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/CS/SB 1256
INTRODUCER:	Rules Committee; Judiciary Committee; Criminal Justice Committee; and Senator Brandes
SUBJECT:	Security of Communications
DATE:	February 26, 2018
REVISED:	

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

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/CS/SB 1256 amends ch. 934, F.S., relating to security of communications, to address privacy issues related to the use of communication technology and the contents of stored electronic communications, and also sets forth requirements relating to obtaining by subpoena certain information in investigations involving child sexual abuse and certain sex crimes.

Communication technology, such as cell phones, laptops, and tablets, may be equipped with location tracking technology which allows the service provider to track the device whenever it is on. The bill replaces the current 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 relevant to communication technology include: defining or amending relevant terms; providing time constraints under which a tracking device must be used and when notice must be provided to the person tracked; providing that a postponement of notice may only be granted by a court for good cause; and permitting emergency tracking under certain circumstances.

The bill also making substantial changes regarding the legal process required to obtain the content of stored wire or electronic communications. The bill requires a warrant to obtain all contents of stored communications, and removes provisions of law relating to obtaining such contents, with prior notice, by court order for disclosure or subpoena. A law enforcement agency must request a prosecutor obtain the subpoena.

In an investigation involving allegations of sexual abuse of a child or the suspected commission of certain sex crimes, a subpoena is authorized to obtain records, documents, or other tangible objects (not related to stored communications). In an investigation involving allegations of sexual abuse of a child, a subpoena is authorized to obtain noncontent basic subscriber information in stored communications. A law enforcement agency must request a prosecutor obtain the subpoena. The bill prohibits a service provider to whom the subpoena is directed from disclosing the existence of the subpoena for a 180-day period if the subpoena is accompanied by written certification by a supervisory official that disclosure may result in an adverse result. Limited disclosure is authorized. The subpoena recipient can petition a court for an order to modify or set aside the disclosure prohibition. The 180-day period can be extended pursuant to a court order as provided in the bill.

Other specific changes relevant to this investigative subpoena include: providing for retention of some subpoenaed tangible objects for specific uses; providing for compensation of a subpoenaed witness and others; providing legal protections for subpoena compliance; and authorizing a court to compel compliance with a subpoena and to sanction refusal to comply with a subpoena.

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

[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.

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]

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.

Advancing Technology - Location Tracking

Cell phones, smartphones, laptops, and tablets are all mobile devices that can be located whenever they are turned on.[7] 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[8] 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.[9]

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."[10]

Florida law defines a "tracking device" as an electronic or mechanical device which permits the tracking of movement of a person or object.[11] 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."[12] If the court grants the order, the officer installs and uses the device.[13] 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;

---

[6] *Id*. and *supra*, n. 1.
[7] *Cell Phone Tracking Methods*, Electronic Privacy Information Center, available at https://epic.org/privacy/location/ (last visited on Feb. 21 2018).
[8] A service provider is the company that provides the internet to the mobile device. *Id.*
[9] *Id.*
[10] 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 visited on Feb. 21, 2018).
[11] Section 934.42(6), F.S.
[12] Section 934.42(1)-(2), F.S.
[13] Section 934.42(3), F.S.

- 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.[14]

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.[15]

The installation and the monitoring of a mobile tracking device are governed by the standards established by the United States Supreme Court.[16]

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).[17] "As the cell phone travels, it connects to various cell phone towers, which means an electronic record of its location is created[.]"[18] The cell phone's location record is held by the telecommunications company that services the device.[19]

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."[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

[14] Section 934.42(2), F.S.
[15] Section 934.42(3) and (4), F.S.
[16] Section 934.42(5), F.S.
[17] Mana Azarmi, *Location Data: The More They Know*, Center for Democracy and Technology (Nov. 27, 2017), available at https://cdt.org/blog/location-data-the-more-they-know/ (last visited on Feb. 21, 2018).
[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] *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 visited on Feb. 21, 2018).
[22] *Id*.
[23] *Id*.

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]

Microphone-Enabled Household Devices

Another emerging technology raising privacy concerns is the smart speaker. Smart speakers, like the Google Home[26] or Amazon Echo,[27] 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. [28]

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. [29]

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.[30]

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

Chapter 934, F.S., closely mirrors the federal Electronic Communications Privacy Act of 1986 (ECPA).[31] Several definitions in this chapter are pertinent to the bill:

---

[24] *GPS Location Privacy*, GPS.gov (last modified Aug. 22, 2017), available at https://www.gps.gov/policy/privacy (last visited on Feb. 21, 2018).
[25] Patrick Bertagna, *How does a GPS tracking system work?* (Oct. 26, 2010), EE Times, available at https://www.eetimes.com/document.asp?doc_id=1278363&page_number=2 (last visited on Feb. 21, 2018). 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. 10.
[26] *Google Home*, Google Store, available at https://store.google.com/product/google_home (last visited on Feb. 21, 2018).
[27] *Echo & Alexa*, Amazon, available at https://www.amazon.com/all-new-amazon-echo-speaker-with-wifi-alexa-dark-charcoal/dp/B06XCM9LJ4 (last visited on Feb. 21, 2018).
[28] 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 visited on Feb. 21, 2018).
[29] *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 visited on Feb. 21, 2018).
[30] Eliott C. McLaughlin, *Suspect OKs Amazon to hand over Echo recordings in murder* case (Apr. 26, 2017), CNN, available at https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html (last visited on Feb. 21, 2018).
[31] The ECPA is codified at 18 U.S.C. s. 2510 et seq.

