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 1256
INTRODUCER:	Senator Brandes
SUBJECT:	Search of the Content, Information, and Communications of Cellular Phones, Portable Electronic Communication Devices, and Microphone-enabled Household Devices
DATE:	February 5, 2018 REVISED:

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

I. Summary:

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

- Providing legislative intent;
- Creating new definitions and amending current definitions in ss. 934.02 and 934.42, F.S.;
- Providing that a court may issue a warrant based upon probable cause for a law enforcement officer to intercept a wire, oral, or electronic communication;
- Providing that a court may issue a warrant based upon probable cause for a law enforcement officer to obtain cellular-site location data, precise global positioning satellite location data, or historical global positioning satellite data;
- Allowing for emergency location tracking under certain circumstances;
- Setting forth time constraints under which location tracking must terminate and that notice must be provided to the person or entity tracked; and
- Prohibiting the intentional, unlawful access, without authorization, to a cellular phone, portable electronic communication device, or microphone-enabled household device when a person obtains wire, oral, or electronic communications stored within the device.

The bill also amends s. 92.605, F.S., to specify that in criminal cases the content of any electronic communication sought from a Florida business or out-of-state corporation be obtained under the provisions in ch. 934, F.S.

The bill is effective July 1, 2018.

II. Present Situation:

Fourth Amendment

The Fourth Amendment of the United States Constitution guarantees:

- The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures shall not be violated; and
- No warrants shall issue without probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

Under Fourth Amendment jurisprudence, a search occurs whenever the government intrudes upon an area in which a person has a reasonable expectation of privacy.[2] A warrantless search is generally per se unreasonable,[3] unless an exception to the warrant requirement applies.[4]

The Florida Constitution similarly protects the people against unreasonable searches and seizures, and that right is construed in conformity with the Fourth Amendment of the U.S. Constitution.[5] Both the Florida and federal constitutions law require a warrant to be supported by probable cause, as established by oath or affirmation, and to particularly describe the place to be searched and items or people to be seized.

Advancing technology has presented law enforcement with new means of investigation and surveillance, and the courts with new questions about the Fourth Amendment implications of this technology.

Searches of Cell Phones

An exception to the warrant requirement is a search incident to arrest, which allows law enforcement to perform a warrantless search of an arrested person, and the area within the arrestee's immediate control, in the interest of officer safety, and to prevent escape and the destruction of evidence.[6]

In *Riley v. California*,[7] the U.S. Supreme Court held that law enforcement must obtain a search warrant to search the digital contents of a cell phone seized incident to arrest. The Court considered the advanced capabilities of modern cell phones and noted that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[8] The Court reasoned that a modern smartphone's immense storage capacity allows that phone to carry a tremendous quantity and

[1] U.S. CONST. AMEND. IV.
[2] *Katz v. United States*, 389 U.S. 347 (1967).
[3] *United States v. Harrison*, 689 F.3d 301, 306 (3d Cir.2012).
[4] Examples of exceptions to the warrant requirement include exigent circumstances, searches of motor vehicles, and searches incident to arrest.
[5] Fla. Const. Art. 1, s. 12.
[6] *Chimel v. California*, 395 U.S. 752 (1969).
[7] 134 S.Ct. 2473 (2014).
[8] *Id.* at 2484.

variety of records regarding a person's private life, such as photographs, prescriptions, bank records, contacts, and videos.[9]

Location Tracking

Cell phones, smartphones, laptops, and tablets are all mobile devices that can be located whenever they are turned on.[10] There are essentially three methods of locating a mobile device:

- *Network-based location* occurs when a mobile device communicates with nearby cell sites. The mobile device communicates through a process called registration even when the device is idle. The service provider of the mobile device[11] can also initiate the registration of a device. This information is stored in provider databases in order to route calls. The smaller the cell site, the more precise the location data.
- *Handset-based location* uses information transmitted by the device itself, such as global positioning system (GPS) data.
- *Third-party methods* facilitate real-time tracking of a mobile signal directly by using technology that mimics a wireless carrier's network.[12]

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.[13]

Florida law defines a "tracking device" as an electronic or mechanical device which permits the tracking of movement of a person or object.[14] Section 934.42, F.S., requires a law enforcement officer to apply to a judge for a *court order* approving the "installation and use of a mobile tracking device" and if the court grants the order, the officer installs and uses the device without the need for assistance. The application for such an order must include:

