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 Rules

BILL:	CS/CS/SB 1256
INTRODUCER:	Judiciary Committee; 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 21, 2018 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Cellon	Jones	CJ	**Fav/CS**
2.	Tulloch	Cibula	JU	**Fav/CS**
3.	Cellon	Phelps	RC	**Pre-meeting**

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/SB 1256 amends Florida law to address privacy issues related to the use of communication technology, such as cell phones, laptops, and tablets. These devices may be equipped with location tracking technology which allows the service provider to track the device whenever it is on.

Most notably, the bill amends ch. 934, F.S. to replace the requirement for a court order supported by a reasonable articulable suspicion to install and use a tracking device with a requirement for a warrant supported by the higher probable cause standard to install and use a tracking device. Similarly, the bill requires law enforcement agencies to obtain a warrant to acquire data identifying the location of a person's cellular phone or portable electronic communications device from the person's service provider.

Other specific changes made by the bill to chapter 934, F.S., include:

- Defining the terms "portable electronic communication device" and "microphone-enabled household device";
- Amending the definition of a tracking device to create a definition for a "mobile tracking device";
- Setting forth time constraints under which a tracking device must be used and when notice must be provided to the person tracked;
- Providing a postponement of notice may only be granted by a court for good cause; and

- Allowing for emergency tracking under certain circumstances

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, 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] Both the Florida and federal constitutions require a warrant to be supported by probable cause, as established by oath or affirmation, and to particularly describe the place to be searched and items or people to be seized.[6]

In the seizure or arrest context, three levels of warrantless citizen encounters with law enforcement officers are generally recognized:
(1) Consensual encounter, where a citizen may either comply or ignore a law enforcement officer's request and is free to leave;[7]
(2) Investigatory or *Terry*[8] stop, where an officer reasonably detains a citizen temporarily based on a "well-founded, articulable suspicion of criminal activity;"[9] and
(3) Arrest, "which must be supported by probable cause that a crime has been or is being committed."[10]

In the communications context, a warrant supported by probable cause is generally required to obtain the contents of a telephone conversation; whereas, information published to a third party generally is not protected by the Fourth Amendment. In *Smith v. Maryland*, the United States Supreme Court held that because "telephone users have no reasonable expectations of privacy in dialed telephone numbers recorded through pen registers and contained in the third-party

[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] *Id.*; *see* n. 1, *supra*.
[7] *Popple v. State*, 626 So. 2d 185, 186 (Fla. 1993).
[8] *Terry v. Ohio*, 392 U.S. 1, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968).
[9] *Popple* at 186.
[10] *Id.*

telephone company's records," the use of a pen register did not constitute a "search" under the Fourth Amendment.[11]

However, advancing technology, particularly the ability to track the location of a person through his or her cellphone, has presented law enforcement with new means of investigation and surveillance. This advancing technology has also led to greater protections over information conveyed to cell service providers. The Stored Communications Act requires the government to obtain a court order based on the *Terry* standard, i.e., a reasonable, articulable suspicion that a crime may be occurring, before obtaining cell phone records.[12] But some information contained in the records obtained under a court order has presented the courts with new questions about the Fourth Amendment implications of this technology.

Advancing Technology - Location Tracking

Cell phones, smartphones, laptops, and tablets are all mobile devices that can be located whenever they are turned on.[13] 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[14] 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.[15]

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.[16]

Florida law defines a "tracking device" as an electronic or mechanical device which permits the tracking of movement of a person or object.[17] 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