- "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.[32]
- "Electronic communication" means the transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, interstate, or foreign commerce. The definition does not include: any wire or oral communication; any communication made through a tone-only paging device; any communication from an electronic or mechanical device which permits the tracking of the movement of a person or an object; or electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.[33]
- "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.[34]
- "Electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.[35]
- "Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, electronic, or oral communication other than any telephone or telegraph instrument, equipment, or facility, or any component thereof:
  - Furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or
  - Being used by a provider of wire or electronic communications service in the ordinary course of its business or by an investigative or law enforcement officer in the ordinary course of her or his duties.[36]
- "Electronic storage" means any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof, and any storage of a wire or electronic communication by an electronic communication service for purposes of backup protection of such communication.[37]
- "Intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.[38]
- "Investigative or law enforcement officer" means any officer of the State of Florida or political subdivision thereof, of the United States, or of any other state or political subdivision thereof, who is empowered by law to conduct on behalf of the Government investigations of, or to make arrests for, offenses enumerated in this chapter or similar federal offenses, any attorney authorized by law to prosecute or participate in the prosecution of such offenses, or any other attorney representing the state or political subdivision thereof in any

[32] Section 934.02(7), F.S.
[33] Section 934.02(12), F.S.
[34] Section 934.02(15), F.S.
[35] Section 934.02(14), F.S.
[36] Section 934.02(4), F.S.
[37] Section 934.02(17), F.S.
[38] Section 934.02(3), F.S.

civil, regulatory, disciplinary, or forfeiture action relating to, based upon, or derived from such offenses.[39]

- "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation does not mean any public oral communication uttered at a public meeting or any electronic communication.[40]
- "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.[41]
- "Subpoena" means any administrative subpoena authorized by federal or Florida law, federal or Florida grand jury subpoena, or any criminal investigative subpoena as authorized by Florida statute which may be utilized on behalf of the government by an investigative or law enforcement officer.[42]
- "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.[43]

Prohibited Access to Stored Communications

Florida law also prohibits accessing stored communications. It is unlawful for a person to:

- Intentionally access a facility through which an electronic communication service is provided; or
- Intentionally exceed an authorization to access; and
- Obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such a system.[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]

[39] Section 934.02(6), F.S.
[40] Section 934.02(2), F.S.
[41] Section 934.02(19), F.S.
[42] Section 934.02(23), F.S.
[43] Section 934.02(1), 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, a fine of up $1,000, or both. 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 5 years in state prison, a fine of up to $5,000, or both. Sections 775.082 and 775.083, F.S.

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

Section 934.23, F.S., and the Federal Stored Communications Act

Major Features of Section 934.23, F.S.

Section 934.23, F.S., is patterned after the federal Stored Communications Act (SCA).[50] It closely tracks 18 U.S.C. s. 2703. "The SCA protects communications held by two defined classes of network service providers[.]"[51] Those classes are electronic communication service (ECS) providers and remote computing service (RCS) providers.[52]

Section 934.23, F.S., specifies how an investigative or law enforcement officer may obtain the content of a wire or electronic communication that has been in electronic storage in an electronic communications system (for a specified period) or held or maintained in a remote computing service, and noncontent records or other information pertaining to a subscriber or customer of such service.

Section 934.23, F.S., also provides procedures for retention of records and other evidence pending issuance of process[53] and provides legal protections[54] and reasonable compensation for those providing assistance.[55]

Disclosure of Records or Information under Section 934.23, F.S.

The SCA (specifically, 18 U.S.C. s. 2703) "provides for different means of obtaining evidence, and different levels of privacy protection, depending on the type of evidence sought and the type

[49] 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.
[50] The "Stored Communications Act" is a term used to describe Title II of the ECPA (codified at 18 U.S.C. ss. 2701-2712), though the term "appears nowhere in the language of the statute." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (July 2009), p. 115, n. 1, U.S. Department of Justice, available at http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (last visited on Feb. 21, 2018).
[51] *Id.* at p. 117.
[52] *Id.*
[53] An ECS provider or RCS provider, upon the request of an investigative or law enforcement officer, must take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process. The records must be retained for a period of 90 days, which is extended for an additional 90 days upon a renewed request by such officer. Section 934.23(7), F.S.
[54] No cause of action lies in any court against an ECS provider, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under ss. 934.21-934.28, F.S. Section 934.23(6), F.S. Further, an ECS provider, RCS provider, or any other person who furnished assistance pursuant to s. 934.23, F.S., is held harmless from any claim and civil liability resulting from the disclosure of information pursuant to that section. Section 934.23(8), F.S.
[55] An ECS provider, RCS provider, or any other person who furnished assistance pursuant to s. 934.23, F.S., must be reasonably compensated for reasonable expenses incurred in providing such assistance. Section 934.23(8), F.S.

of provider possessing it."[56] Section 934.23, F.S., mirrors this approach. The types of evidence obtainable by different means are discussed in detail below.[57]

No Process – Consent of the Subscriber or Customer

An investigative or law enforcement officer may require an ECS provider or RCS provider to disclose a record or other information pertaining to a subscriber or customer of such service, not including the contents of a communication, if the officer has the consent of the subscriber or customer to such disclosure.[58]

Subpoena

An investigative or law enforcement officer who obtains a subpoena may obtain from the ECS provider or RCS provider basic information, including session information, regarding a subscriber or customer of the provider.[59] This information includes:

- Name and address;
- Local and long-distance telephone connection records or records of session times or durations;
- Length of service, including the starting date of service;
- Types of services used;
- Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- Means and source of payment, including any credit card or bank account number of a subscriber to or customer.[60]

Subpoena with Prior Notice to the Subscriber or Customer

An investigative or law enforcement officer who obtains a subpoena and provides prior notice to the subscriber or customer or with delayed notice pursuant to s. 934.25, F.S., may obtain:

- Whatever can be obtained by subpoena without prior notice;
- Contents of a wire or electronic communication that has been held in electronic storage in an electronic communication system for more than 180 days;[61]
- An electronic communication that is held or maintained on a RCS:
    - On behalf of a subscriber or customer of the RCS and received by means of electronic transmission from, or created by means of computer processing of communications

[56] *Matter of Search Warrant for [redacted].com*, 248 F.Supp. 3d 970, 975 (C.D. Cal. 2017). "The structure of the SCA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests." *Supra*, n. 50, at p. 115. "Some information can be obtained from providers with a subpoena, other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not." *Id.* at p. 116.

