

The Florida Senate
BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Rules

BILL: CS/CS/SB 618

INTRODUCER: Judiciary Committee; Criminal Justice Committee; and Senator Baxley and others

SUBJECT: Subpoenas in Investigations of Sexual Offenses

DATE: February 14, 2018

REVISED: _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	<u>Erickson</u>	<u>Jones</u>	<u>CJ</u>	<u>Fav/CS</u>
2.	<u>Tulloch</u>	<u>Cibula</u>	<u>JU</u>	<u>Fav/CS</u>
3.	<u>Erickson</u>	<u>Phelps</u>	<u>RC</u>	<u>Pre-meeting</u>

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/SB 618 addresses the use of an investigatory subpoena to obtain a customer's information from an electronic communications or remote computing service in an investigation involving allegations of sexual abuse of a child or the suspected commission of certain sex crimes. Of particular significance, the bill extends the period of time in certain sex crime investigations during which notice of the existence of a subpoena to the customer may be delayed, but only if the subpoena is used to obtain the contents of a communication that has been in electronic storage for more than 180 days.

Specifically, the bill provides that in investigations involving sexual abuse of a child, an investigative or law enforcement officer may:

- Without notice to the subscriber or customer of a provider of an electronic communication service or remote computing service, use a subpoena to obtain information pertaining to the subscriber or customer, excluding contents of a communication; and
- With prior notice or delayed notice, use a subpoena to obtain contents of a communication that has been in electronic storage in an electronic communications system for more than 180 days.

An investigative or law enforcement officer may prohibit a subpoena recipient from disclosing to any person for 180 days the existence of the subpoena or delay required notification 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.

Limited disclosure of the subpoena, however, is authorized. A court may grant an extension of the nondisclosure period or the delay of notification.

The bill also: authorizes a petition to modify or set aside a subpoena or disclosure prohibition; permits the retention of subpoenaed information for specific uses; specifies what notice is required; specifies procedures for retention of records; provides for compensation of a subpoenaed witness and others; provides legal protections for subpoena compliance; and authorizes a court to compel compliance with a subpoena and to sanction refusal to comply.

II. Present Situation:

Subpoenas and Criminal Investigations

Subpoenas Generally

A “subpoena,” which literally means “under penalty,”¹ 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.² 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.³ The subpoena duces tecum is used to compel production of documents, materials, or other tangible information.⁴

Subpoenas may generally be used by any party in a legal action as an investigative tool. For example, after a civil lawsuit alleging a breach of contract is filed, either side may obtain a subpoena to compel discovery of evidence pertaining to the alleged breach. In a criminal case, after the defendant is officially charged by an information or indicted, the defendant has a constitutional right to subpoena defense witnesses to testify during trial.⁵

Criminal Investigations Generally

A criminal investigation “begins when a victim, or one having knowledge of a crime, files a sworn statement . . . known as a complaint” with the proper authority.⁶ “Once a complaint has been investigated, and the complaint is found to have probable cause, a crime can be charged either by information or indictment.”⁷ “An information is a sworn document signed by the prosecuting authority . . . which charges a person with [a] violation of the law.”⁸ In Florida,

¹ Webster’s New World College Dictionary, 5th Ed. (2014).

² Op. Att’y Gen. Fla. 81-65 (1981) (citations omitted), available at <http://www.myfloridalegal.com/ago.nsf/Opinions/6515E4FA246990B085256587004F3F07> (last visited on Jan. 12, 2018).

³ “What is a Subpoena?,” FindLaw, available at <http://litigation.findlaw.com/going-to-court/what-is-a-subpoena.html> (last visited on Jan. 12, 2018).

⁴ *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 (on file with the Senate Committee on the Judiciary).

⁵ Trial Handbook for Florida Lawyers, s. 12:7 *Subpoena duces tecum* (3d ed.).

⁶ Florida Office of the Attorney General, Office of Statewide Prosecution, *A Guide for Victims*, <http://myfloridalegal.com/pages.nsf/Main/e99f7f48df3b5d7485256cca0052aa0f> (last visited Jan. 18, 2018).

⁷ *Id.*

⁸ *Id.*

“[a]n information may charge any crime except a crime punishable by death.”⁹ On the other hand, “[a]n indictment is a charging document filed by a grand jury and may indict on any crime.”¹⁰ “A grand jury consists of 18 citizens who hear allegations and evidence brought before them by the prosecuting authority and decide who, if anyone, should be charged with what crime(s).”¹¹

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 occurring.”¹² “[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.”¹³ “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.”¹⁴

Thus, to carry out its investigative duties, the State has “the authority to issue an investigative subpoena duces tecum.”¹⁵ As Florida courts have often recognized, the “the state attorney acts as a one-person grand jury in carrying out investigations into noncapital criminal conduct”¹⁶ 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 (the sworn document noted above). 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.”¹⁷

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.¹⁸ 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.¹⁹

“The decision to charge and prosecute criminal offenses is an executive responsibility over which the state attorney has complete discretion[.]”²⁰ “The State clearly has a strong interest in

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² *State v. Investigation*, 802 So. 2d 1141, 1144 (Fla. 2d DCA 2001).