[11] *United States v. Davis*, 785 F.3d 498, 507 (11th Cir. 2015) (citing *Smith v. Maryland*, 442 U.S. 735, 742-46 (1979)).
[12] 18 U.S.C. § 2703(d). *See also, id.* at 505, explaining that "[w]hile this statutory standard is less than the probable cause standard for a search warrant, the government is still required to obtain a court order and present to a judge specific and articulable facts showing reasonable grounds to believe the records are relevant and material to an ongoing criminal investigation."
[13] Electronic Privacy Information Center, *Cell Phone Tracking Methods*, https://epic.org/privacy/location/ (last visited Feb. 11 2018).
[14] A service provider is the company that provides the internet to the mobile device. *Id.*
[15] *Id.*
[16] Ian Herbert, *Where We are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, BERKELEY J. OF CRIM. LAW, Vol. 16, Issue 2, 442, n. 1 (Fall 2011), http://www.bjcl.org/articles/16_2%20herbert_formatted.pdf (last visited Feb. 11, 2018).
[17] Section 934.42(6), F.S.

tracking device."[18] If the court grants the order, the officer installs and uses the device.[19] 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.[20]

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.[21]

The installation and the monitoring of a mobile tracking device are governed by the standards established by the United State Supreme Court.[22]

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).[23] "As the cell phone travels, it connects to various cell phone towers, which means an electronic record of its location is created[.]"[24] The cell phone's location record is held by the telecommunications company that services the device.[25]

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, processed 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."[26] Historic CSLI enables law enforcement to piece together past events by connecting a suspect to the location of a past crime.[27] Prospective location information helps law enforcement trace the current whereabouts of a suspect.[28]

---

[18] Section 934.42(1)-(2), F.S.
[19] Section 934.42(3), F.S
[20] Section 934.42(2), F.S.
[21] Section 934.42(3) and (4), F.S.
[22] Section 934.42(5), F.S.
[23] Mana Azarmi, *Location Data: The More They Know*, Center for Democracy and Technology (Nov. 27, 2017), https://cdt.org/blog/location-data-the-more-they-know/ (last visited Feb. 11, 2018).
[24] *Id*.
[25] *Id*.
[26] *Id*.
[27] National Association of Criminal Defense Lawyers, *Cell Phone Location Tracking*, https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf (last visited Feb. 11, 2018).
[28] *Id*.

GPS Location Data

A cell phone's GPS capabilities allow it to be tracked to within 5 to 10 feet.[29] GPS provides users with positioning, navigation, and timing services based on data available from satellites orbiting the earth.[30] If a mobile device is equipped with GPS technology, significantly more precise location information is then sent from the handset to the carrier.[31]

Developing Fourth Amendment Implications of Location Tracking Technology

In the 2012 case of *U.S. v. Jones*, the United States Supreme Court considered the issue of whether GPS tracking of a criminal suspect's vehicle was a search under the Fourth Amendment.[32] Noting first that a motor vehicle is an "effect" under the Fourth Amendment, the Supreme Court held that the government's installation and use of a GPS[33] tracking device on a suspect's vehicle constituted a "search."[34] As noted in *Jones*,

> It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.[35]

In 2014, the Florida Supreme Court decided *Tracey v. State*, involving law enforcement's use of real-time cell phone location data. [36] In that case, law enforcement was conducting surveillance on a suspected drug dealer, and had applied for and received a court order to install a "pen register" and "trap and trace device" on the defendant's cell phone. Although not specifically requested in the application or authorized by the order, the defendant's cell phone provider also provided real time cell site location information.[37] After receiving a tip from a confidential informant one evening, law enforcement used real time cell site location data to find the defendant and discovered he had a kilogram brick of cocaine hidden in the spare tire wall of his vehicle.[38] The defendant moved to suppress the evidence on the basis that the police should have obtained a warrant before using his real time cell site location to find him.[39]

---

[29] *Id.*
[30] GPS.gov, *GPS Location Privacy*, last modified August 22, 2017, available at https://www.gps.gov/policy/privacy (last visited January 30, 2018).
[31] 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).
[32] 565 U.S. 400, 404 (2012) (citing *United States v. Chadwick,* 433 U.S. 1, 12 (1977)).
[33] GPS is the acronym for "global positioning system." *Id.*. at 402.
[34] *Id.* at 404 (citing *United States v. Chadwick,* 433 U.S. 1, 12 (1977)).
[35] *Id.* at 404-05.
[36] 152 So. 3d 504, 525-26 (2014).
[37] *Id.* at 506-07.
[38] *Id.* at 507. The person the defendant was meeting had $23,000 cash on him. *Id.*
[39] *Id.* at 508.