[57] This analysis follows the format provided by the DOJ in its discussion of the SCA. *Supra*, n. 50.

[58] Section 934.23(4)(a)3., F.S. (similar to 18 U.S.C. s. 2703(c)(1)(C)).

[59] Section 934.23(4)(a)4. and (4)(b), F.S.

[60] Section 934.23(4)(b), F.S. (similar to 18 U.S.C s. 2703(c)(2)). "In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records. In the Internet context, 'any temporarily assigned network address' includes the IP address used by a customer for a particular session. For example, for a webmail service, the IP address used by a customer accessing her email account constitutes a 'temporarily assigned network address.' This list does not include other, more extensive transaction-related records, such as logging information revealing the email addresses of persons with whom a customer corresponded." *Supra*, n. 50, at p. 121.

[61] Section 934.23(1) and (2)(b)1., F.S. (similar to 18 U.S.C. s. 2703(a) and (b)(1)(B)(i)).

received by means of electronic transmission from, a subscriber or customer of such service; and
- Solely for the purposes of providing storage or computer processing services to a subscriber or customer, if the provider is not authorized to access the contents of any such communication for purposes of providing any service other than storage or computer processing.[62]

Court Order for Disclosure without Prior Notice

Pursuant to s. 934.23(5), F.S., a court may issue an order for disclosure only if the investigative or law enforcement officer offers specific and articulable facts showing that there are reasonable grounds to believe the contents of a wire or electronic communication or the records of other information sought are relevant and material to an ongoing criminal investigation.[63]

An investigative or law enforcement officer who obtains a court order for disclosure may obtain:
- Whatever can be obtained by subpoena without prior notice; and
- From an ECS provider or RCS provider, a record or other information pertaining to the subscriber or customer of such service, not including contents of communications.[64]

Court Order for Disclosure with Prior Notice

An investigative or law enforcement officer who obtains a court order for disclosure without prior notice, and either gives prior notice to the subscriber or customer or complies with delayed notice provisions of s. 934.25, F.S., may obtain:
- Whatever can be obtained by a court order for disclosure;
- Contents of a wire or electronic communication that has been held in electronic storage in an electronic communication system for more than 180 days;[65] and
- Contents of an electronic communication that is held or maintained on a RCS as described in s. 934.23(3), F.S.[66]

Search Warrant

An investigative or law enforcement officer who obtains a search warrant may obtain:
- Whatever can be obtained pursuant to a court order for disclosure with notice; and

[62] Section 934.23(2)(b)1. and (3), F.S. (similar to 18 U.S.C. s. 2703(b)(1)(B)(i) and (2)). According to the DOJ, "[o]utside the Ninth Circuit …, this third category will include opened and sent e-mail." *Supra*, n. 50, at p. 129.
[63] According to the DOJ, the equivalent federal court order for disclosure (under 18 U.S.C. s. 2703(d)) is needed "to obtain most account logs and most transactional records." *Supra*, n. 50, at p. 130.
[64] Section 934.23(4)(a)2., F.S. (similar to 18 U.S.C. s. 2703(c)(1)(B)). "This is a catch-all category that includes all records that are not contents, including basic subscriber and session information…. As one court explained, 'a record means something stored or archived. The term information is synonymous with data.' *In re United States*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007)." *Supra*, n. 50, at p. 122.
[65] Section 934.23(1), F.S. (similar to 18 U.S.C. s. 2703(a)).
[66] Section 934.23(2)(b)2. and (3), F.S. According to the DOJ, except in the federal Ninth Circuit, the federal government can obtain with a court order for disclosure with prior notice "the full contents of a subscriber's account except unopened email and voicemail that have been in the account for 180 days or less." *Supra*, n. 50, at p. 132.

- Contents of a wire or electronic communication that has been held in electronic storage in an electronic communication system for 180 days or less.[67]

Section 934.25, F.S. (Delayed Notice)

Section 934.25, F.S., is also patterned after the SCA. It closely tracks 18 U.S.C. s. 2705. Pursuant to s. 934.25(1), F.S., if an investigative or law enforcement officer seeks to obtain content of stored communications pursuant to a court order for disclosure (with prior subscriber notice) or subpoena (with prior subscriber notice) s. 934.23(2), F.S, the officer may delay the required notice for a period not exceeding 90 days as provided:

- Where a court order for disclosure is sought, the officer includes in the application a request for an order delaying the notification for a period not to exceed 90 days, which request the court must grant if it determines that there is reason to believe that notification of the existence of the court order *may* have an "adverse result."[68]
- Where a subpoena is obtained, the officer may delay the notification for a period not to exceed 90 days upon the execution of a written certification of a supervisory official[69] that there is reason to believe that notification of the existence of the subpoena may have an "adverse result"[70] described in subsection (2).[71]