- A statement of the identity of the applicant and the identity of the law enforcement agency conducting the investigation.
- A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the investigating agency.
- A statement of the offense to which the information likely to be obtained relates.
- A statement whether it may be necessary to use and monitor the mobile tracking device outside the jurisdiction of the court from which authorization is being sought.[15]

---

[9] *Id.* at 2489.
[10] Electronic Privacy Information Center, *Locational Privacy Issues*, available at https://epic.org/privacy/location/ (last visited January 30, 2018).
[11] A service provider is the company that provides the internet to the mobile device. *Id.*
[12] *Id.*
[13] *Where We Are with Location Tracking: A look at the Current Technology and the Implications on Fourth Amendment Jurisprudence*, Ian Herbert, Issue 16.2, (Fall 2011) available at http://www.bjcl.org/articles/16_2%20herbert_formatted.pdf (last visited February 3, 2018).
[14] Section 934.42(6), F.S.
[15] Section 934.42(2), F.S.

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.[16]

The installation and the monitoring of a mobile tracking device are governed by the standards established by the United State Supreme Court.[17]

Cellular-Site Location Data

There are currently 327.6 million cell phones in use in the United States and more than the 315 million people living in the United States.[18] As the cell phone travels, it connects to various cell phone towers, which means an electronic record of its location is created. The location record is held by the telecommunications company that services the device.[19]

Cellular-site location information (CSLI) is information that is created when a cell phone connects and identifies its location to a nearby cell tower that would process a phone call or text message made by the cell phone. CSLI can be "historic," which is the record of the phone's past movements, or it can be "real-time" or prospective, which is the information that reveals the phone's current location.[20] Historic CSLI enables law enforcement to piece together past events by connecting a suspect to the location of a past crime.[21] Prospective location information helps law enforcement trace the current whereabouts of a suspect.[22]

GPS Location Data

A cell phone's GPS capabilities allow it to be tracked to within 5 to 10 feet.[23] GPS provides users with positioning, navigation, and timing services based on data available from satellites orbiting the earth.[24] If a mobile device is equipped with GPS technology, significantly more precise location information is then sent from the handset to the carrier.[25]

---

[16] Section 934.42(3) and (4), F.S.
[17] Section 934.42(5), F.S.
[18] Center for Democracy and Technology, *Location Data: The More They Know*, Mana Azarmi, November 27, 2017, available at https://cdt.org/blog/location-data-the-more-they-know/ (last visited January 31, 2016).
[19] *Id*.
[20] *Id*.
[21] National Association of Criminal Defense Lawyers, *Cell Phone Location Tracking*, available at https://www.law.berkeley.edu/wp-content/uploads/2015/04/2016-06-07_Cell-Tracking-Primer_Final.pdf (last visited January 30, 2018).
[22] *Id*.
[23] *Id.*
[24] GPS.gov, *GPS Location Privacy*, last modified August 22, 2017, available at https://www.gps.gov/policy/privacy (last visited January 30, 2018).
[25] 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).

Microphone-Enabled Household Devices

Smart speakers are devices that use voice-activated artificial intelligence technology to respond to commands. They are designed as virtual home assistants and intended to be used in as many different ways as possible. [26]

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. [27]

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.[28]

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.[29]
- "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.[30]

[26] NextAdvisor, *Smart Speakers and Voice Recognition: Is Your Privacy at Risk?*, Jocelyn Baird, April 4, 2017, available at https://www.nextadvisor.com/blog/2017/04/04/smart-speakers-and-voice-recognition-is-your-privacy-at-risk/ (last visited February 1, 2018).
[27] *Id*.; *See also* The Future of Privacy Forum, *Always On: Privacy Implications Of Microphone-Enabled Devices*, Stacey Gray, April 2016, available at https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf (last visited February 1, 2018).
[28] 18 U.S.C. 2510-3127.
[29] Section 934.02(1), F.S.
[30] Section 934.02(12), F.S.

- "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.[31]
- "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.[32]
- "Contents" when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.[33]
- "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.[34]
- "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.[35]

Interception and Disclosure of Wire, Oral, or Electronic Communications

Florida law generally prohibits the interception and disclosure of wire, oral, or electronic communications.[36] However there are some exceptions for law enforcement and an electronic communications services provider and other specified persons.

