizures.

Legislative Findings for Chapter 934, F.S. (Section 3)

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

[60] Section 934.21(1), F.S.
[61] *See* s. 934.21(2), F.S.
[62] 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.
[63] Section 934.21(2), F.S.
[64] 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.
[65] 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.

phone, or portable electronic communication device[66] 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[67] 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 4)

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.

Interception of Wire, Oral, or Electronic Communications (Sections 5 – 9)

Section 5: The bill amends s. 934.03(2)(a), F.S., to require a search warrant, rather than a court order, for a law enforcement officer authorized by law to intercept wire, oral, or electronic communications to obtain information, facilities, or technical assistance from a wire, oral, or electronic communication service provider.

[66] The term "portable electronic communication device" is defined in Section 2 of the bill.
[67] The term "microphone-enabled household device" is defined in Section 2 of the bill.

Section 6: Section 934.06, F.S., currently prohibits the use of intercepted wire or oral communication as evidence if the disclosure of that information would violate a provision of ch. 934, F.S. The bill adds the content of a cellular phone, microphone-enabled household device, or portable electronic communication device to this prohibition, and requires a search warrant to obtain that content. The bill also specifically provides that the communication may be used as evidence if the communication is lawfully obtained under circumstances where a search warrant is not required.

Section 7: The bill amends s. 934.07(1) and (2), F.S., to require a search warrant, rather than a court order, for the interception of wire, oral, or electronic communications.

Section 8: The bill amends the procedures found in s. 934.09, F.S., for intercepting the contents of wire, oral, or electronic communications to require that a judge issue a search warrant, rather than a court order. This section retains the procedure an investigative or law enforcement officer would currently follow to by-pass obtaining a search warrant for up to 48 hours under certain emergency circumstances.

Section 9: The bill retains current law relating to the civil remedies available to a person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of ss. 934.03-934.09, F.S., while replacing the terms court order, subpoena, and legislative authorization with the term search warrant.

Penalties for Accessing Stored Communications (Section 10)

The bill amends s. 934.21, F.S., to clarify 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[68] or user[69] of wire, oral, or electronic communications services through cellular phones, portable electronic communication devices, or microphone-enabled household devices;
- Under ch. 933, F.S.;[70] or
- For legitimate business purposes that do not identify the user.

Location Tracking (Section 11)

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.

[68] Section 934.21(3)(a), F.S.
[69] Section 934.21(3)(b), F.S.
[70] Chapter 933, F.S., authorizes search and inspection warrants.

- "Historical location data" means historical precise GPS location data in the possession of a provider.

The bill also amends s. 934.42, F.S., to require a search warrant rather than a court order for an investigative or 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 an investigative or law enforcement officer must meet the higher standard of having probable cause for purposes of a search warrant rather than the lower standard of having a reasonable, articulable suspicion.

The bill requires that the application for a search 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 search 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 search warrant, the search warrant must also require the investigative or law enforcement officer to complete any authorized installation within a specified time-frame no longer than 10 days. A search 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 search warrant ending. Additionally, a search 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 investigative or law enforcement officer executing the search warrant must serve a copy of the search warrant on the person who was tracked, whose property was tracked, or whose historical location data was received.[71] 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 retains current provisions for real-time tracking without a search 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.[72]

[71] 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.
[72] This exception is similar to that found in s. 934.09(7), F.S., related to intercepting wire, oral, or electronic communication.

Within 48 hours after the tracking has occurred or begins to occur, a search warrant approving the real-time tracking must be issued in accordance with s. 934.42, F.S. When an application for a search 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.

Sections 12 – 17

Sections 12-17 of the bill reenact ss. 934.22, 934.23, 934.24, 934.25, 934.27, and 934.28, F.S., to incorporate the changes made by the act.

The bill is effective July 1, 2019.

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.[73]

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.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 933.02, 933.04, 934.01, 934.02, 934.03, 934.06, 934.07, 934.08, 934.09, 934.10, 934.21, and 934.42.

The bill reenacts the following sections of Florida Statutes: 934.22, 934.23, 934.24, 934.25, 934.27, and 934.28.

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 11, 2019:
The Committee Substitute:

- Amends s. 933.02, F.S., to require a search warrant for the content in certain communication devices if such content constitutes evidence relevant to proving a felony has been committed.
- Codifies in s. 933.04, F.S., the provision in Art. I, s. 12 of the State Constitution that extends the security against unreasonable searches or seizures to the interception of private communications by any means.
- Requires a search warrant for the interception of wire, oral, or electronic communications in ch. 934, F.S.
- Requires a search warrant for a law enforcement officer to obtain information, facilities, or technical assistance from a wire, oral, or electronic communication service provider under certain circumstances.
- Amends s. 934.06, F.S., which currently prohibits the use of intercepted wire or oral communication as evidence if the disclosure of that information would violate a provision of ch. 934, F.S.

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

- Sets forth time constraints under which a tracking device must be used and when notice must be provided to the person tracked.
- Provides for emergency tracking or the interception of oral communications without a search warrant under certain circumstances.
- The bill reenacts ss. 934.22, 934.23, 934.24, 934.25, 934.27, and 934.28, F.S.

B. Amendments:

None.