Section 934.25(4), F.S., provides that the 90-day period may be extended by court order, but only in 90-day increments and only in accordance with s. 934.25(6), F.S., which effectively requires the officer to demonstrate to the court or certify that there is reason to believe notification *will* result in any act specified in that subsection (acts identical to those acts that constitute an "adverse result" [72] under subsection (2)).[73]

Section 934.25(5), F.S., provides that, upon the expiration of the period of delay of notification under s. 934.25(1), F.S., or s. 934.25(4), F.S., the investigative or law enforcement officer must serve upon or deliver by registered or first-class mail to the subscriber or customer a copy of the process or request together with notice which:

- States with reasonable specificity the nature of the law enforcement inquiry, and
- Informs the subscriber or customer:

---

[67] Section 934.23(1), F.S. (similar to 18 U.S.C. s. 2703(a)). "Investigators can obtain everything associated with an account with a search warrant. The SCA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant." *Supra*, n. 50, at p. 133.

[68] Section 934.25(1)(a), F.S. (similar to 18 U.S.C. s. 2705(a)(1)(A)). An "adverse result" is defined in s. 934.25(2) and (6), F.S., as any of the following acts: endangering the life or physical safety of an individual; fleeing from prosecution; destroying or tampering with evidence; intimidating potential witnesses; or seriously jeopardizing an investigation or unduly delaying a trial. This definition is identical to the definition of the term in 18 U.S.C. s. 2705(a)(2).

[69] A "supervisory official" is "the person in charge of an investigating or law enforcement agency's or entity's headquarters or regional office; the state attorney of the circuit from which the subject subpoena has been issued; the statewide prosecutor; or an assistant state attorney or assistant statewide prosecutor specifically designated by the state attorney or statewide prosecutor to make such written certification. Section 934.25(7), F.S. (similar to 18 U.S.C. s. 2705(a)(6)).

[70] *Supra*, n. 68.

[71] Section 934.25(1)(b), F.S. (similar to 18 U.S.C. s. 2705(a)(1)(B)). The investigative or law enforcement officer has to maintain a true copy of a certification obtained under paragraph (1)(b). Section 934.25(3), F.S. (similar to 18 U.S.C. s. 2705(a)(3)).

[72] *Supra*, n. 68.

[73] Similar to 18 U.S.C. s. 2705(a)(4).

- That information maintained for such subscriber or customer by the service provider named in the process or request was supplied to or requested by the investigative or law enforcement officer and the date on which such information was so supplied or requested;
- That notification of such subscriber or customer was delayed;
- What investigative or law enforcement officer or what court made the certification or determination pursuant to which that delay was made; and
- Which provision of ss. 934.21-934.28, F.S., allowed such delay.[74]

Section 934.25(6), F.S., also authorizes an investigative or law enforcement officer acting under s. 934.23, F.S., when not required to notify the subscriber or customer under s. 934.23(2)(a), F.S. (warrant), or to the extent such notice may be delayed pursuant to s. 934.25(1), F.S. (court order for disclosure or subpoena in which notice is required), to apply to a court for an order commanding an ECS provider or RCS provider to whom a warrant, subpoena, or court order is directed not to notify any other person of the existence of the warrant, subpoena, or court order. The order of nondisclosure is "for such period as the court deems appropriate" and can only be entered if the court determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order *will* result in any act specified in that subsection (acts identical to those acts that constitute an "adverse result").[75]

Investigative Subpoenas

Subpoenas Generally

A "subpoena," which literally means "under penalty,"[76] is a "process or a writ of a judicial nature" used by a court or, when authorized, by an investigative or administrative body, to compel compliance in a proceeding, usually after the proceeding has been initiated.[77] There are two types of subpoenas used in both the civil and criminal context. The subpoena ad testificandum is used to compel the attendance and testimony of witnesses.[78] The subpoena duces tecum is used to compel production of documents, materials, or other tangible information.[79]

Investigative Subpoena Powers

An investigative subpoena is used by the proper authority to investigate a crime after a crime is reported or a complaint is filed. "The purpose of an investigative subpoena is to allow the State to obtain the information necessary to determine whether criminal activity has occurred or is

[74] Similar to 18 U.S.C. s. 2705(a)(5) and (b).
[75] *Supra*, n. 68. Similar to 18 U.S.C. s. 2705(b).
[76] Webster's New World College Dictionary, 5th Ed. (2014).
[77] Op. Att'y Gen. Fla. 81-65 (1981) (citations omitted), available at http://www.myfloridalegal.com/ago.nsf/Opinions/6515E4FA246990B085256587004F3F07 (last visited on Feb. 21, 2018).
[78] *What is a Subpoena?*, FindLaw, available at http://litigation.findlaw.com/going-to-court/what-is-a-subpoena.html (last visited on Feb. 21, 2018).
[79] *Id.* Information may include data, such as "non-content information, connected to our Internet transactions (e.g., websites visited, to/from and time/date stamps on emails)." Richard M. Thompson II & Jared P. Cole, *Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)*, CRS Report 44036 (May 19, 2015), p. 2 (summary), Congressional Research Service, available at https://digital.library.unt.edu/ark:/67531/metadc811160/m1/1/ (last visited on Feb. 21, 2018).

occurring."[80] "[T]he State cannot be required to prove that a crime has occurred before it can issue an investigative subpoena because the entire purpose of the investigative subpoena is to determine whether a crime occurred."[81] "To require the State to prove that a crime occurred before it can issue an investigative subpoena puts the State in an impossible catch-22."[82]