Law Enforcement

Only the Governor, the Attorney General, the statewide prosecutor, or any state attorney may authorize an application to the court for an order authorizing the interception of, wire, oral or electronic communications.[37]

[31] Section 934.02(2), F.S.
[32] Section 934.02(3), F.S.
[33] Section 934.02(7), F.S.
[34] Section 934.02 (4), F.S.
[35] Section 934.02(6), F.S.
[36] Section 934.03, F.S.
[37] Section 934.07(1), F.S.

The following criteria must be met for the court to grant an *order* authorizing an interception:

- There is *probable cause* for the belief that an individual is committing, has committed, or is about to commit an offense provided in s. 934.07, F.S.;[38]
- There is *probable cause* for the belief that particular communications concerning that offense will be obtained through such interception;
- Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and
- There is *probable cause* for the belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person. [39]

Interception under the order may occur for 30 days and the court can extend the order for an additional 90 days upon application for an extension.[40]

The applications and orders granted for the interception of a wire, oral, or electronic communication are sealed by the judge and only disclosed upon a showing of good cause.[41]

The contents of any intercepted wire, oral, or electronic communication or evidence derived therefrom cannot be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding unless each party, not less than *10 days before* the trial, hearing, or proceeding, has been furnished with a copy of the court order and accompanying application under which the interception was authorized or approved. This 10-day period may be waived by the judge if he or she finds that it was not possible to furnish the party with the above information 10 days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

The contents of any wire, oral, or electronic communication intercepted must, if possible, be recorded on tape or wire or other comparable device. This recording must be kept in such a way to protect the recording from editing or other alterations. Duplicate recordings may be made for use or disclosure in other investigations.[42]

Wire, Oral, or Electronic Communication Service Provider and Others Exception

An officer, employee or agent of a wire, oral, or electronic communication service provider, landlord, custodian or other person may provide information, facilities or technical assistance to a person who is authorized by law to intercept wire, oral, or electronic communications if he or she has been provided with a:

---

[38] The offenses enumerated in s. 934.07, F.S., include: 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., inclusive; any violation of s. 787.06, F.S.; any violation of ch. 893, F.S.; any violation of the provisions of the Florida Anti-Fencing Act; any violation of ch. 895, F.S.; any violation of ch. 896, F.S.; any violation of ch 815, F.S.; any violation of ch. 847, F.S.; any violation of s. 827.071, F.S.; any violation of s. 944.40, F.S.; or any conspiracy or solicitation to commit any violation of the laws of this state relating to the crimes specifically enumerated in this section.
[39] Section 934.09(3)(a)-(d), F.S.
[40] Section 934.09(5) and (8)(e), F.S.
[41] Section 934.09(8)(c), F.S.
[42] Section 934.09(8)(a), F.S.

- Court order; or
- Certificate by a law enforcement officer that no warrant or court order is required and all statutory requirements have been met.[43]

The wire, oral, or electronic communication service provider, landlord, custodian, or other person may not disclose the existence of any interception or the device used to accomplish the interception to which the order pertains.

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.[44]

The penalties for this offense vary based on the specific intent and the number of offenses.[45] It is a first degree misdemeanor[46] if the above described offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain.[47] Any subsequent offense with this intent is a third degree felony.[48]

If the person did not have the above described intent then the above described offense is a second degree misdemeanor.[49]

Florida Businesses and Out-of-State Corporations Records

Section 92.605, F.S., relates to the production of business records by Florida corporations and out-of-state corporations. Specifically, s. 92.605(9), F.S, provides that in a criminal case, the content of any electronic communication may be obtained only by court order or by the issuance of a search warrant, unless otherwise provided under the federal Electronic Communications Privacy Act of 1986 or other provision of law.

Recent Location Privacy Legislation and Case Law in Other States

At least 18 states now require law enforcement to get a probable cause warrant before obtaining people's cell phone location information. Six of those states protect both historical and real-time location information from warrantless search. State supreme courts have decided this issue as

[43] Section 934.03(2)(a)2., F.S.
[44] Section 934.21(1), F.S.
[45] *See* s. 934.21(2), F.S.
[46] 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.
[47] Section 934.21(2), F.S.
[48] 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.
[49] 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.

well in some states, ruling that a probable cause warrant for cell phone location information is required by the state's constitution.[50]

III. Effect of Proposed Changes:

Legislative Findings for Chapter 934, F.S. (Section 2)

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

The bill also creates new legislative findings:

- Recognizing a subjective and objectively reasonable expectation of privacy in precise location data. Finding that a warrant should be issued by a court for law enforcement to obtain the precise location of a person, a cellular phone, or a portable electronic communication device[51] without the consent of the device owner.
- Recognizing that portable electronic 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. Finding that 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[52] 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.