The Florida Supreme Court agreed with the defendant in *Tracey* and held that a person has an expectation of privacy in his or her real-time cell site location data which society is prepared to recognize as a reasonable under the Fourth Amendment.[40] The Florida Supreme Court concluded that cell phones are "effects" under the Fourth Amendment, and reasoned that because users of cell phones, especially smart phones, often keep these devices on their person, tracking the location of these devices may breach the walls of the user's home, showing the location of the person within their home.[41] "This real risk of 'inadvertent' violation of Fourth Amendment rights is not a risk worth imposing on the citizenry when it is not an insurmountable task for the government to obtain a warrant based on probable cause when such tracking is truly justified."[42] Thus, in *Tracey*, the evidence of cocaine trafficking was suppressed.

In 2015, the First District Court of Appeal in *Herring v. State* applied the holding in *Tracey* to a case in which real time cell site location data was used to track down a murderer within five hours of shooting two victims.[43] The First District noted that exigent circumstances were present based on the belief that the defendant was still armed, because the defendant had recently killed one person and attempted to kill another, and because delay in apprehending the defendant may jeopardize the safety of both law enforcement and the public.[44] While such exigent circumstances would ordinarily relieve law enforcement from the duty of obtaining a warrant, the First District panel held that under the totality of the circumstances, the officers had plenty of time, 2.5 hours, to obtain a warrant before tracking the defendant's real time cell site location. Thus, the First District held that law enforcement had not overcome the warrant requirement under the circumstances.[45]

Recently, the United States Supreme court heard oral arguments in the case of *Carpenter v. United States*.[46] In the underlying case under review, *U.S. v. Carpenter*,[47] the Sixth Circuit held that the government had not conducted a "search" under the Fourth Amendment by obtaining historic cell tower location data as part of the business records obtained from the defendant's wireless cell phone carrier. The business records were obtained pursuant to a court order under the Stored Communications Act.[48] The Sixth Circuit reasoned that the defendant had no expectation of privacy in his cell tower location data for Fourth Amendment purposes, because "the federal courts have long recognized a core distinction: although the content of personal communications is private, the information necessary to get those communications from point A to point B is not."[49]

---

[40] *Id.*
[41] *Id.* at 524 (noting that cell phones and "smart phones" have "become virtual extensions of many of the people using them for all manner of necessary and personal matters.").
[42] *Id.*
[43] 168 So. 3d 240, 241-42 (2015).
[44] *Id.* at 243.
[45] *Id.* at 243-44. *Compare United States v. Caraballo*, 831 F.3d 95, 104 (2d Cir. 2016) (holding that officers' warrantless pinging of the defendant's cell phone was justified under the exigent circumstances exception in part because the defendant, who had just brutally killed a victim execution style, was still likely armed and on the loose).
[46] Supreme Court of the United States, Transcripts of November 29, 2017 oral argument, *Carpenter v. State*, No. 16-402, https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_3f14.pdf (last visited Feb. 11, 2018).
[47] *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).
[48] *See infra*, p. 8.
[49] *Carpenter*, 819 F.3d at 886.