Thus, to carry out its investigative duties, the State has "the authority to issue an investigative subpoena duces tecum."[83] As Florida courts have often recognized, "the state attorney acts as a one-person grand jury in carrying out investigations into noncapital criminal conduct"[84] where the state attorney must investigate to determine if there is probable cause to charge someone with a crime, and then charge that person by information. Because "the state attorney must be granted reasonable latitude" in its investigative role, "section 27.04, Florida Statutes . . . , allows the state attorney to issue subpoenas duces tecum for records as part of an ongoing investigation."[85]

Under s. 27.04, F.S., the state attorney's authority to "use the process of court" includes both compelling witness testimony and production of records and other information.[86] Section 16.56(3), F.S., provides the same authority to the statewide prosecutor. When the Department of Law Enforcement is involved in the investigation, the Department of Legal Affairs (Attorney General's Office) is the legal adviser and attorney to the department.[87]

"The decision to charge and prosecute criminal offenses is an executive responsibility over which the state attorney has complete discretion[.]"[88] "The State clearly has a strong interest in gathering information relevant to an initial inquiry into suspected criminal activity[.]"[89] However, the State's investigative powers are not unlimited. Rather, "[a] judicial limit to this discretion arises where constitutional constraints are implicated."[90]

Section 92.605, F.S., and the Federal Stored Communications Act

The provisions of s. 92.605, F.S., apply to a search warrant, court order, or subpoena issued in compliance with the federal Stored Communications Act (SCA). Section 92.605, F.S., allows a search for records that are in the actual or constructive possession of an out-of-state corporation that provides electronic communication services or remote computing services to the public, when those records would reveal:

- The identity of the customers using those services;
- Data stored by, or on behalf of, the customers;
- The customers' usage of those services; or

[80] *State v. Investigation*, 802 So. 2d 1141, 1144 (Fla. 2d DCA 2001).
[81] *Id.*
[82] *Id.*
[83] *Id.* at p. 1143-44.
[84] *Id.* at p. 1144 (citations omitted).
[85] *Id.*
[86] *State v. Jett*, 358 So.2d 875, 876-77 (Fla. 3d DCA 1978).
[87] Section 934.03(8), F.S.
[88] *State v. Gibson*, 935 So. 2d 611, 613 (Fla. 3d DCA 2006) (quoting *State v. Bloom*, 497 So. 2d 2, 3 (Fla. 1986) (internal quotations omitted)).
[89] *Id.* (quoting *Doe v. State*, 634 So.2d 613, 615 (Fla. 1994) (internal quotations omitted)).
[90] *State v. J.M.*, 718 So.2d 316, 317 (Fla. 2d DCA 1998).

- The recipients or destinations of communications sent to or from those customers.[91]

Under s. 92.605, F.S., when an out-of-state corporation subject to this section is properly served[92] by an applicant[93] for the subpoena, court order, or search warrant, the out-of-state-corporation must provide to the applicant all records sought pursuant to the process within 20 business days after receipt, or the date indicated within the subpoena, if later, including those records maintained or located outside the state.[94] If the records cannot be produced within the 20-day time period, the out-of-state corporation must notify the applicant within the 20-day time period and agree to produce the documents at the earliest possible time. The applicant must pay the out-of-state corporation the reasonable expenses associated with compliance.[95]

When the applicant makes a showing and the court finds that failure to produce records within 20 business days would cause an adverse result, the subpoena, court order, or warrant may require production of records within less than 20 business days. A court may reasonably extend the time required for production of the records upon finding that the out-of-state corporation needs the extension and that the extension would not cause an adverse result.[96]

Additionally, s. 92.605, F.S.:

- Requires that an out-of-state corporation seeking to quash or object to the subpoena, court order, or warrant seek relief from the court issuing such subpoena, court order, or warrant in accordance with s. 92.605, F.S.;[97]
- Requires verification of the authenticity of produced records upon written request from the applicant or if ordered by the court;[98]
- Provides that a cause of action does not arise against any out-of-state corporation or Florida business for providing records, information, facilities, or assistance in accordance with the terms of a subpoena, court order, or warrant subject to s. 92.605, F.S.;[99] and
- Provides for admissibility in evidence in a criminal proceeding of records produced in compliance with s. 92.605, F.S.[100]

[91] Section 92.605(2), F.S.
[92] "Properly served" means delivery by hand or in a manner reasonably allowing for proof of delivery if delivered by United States mail, overnight delivery service, or facsimile to a person or entity properly registered to do business in any state. In order for an out-of-state corporation to be properly served, the service must be effected on the corporation's registered agent. Section 92.605(1)(h), F.S.
[93] "Applicant" means a law enforcement officer who is seeking a court order or subpoena under s. 16.56, F.S., s. 27.04, F.S., s. 905.185, F.S., or s. 914.04, F.S., or who is issued a search warrant under s. 933.01, F.S., or anyone who is authorized to issue a subpoena under the Florida Rules of Criminal Procedure. Section 92.605(1)(b), F.S.
[94] Section 92.605(2)(b), F.S. In any criminal case, the content of any electronic communication may be obtained under s. 92.605, F.S., only by court order or by the issuance of a search warrant, unless otherwise provided under the ECPA or other provision of law. Section 92.605(9), F.S.
[95] Section 92.605(2)(b), F.S.
[96] Section 92.605(2)(c), F.S. Section 92.605(1)(a), F.S., contains a definition of "adverse result" that is identical to the definitions of that term in s. 934.25(2) and (6), F.S. See, *infra*, n. 46.
[97] Section 92.605(2)(d), F.S.
[98] Section 92.605(2)(e), F.S.
[99] Section 92.605(4), F.S.
[100] Section 92.605(5)-(8), F.S A Florida ECS provider or RCS provider is required to produce the same records previously described when served with a subpoena, court order, or warrant issued by another state. Section 92.605(3), F.S.