Location Tracking (Section 10)

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

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

---

[50] American Civil Liberties Union, Speech, Privacy, and Technology Project, *Status of Location Privacy Legislation in the States: 2015*, Peter Cihon, August 25, 2015, available at https://www.aclu.org/blog/privacy-technology/location-tracking/status-location-privacy-legislation-states-2015?redirect=blog/free-future/status-location-privacy-legislation-states-2015 (last visited January 30, 2018). *See* the chart contained within this article for the state legislation and court decisions as of the October 13, 2015.

[51] The term "portable electronic communication device" is defined in Section 3 of the bill.

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

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

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

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

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

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

The bill also allows for the installation of a mobile tracking device without a warrant if an emergency exists which:

- Involves immediate danger of death or serious physical injury to any person or the danger of escape of a prisoner;
- Requires the installation or use of a mobile tracking device before a warrant authorizing such installation or use can, with due diligence, be obtained; and
- There are grounds upon which a warrant could be issued to authorize such installation or use.[53]

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. If a law enforcement officer continues use of such a device he or she commits a first degree misdemeanor.

Chapter 934, F.S., Security of Communications Definitions (Section 3)

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

[53] This exception is similar to that found in s. 934.09(7), F.S.

- The current definition of "oral communication" is amended to include interception through the use of a microphone-enabled device.
- 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.
- The definition of "microphone-enabled household device" is created and is defined as a device, sensor, or other physical object within a residence which:
  - Is capable of connecting to the Internet, directly or indirectly, or to another connected device;
  - Is capable of creating, receiving, accessing, processing, or storing electronic data or communications;
  - Communicates with, by any means, another device, entity, or individual; and
  - Contains a microphone designed to listen for and respond to environmental cues.

Interception of Wire, Oral, or Electronic Communications

Law Enforcement (Sections 5, 6, and 7)

The bill amends the application that the Governor, the Attorney General, the statewide prosecutor, or any state attorney can authorize from a *court order* to a *warrant*.

The bill also amends s. 934.09, F.S., to require a *warrant* rather than a *court order* for the interception of a wire, oral, or electronic communication to require a *warrant* for such interception. The bill retains all of the requirements necessary for a *court order* to require the same for a *warrant*.

The bill specifies that a law enforcement officer who intercepts oral, wire, or electronic communications under the authority of a *warrant* is allowed to disclose or use additional evidence unrelated to the warrant, under certain specified circumstances.[54]

The bill amends the requirement of the disclosure of the contents of an intercepted wire, oral, or electronic communication to remove that such disclosure must be made 10 days prior to certain proceedings.

The bill also provides that duplicate recordings of the interceptions, warrant applications, and warrants may be disclosed for purposes of discovery.

The bill specifies that the Florida Rules of Criminal Procedure govern motions to suppress the contents of the interception or evidence derived from the interception. The bill also clarifies that if a motion to suppress is granted, the contents and evidence are not admissible.

Wire, Oral, or Electronic Communication Service Provider and Others Exception (Section 4)

The bill adds a warrant to the list of documentation that can be provided to a wire, oral, or electronic service provider or other listed person that allows him or her to provide assistance in

[54] *See* s. 934.08(1)-(2), F.S.

the interception of a wire, oral, or electronic communication. The bill also specifies that any of above listed persons cannot disclose the existence of any interception or the device used to accomplish the interception that was authorized by the warrant.

Stored Communications (Section 9)

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

Florida Businesses and Out-of-State Corporations Records (Section 1)

The bill amends s. 92.605, F.S., to specify that in criminal cases the content of any electronic communication sought from a Florida business or out-of-state corporation be obtained under the provisions in ch. 934, F.S.

Other (Sections 8, 11, 12, 13, 14, 15, 16 and 17)

The bill provides that a good faith reliance on a *warrant* is complete defense to any related civil, criminal, or administrative action arising out of conduct provided for by law.

The bill also reenacts ss. 934.22, 934.23, 934.24, 934.25, 934.27, and 934.28, F.S., to incorporate amendments made by this act.

The bill is effective July 1, 2018.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The Florida Department of Law Enforcement does not expect any fiscal impact from this bill.[55]

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 92.605, 934.01, 934.02, 934.03, 934.07, 934.08, 934.09, 934.10, 934.21, and 934.42.

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

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.

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