The Eleventh Circuit in *U.S. v. Davis* similarly held that the defendant, who was using old technology and *not* a smart phone equipped with GPS, did not have a reasonable expectation of privacy in his phone records transmitted to a third party, his cell phone provider, particularly where the government did not obtain recordings of conversations.[50] The records in *Davis* were obtained by the government pursuant to a court order under the Stored Communications Act. As explained by the Eleventh Circuit, "[t]he Fourth Amendment prohibits *unreasonable* searches, not warrantless searches,"[51] and:

> [T]raditional Fourth Amendment analysis supports the reasonableness of the § 2703(d) [Stored Communications Act] order in this particular case. . . .
> . . . .
> [A] § 2703(d) court order functions as a judicial subpoena, but one which incorporates additional privacy protections that keep any intrusion minimal. The SCA guards against the improper acquisition or use of any personal information theoretically discoverable from such records. . . . Under § 2703(d), investigative authorities may not request such customer-related records merely to satisfy prurient or otherwise insubstantial governmental interests. Instead, a neutral and detached magistrate must find, based on "specific and articulable facts," that there are "reasonable grounds to believe" that the requested records are "relevant and material to an ongoing criminal investigation." Such protections are sufficient to satisfy "the primary purpose of the Fourth Amendment," which is "to prevent arbitrary invasions of privacy." *Brock v. Emerson Elec. Co., Elec. & Space Div.*, 834 F.2d 994, 996 (11th Cir.1987); *see, e.g., Terry v. Ohio*, 392 U.S. 1, 21, 88 S.Ct. 1868, 20 L.Ed.2d 889 n.18, 392 U.S. 1, 88 S.Ct. 1868, 1880 n. 18, 20 L.Ed.2d 889 (1968) (explaining that the "demand for specificity in the information upon which police action is predicated is the central teaching of this Court's Fourth Amendment jurisprudence").[52]

Microphone-Enabled Household Devices

Another emerging technology raising privacy concerns is the smart speaker. Smart speakers, like the Google Home[53] or Amazon Echo,[54] 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.[55]

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

[50] *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015).
[51] *Id.* at 516 (emphasis added).
[52] *Id.* at 517 (citation omitted). A petition for certiorari review has been filed in the United States Supreme Court.
[53] Google Home, https://store.google.com/product/google_home (last visited Feb. 11, 2018).
[54] Amazon, Echo & Alexa, https://www.amazon.com/all-new-amazon-echo-speaker-with-wifi-alexa-dark-charcoal/dp/B06XCM9LJ4 (last visited Feb. 11, 2018).
[55] Jocelyn Baird, *Smart Speakers and Voice Recognition: Is Your Privacy at Risk?*, NextAdvisor (Apr. 4, 2017), https://www.nextadvisor.com/blog/2017/04/04/smart-speakers-and-voice-recognition-is-your-privacy-at-risk/ (last visited February 11, 2018).

phrase that triggers the device to begin actively recording and transmitting audio outside of the device to the service provider. [56]

In one ongoing murder investigation in Arkansas, the victim died during a party at the suspect's home. The suspect owned an Amazon Echo, which other guests remembered was on and playing music. A law enforcement agency sought the information recorded by the suspect's Echo on the night of the victim's death, but Amazon initially refused to turn the information over on First Amendment privacy grounds. Ultimately, it appears the suspect has given Amazon permission to turn the recordings over to the law enforcement agency.[57]

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 wiretapping or interception, and tracking devices. This chapter closely mirrors the federal statutory law found in the Electronic Communications Privacy Act of 1986.[58]

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.[59]
- "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.[60]
- "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.[61]

[56] *Id*.; *See also* Stacey Gray, *Always On: Privacy Implications Of Microphone-Enabled Devices*, The Future of Privacy Forum (Apr. 2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf (last visited Feb. 11, 2018).
[57] Eliott C. McLaughlin, *Suspect OKs Amazon to hand over Echo recordings in murder case*, CNN, Apr. 26, 2017 https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html (last visited February 11, 2018).
[58] 18 U.S.C. 2510 et seq.
[59] Section 934.02(1), F.S.
[60] Section 934.02(12), F.S.
[61] Section 934.02(2), F.S.