III. Effect of Proposed Changes:

Communications Technology

Legislative Findings for Chapter 934, F.S.

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 three new legislative findings. First, 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 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, 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

The bill amends s. 934.02, F.S., the definitions section of ch. 934, F.S., to amend a current definition and create new definitions:

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

creating, receiving, accessing, or storing electronic data or communications and which communicates with, by any means, another device, entity, or individual.

Location Tracking

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.

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 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, 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.[101]

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.

Changes to Sections 934.21, 934.23, 934.24, and 934.25, F.S., Relating to Stored Communications

Penalties for Accessing Stored Communications

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

- By the provider[102] or user[103] of wire, oral, or electronic communications services through cellular phones, portable electronic communication devices, or microphone-enabled household devices;
- Under ch. 933, F.S.;[104] or
- For legitimate business purposes that do not identify the user.

New Warrant Requirement under Section 934.23, F.S., for Contents of Stored Communications

The bill amends s. 934.23, F.S., to require a warrant for all contents of stored wire or electronic communications. The bill removes current provisions relating to obtaining some contents of stored communications with a court order for disclosure (with prior subscriber notice) or a subpoena (with prior subscriber notice).

Currently, s. 934.23(4)(b), F.S., specifies that certain basic subscriber information is obtainable with a subpoena. Paragraph (4)(c) states that no prior subscriber notice is required for this subpoena. The bill deletes paragraph (4)(c). This paragraph was only necessary to distinguish the subpoena in paragraph (4)(c) from the subpoena (with prior subscriber notice) in subsection (2), which the bill deletes.

The bill also creates a definitions subsection, which includes the current definition in the section of "a court of competent jurisdiction" and adds a definition of "investigative or law enforcement officer." An "investigative or law enforcement officer" is defined as having the same meaning as s. 934.02(6), F.S., *except that in any criminal investigation, if a law enforcement agency seeks disclosure of information obtainable by a subpoena under this section, the agency must request a*

[101] This exception is similar to that found in s. 934.09(7), F.S.
[102] Section 934.21(3)(a), F.S.
[103] Section 934.21(3)(b), F.S.
[104] Chapter 933, F.S., authorizes search and inspection warrants.

state attorney, an assistant state attorney, the statewide prosecutor, or an assistant statewide prosecutor obtain such subpoena.[105]

Repealing Section 934.24, F.S. (Backup Preservation)

Section 934.24, F.S., addresses backup preservation pertaining to some contents of stored communications obtained by court order for disclosure (with prior subscriber notice) or subpoena (with prior subscriber notice) under current s. 934.23(2)(b), F.S., and authorizes a subscriber to file a motion to quash such subpoena or vacate such order. However, since the bill deletes s. 934.23(2)(b), F.S., and requires a warrant for the contents of all stored communications, this section is no longer relevant. Preservation of records and other evidence is addressed in s. 934.23, F.S., which the bill does not delete.

Deleting Provisions in Section 934.25, F.S. (Delayed Notice)

Section 934.25, F.S., in part, addresses delay of subscriber notice required under s. 934.23(2), F.S. Section 934.23(2)(b), F.S., specifically provides that some contents of stored communications may be obtained with a court order for disclosure (with prior subscriber notice) or a subpoena (with prior subscriber notice). However, since the bill deletes s. 934.23(2)(b), F.S., and requires a warrant for the contents of all stored communications, these provisions are no longer relevant.

The bill retains a provision authorizing a court to prohibit disclosure of the existence of a warrant, court order for disclosure, or subpoena for such period as the court deems appropriate based on criteria specified in the statute.

Investigative Subpoenas

The bill creates s. 934.255, F.S., pertaining to investigative subpoenas in investigations of sexual abuse of a child and specified sex crimes.

Definitions

The bill provides the following definitions of terms relevant to the investigative subpoena provisions of the bill:

- "Adverse result" means any of the following acts:
  - Endangering the life or physical safety of an individual.
  - Fleeing from prosecution.
  - Destroying or tampering with evidence.
  - Intimidating potential witnesses.
  - Seriously jeopardizing an investigation or unduly delaying a trial.
- "Child" means a person under 18 years of age.
- "Investigative or law enforcement officer" has the same meaning as s. 934.02(6), F.S., *except that in any criminal investigation, if a law enforcement agency seeks disclosure of information obtainable by a subpoena under this section, the agency must request a state*

[105] The bill does not impose any requirement that a law enforcement agency request a prosecutor obtain a court order for disclosure or warrant. A law enforcement agency is not prohibited from *directly* obtaining a court order for disclosure or warrant.

attorney, an assistant state attorney, the statewide prosecutor, or an assistant statewide prosecutor obtain such subpoena.[106]

- "Sexual abuse of a child" means a criminal offense based on any conduct described in s. 39.01(71), F.S.
- "Supervisory official" means the person in charge of an investigating or law enforcement agency's or entity's headquarters or regional office; the state attorney of the circuit from which the subpoena has been issued; the statewide prosecutor; or an assistant state attorney or assistant statewide prosecutor specifically designated by the state attorney or statewide prosecutor to make such written certification.

Investigative Subpoena for Records, Documents, or Other Tangible Objects

In an investigation into allegations of the sexual abuse of a child or an individual's suspected commission of any of a list of specified sex crimes,[107] an investigative or law enforcement officer may use a subpoena to compel the production of records, documents, or other tangible objects and the testimony of the subpoena recipient to authenticate such tangible objects. This investigative subpoena does not specifically address stored communications information, which is addressed separately in the bill.

Investigative Subpoena Directed to ECS Provider or RCS Provider

In an investigation involving sexual abuse of a child, an investigative or law enforcement officer may use a subpoena to require an ECS provider or RCS provider to disclose basic subscriber identity and session information described in s. 934.23(4)(b), F.S.:[108]

- Name and address;
- Local and long-distance telephone connection records, or records of session times or durations;
- Length of service, including the starting date of service;
- Types of services used;
- Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- Means and source of payment, including any credit card or bank account number of a subscriber to or customer.

Requirements Relating to Subpoena and Production of Subpoenaed Information

The bill requires that a subpoena describe the records, documents, or other tangible objects required to be produced, and prescribe a date by which such information must be produced. This provision applies to a subpoena to compel the production of records, documents, or other tangible objects, not a subpoena used to obtain basic subscriber identity and session information described in s. 934.23(4)(b), F.S.

---

[106] *Id.*

[107] The crimes are listed in s. 943.0435(1)(h)1.a.(I), F.S., and include but are not limited to: various sex trafficking crimes under s. 787.06, F.S.; sexual battery offenses under ch. 794, F.S.; lewd offenses under ss. 800.04 and 825.1025, F.S.; sexual performance by a child under s. 827.071, F.S.; various computer pornography crimes under ch. 847, F.S.; and selling or buying a minor to engage in sexually explicit conduct under s. 847.0145, F.S.

[108] This is stored communications information.

Petition for an Order Modifying or Setting Aside a Disclosure Prohibition

At any time before the date prescribed in the subpoena for production of records, documents, or other tangible objects, or the subpoena for basic subscriber identity and session information, a person or entity receiving the subpoena may, before a judge of competent jurisdiction, petition for an order modifying or setting aside a prohibition of disclosure.

Retention of Subpoenaed Records or Other Information for Use in an Investigation

An investigative or law enforcement officer who uses a subpoena to obtain any record, document, or other tangible object may retain such items for use in any ongoing criminal investigation or a closed investigation with the intent that the investigation may later be reopened. This provision applies to a subpoena to compel the production of records, documents, or other tangible objects, not a subpoena used to obtain basic subscriber identity and session information described in s. 934.23(4)(b), F.S.

Nondisclosure of the Existence of a Subpoena

The bill authorizes an investigative or law enforcement officer to prohibit a subpoena recipient from disclosing the existence of the subpoena to any person for 180 days if the subpoena is accompanied by a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena *may* have an adverse result. However, a subpoena recipient may disclose information otherwise subject to any applicable nondisclosure requirement to:

- Persons as is necessary to comply with the subpoena;
- An attorney in order to obtain legal advice or assistance regarding compliance with the subpoena; or
- Any other person as allowed and specifically authorized by the investigative or law enforcement officer who obtained the subpoena or the supervisory official who issued the written certification.

This provisions applies to a subpoena to compel the production of records, documents, or other tangible objects, and a subpoena used to obtain basic subscriber identity and session information described in s. 934.23(4)(b), F.S.

The subpoena recipient must notify any person to whom disclosure of the subpoena is made of the existence of, and length of time associated with, the nondisclosure requirement. A person to whom disclosure of the subpoena is made cannot disclose the existence of the subpoena during the nondisclosure period.

At the request of the investigative or law enforcement officer who obtained the subpoena or the supervisory official who issued the written certification, the subpoena recipient must identify to the officer or supervisory official, before or at the time of compliance with the subpoena, the name of any person to whom disclosure was made. If the officer or supervisory official makes such a request, the subpoena recipient has an ongoing duty to disclose the identity of any individuals notified of the subpoena's existence throughout the nondisclosure period.

Extension of the Nondisclosure Period

A court may grant an extension of the nondisclosure period. An investigative or law enforcement officer may apply to a court for an order prohibiting an ECS provider or RCS provider from notifying anyone of the existence of the subpoena for such period as the court deems appropriate. The court must enter the order if it determines that there is reason to believe that notification of the existence of the subpoena *will* result in an adverse result.

This provision applies to the subpoena used to obtain basic subscriber identity and session information described in s. 934.23(4)(b), F.S., not a subpoena to compel the production of records, documents, or other tangible objects.

Compelling Compliance with a Subpoena and Sanctioning Noncompliance

In the case of contumacy[109] by a person served a subpoena, i.e., his or her refusal to comply with the subpoena, the investigative or law enforcement officer who sought the subpoena may petition a court of competent jurisdiction to compel compliance. The court may address the matter as indirect criminal contempt pursuant to Rule 3.840 of the Florida Rules of Criminal Procedure.

Any prohibited disclosure of a subpoena during an initial or extended period of prohibition of disclosure is punishable as provided in s. 934.43, F.S. As applicable to a subpoena, s. 934.43, F.S., provides that it is a third degree felony for a person having knowledge of a subpoena issued or obtained by an investigative or law enforcement officer to give notice or attempt to give notice of the subpoena with the intent to obstruct, impede or prevent:

- A criminal investigation or prosecution; or
- The officer from obtaining the information or materials sought pursuant to the subpoena.

Records Retention by a Provider

An ECS provider or a RCS provider, upon the request of an investigative or law enforcement officer, must take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process. The records must be retained for a period of 90 days, which is extended for an additional 90 days upon a renewed request by an investigative or law enforcement officer.