- "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.[62]
- "Contents" when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.[63]
- "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.[64]
- "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 of Florida or political subdivision thereof in any civil, regulatory, disciplinary, or forfeiture action relating to, based upon, or derived from such offenses.[65]

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.[66]

The penalties for this offense vary based on the specific intent and the number of offenses.[67] It is a first degree misdemeanor[68] if the above described offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain.[69] Any subsequent offense with this intent is a third degree felony.[70]

[62] Section 934.02(3), F.S.
[63] Section 934.02(7), F.S.
[64] Section 934.02(4), F.S.
[65] Section 934.02(6), F.S.
[66] Section 934.21(1), F.S.
[67] *See* s. 934.21(2), F.S.
[68] 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.
[69] Section 934.21(2), F.S.
[70] 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.

If the person did not have the above described intent then the above described offense is a second degree misdemeanor.[71]

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 three legislative findings. First, in accord with the Florida Supreme Court's holding in *Tracey*, the bill adds a legislative finding recognizing that a person has a subjective expectation of privacy in his or her precise location data that is objectively reasonable.

As such, a law enforcement agency's collection of the precise location of a person, cellular phone, or portable electronic communication device[72] 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.

Second, the bill adds a legislative finding recognizing that the use of portable electronic devices, which can store almost limitless amounts of personal or private data, is growing rapidly. Portable electronic devices can be used to access personal and business information and other data stored in computers and servers located anywhere in the world. Given the nature of the information that can be contained in a portable electronic device, the legislature recognizes that a person using such a device has a reasonable and justifiable expectation of privacy in the information contained in that device.

Third, the bill adds a legislative finding recognizing that microphone-enabled household devices,[73] a new piece of technology being marketed to consumers, often contain microphones that listen for and respond to environmental triggers. These devices are generally connected to and communicate through the Internet, resulting in the storage of and accessibility of daily household information in either the device itself or in a remote computing service. In recognition of the private data such a device could transmit or store, the bill recognizes 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*.

[71] 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.
[72] The term "portable electronic communication device" is defined in Section 2 of the bill, *infra*.
[73] The term "microphone-enabled household device" is defined in Section 2 of the bill, *infra*.

- 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 makes 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[74] or user[75] of wire, oral, or electronic communications services through cellular phones, portable electronic communication devices, or microphone-enabled household devices;
- Under chapter 933;[76] or
- For legitimate business purposes that do not identify the user.

Location Tracking (Section 4)

The bill amends the definition for a "tracking device" in s. 934.42, F.S. to create the 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 which permits the tracking of a person's movements. Such devices are defined to include a cellular phone or a portable electronic communication device that can be used to access real time 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. 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 for purposes of obtaining a court order under the federal Stored Communications Act.

The bill requires that the application for a *warrant* 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

[74] Section 934.21(3)(a), F.S.
[75] Section 934.21(3)(b), F.S.
[76] Chapter 933 authorizes search and inspection warrants.

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 a warrant for the use of a tracking device or mobile tracking device. If the court issues a warrant, 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. Additionally, when the warrant authorizes the collection of historical global positioning satellite data, the officer that executed the warrant must return it to the judge within 10 days after receiving the records.

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 a showing of good cause for postponement, the court may grant a postponement of notice in 90 day increments.

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.[77]

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.[78]

The bill is effective July 1, 2018.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

[77] This exception is similar to that found in s. 934.09(7), F.S.
[78] It appears this provision overrules the *Herring* case.

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.[79]

VI. Technical Deficiencies:

None.

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/CS by Judiciary on February 13, 2018:
The Committee Substitute:

- Eliminating penalty and violation provisions which may subject police officers to criminal penalties when a warrantless search is subsequently deemed illegal under the Fourth Amendment.

[79] The Florida Department of Law Enforcement, *2018 Legislative Bill Analysis*, January 4, 2018 (on file with the Senate Committee on Criminal Justice).

- Provides that a law enforcement officer must return a warrant to the judge for records of a subscriber's historical global positioning data within 10 days of receiving the records.
- Requires that a law enforcement officer show good cause before the court can grant a postponement in providing notice of the warrant's existence to the person being tracked.
- Makes various technical changes.

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.