Protection from Claims and Civil Liability

No cause of action lies in any court against a provider of wire or electronic communication service for providing information, facilities, or assistance in accordance with the terms of a subpoena. An ECS provider, a RCS provider, or any other person who furnished assistance with complying with a subpoena (as provided in the bill) is held harmless from any claim and civil liability resulting from the disclosure of information (as provided in the bill).

[109] Merriam-Webster's online dictionary defines "contumacy" as "stubborn resistance to authority; *specifically*: willful contempt of court." *See* https://www.merriam-webster.com/dictionary/contumacy (last visited on Feb. 21, 2018).

Compensation

An ECS provider, a RCS provider, or any other person who furnished assistance with complying with a subpoena (as provided in the bill) must be reasonably compensated for reasonable expenses incurred in providing such assistance.

A witness who is subpoenaed to appear and provide testimony to authenticate subpoenaed records or other information must be paid the same fees and mileage rate paid to a witness appearing before a court in this state.

Effective Date

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:

There may be some indeterminate litigation costs to the subpoena recipient if the recipient elects to challenge provisions of the bill in court.

C. Government Sector Impact:

The Florida Department of Law Enforcement does not expect any fiscal impact from this bill.[110]

There may be a workload impact in regard to preparing and submitting written certifications relevant to nondisclosure of investigative subpoenas, but this impact is

[110] *2018 Legislative Bill Analysis* (SB 1256) (Jan. 4, 2018), The Florida Department of Law Enforcement (on file with the Senate Committee on Criminal Justice).

indeterminate. There may also be some indeterminate litigation costs associated with defending provisions of the bill if challenged in court.

VI. Technical Deficiencies:

None.

VII. Related Issues:

Although the SCA and current Florida law authorize obtaining some contents of stored communications with a court order for disclosure (with prior subscriber notice) or a subpoena (with prior subscriber notice),[111] this does not necessarily mean that content information is being obtained without a warrant. The federal Sixth Circuit held in *United States v. Warshak* that a warrant is required for all communications content.[112] Although the Sixth Circuit's holding is not binding on other federal circuits, it is a watershed case. "In those [f]ederal districts where *Warshak* has become the de facto law, law enforcement has been required to obtain a warrant even in those cases where lesser process is still permitted by statute. Soon after the decision, the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013."[113]

VIII. Statutes Affected:

This bill substantially amends the following sections of the Florida Statutes: 934.01, 934.02, 934.21, 934.23, 934.25, and 934.42.

This bill creates section 934.255 of the Florida Statutes.

This bill repeals section 934.24 of the Florida Statutes.

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/CS by Rules on February 22, 2018:
The Committee Substitute:

- Requires a warrant for all contents of stored communications, and deletes provisions relating to obtaining such contents with a court order for disclosure (with prior subscriber notice) or a subpoena (with prior subscriber notice);
- Defines terms and specifies that an exception to the definition of "investigative or law enforcement officer" is that in any criminal investigation a law enforcement agency must request a prosecutor obtain a subpoena for information obtainable by a subpoena;

[111] See "Present Situation" section of this analysis.
[112] *United States v. Warshak*, 631 F.3d 266, 283-288 (6th Cir. 2010).
[113] *Email Privacy Act*, Report 114-528, p. 9, 114th Congress 2d Session, Committee on the Judiciary, U.S. House of Representatives, available at https://www.congress.gov/congressional-report/114th-congress/house-report/528/1 (last visited on Feb. 21, 2018).

- Deletes a provision on not providing notice regarding a subpoena for basic subscriber information;
- Repeals s. 934.24, F.S., which addresses backup protection for content of stored communication obtained by court order for disclosure (with prior subscriber notice) or subpoena (with prior subscriber notice), and authorizes a subscriber to move to quash such subpoena or vacate such order;
- Deletes provisions relating to delaying subscriber notice when such notice is required for obtaining contents of stored communications pursuant to a court order for disclosure or subpoena;
- Deletes reference to subscriber notice or delay of such notice in provisions relating to nondisclosure of a warrant, court order, or subpoena for stored communications;
- Defines terms relevant to an investigative subpoena in investigations of sexual abuse of a child and certain sex crimes, and includes a similar exception to the definition "investigative or law enforcement officer" (as previously described);
- In an investigation involving sexual abuse of a child or certain sex crimes, authorizes use of a subpoena to compel production of records, documents, or other tangible things;
- In an investigation of sexual abuse of a child, authorizes use of a subpoena to obtain disclosure of (noncontent) basic subscriber information;
- Specifies requirements for the issuance of a subpoena;
- Authorizes a subpoenaed person to petition a court for an order modifying or setting aside a prohibition on disclosure;
- Authorizes, under certain circumstances, retention of subpoenaed records, documents, or other tangible objects;
- Prohibits the disclosure of a subpoena for a specified period if the disclosure might result in an adverse result, and provides exceptions;
- Requires an investigative or law enforcement officer to maintain a true copy of a written certification required for nondisclosure;
- Authorizes an investigative or law enforcement officer to apply to a court for an order prohibiting certain entities from notifying any person of the existence of a subpoena under certain circumstances;
- Authorizes an investigative or law enforcement officer to petition a court to compel compliance with a subpoena;
- Authorizes a court to punish a person who does not comply with a subpoena as indirect criminal contempt;
- Provides for criminal penalties;
- Precludes a cause of action against certain entities or persons for providing information, facilities, or assistance in accordance with terms of a subpoena;
- Provides for preservation of evidence pending issuance of legal process;
- Provides that certain entities or persons shall be held harmless from any claim and civil liability resulting from disclosure of specified information;
- Provides for reasonable compensation for reasonable expenses incurred in providing assistance; and
- Requires that a subpoenaed witness be paid certain fees and mileage.

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

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