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *State v. Investigation*, 802 So. 2d 1141, 1143–44 (Fla. 2d DCA 2001).

¹⁶ *Id.* at 144 (citing *Doe v. State*, 634 So. 2d 613, 615 (Fla. 1994); *Imparato v. Spicola*, 238 So. 2d 503, 506 (Fla. 2d DCA 1970); *State v. Nat’l Research Sys., Inc.*, 459 So.2d 1134, 1135 (Fla. 3d DCA 1984); Op. Att’y Gen. Fla. 94-86 (1994)). See also *State v. Gibson*, 935 So. 2d 611, 613 (Fla. 3d DCA 2006).

¹⁷ *Id.*

¹⁸ *State v. Jett*, 358 So.2d 875, 876-77 (Fla. 3d DCA 1978).

¹⁹ Section 943.03(8), F.S.

²⁰ *Gibson*, 935 So. 2d at 613 (quoting *State v. Bloom*, 497 So. 2d 2, 3 (Fla.1986) (internal quotations omitted)).

gathering information relevant to an initial inquiry into suspected criminal activity[.]”²¹ However, the State’s investigative powers are not unlimited. Rather, “[a] judicial limit to this discretion arises where constitutional constraints are implicated.”²²

Investigative Subpoenas and the Fourth Amendment

Under both the United States and Florida Constitution, people have a right to be free from *unreasonable* searches and seizures.²³ The United States Supreme Court has explained that “[t]he Fourth Amendment protects people, not places,’ . . . and wherever an individual may harbor a reasonable ‘expectation of privacy,’ . . . he is entitled to be free from unreasonable governmental intrusion.”²⁴ “Of course, the specific content and incidents of this right must be shaped by the context in which it is asserted.”²⁵ “For ‘what the Constitution forbids is not all searches and seizures, but *unreasonable* searches and seizures.’”²⁶

In applying the foregoing Fourth Amendment principles to investigative subpoenas in *State v. Tsavaris*, the Florida Supreme Court held that “a properly limited” investigative subpoena “does not constitute an unreasonable search and seizure” so long as it is “not overly broad” but “properly limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.”²⁷ The Florida Supreme Court has also explained that “[s]ubpoenas duces tecum are different from search warrants and are indisputably less intrusive” in two major ways:

[1] While there is no opportunity to challenge a search warrant, a subpoena duces tecum is subject to a motion to quash *prior to the production* of the requested materials. [2] While a search warrant may involve the police rummaging through one’s belongings and may involve the threat or actual use of force, a subpoena duces tecum requires the subpoenaed person to *bring the materials sought* at a time and place described in the subpoena.²⁸

Thus, while “[a]n investigative subpoena has the potential to violate the Constitution of the United States or the Florida Constitution,”²⁹ a properly limited subpoena does not give rise to Fourth Amendment concerns. And when there is some concern over an investigative subpoena, a motion may be filed so that a court can “determine the reasonableness of the subpoena”³⁰ and ensure that “an unlawful warrantless search and seizure” is not “sanctioned under the guise of a subpoena duces tecum.”³¹

²¹ *Id.* (quoting *Doe v. State*, 634 So.2d 613, 615 (Fla.1994) (internal quotations omitted)).

²² *State v. J.M.*, 718 So.2d 316, 317 (Fla. 2d DCA 1998).

²³ *Terry v. Ohio*, 392 U.S. 1, 8 (1968) (“The Fourth Amendment provides that ‘the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.’”).

²⁴ *Id.* (quoting *Elkins v. United States*, 364 U.S. 206, 222 (1960), accord *Katz v. United States*, 389 U.S. 347, 351, 361 (1967)).

²⁵ *Id.*

²⁶ *Id.* (emphasis added).

²⁷ *State v. Tsavaris*, 394 So. 2d 418, 426–27 (Fla. 1981) (receded from by *Dean v. State*, 478 So. 2d 38, 41 (Fla. 1985), on other grounds (standing issue)).

²⁸ *Id.* (emphasis added).

²⁹ *State v. Investigation*, 802 So. 2d at 1146.

³⁰ *Id.* (citations omitted).

³¹ *Dean v. State*, 478 So. 2d 38, 41 (Fla. 1985).

While the court acts as a gatekeeper on the back end, some of the proper limitations of an investigatory subpoena are determined on the front end by statutes aimed at protecting the privacy of individuals. The federal Stored Communications Act, for example, limits what information an investigative body may obtain from a remote computing service or an electronic communication service. These services generally maintain information generated by a person's use of a computer service or an electronic device, such as a cell phone. For instance, an electronic communication service providing cell phone service maintains business records on subscribers for billing purposes which may be pertinent to a criminal investigation.³²

As explained in more detail below, the federal Stored Communications Act delineates when an investigatory subpoena may be used and when a search warrant or a court order must be obtained based on the type of information sought.

Section 92.605, F.S., and the 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).³³ 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
- The recipients or destinations of communications sent to or from those customers.³⁴

Under s. 92.605, F.S., when an out-of-state corporation subject to this section is properly served³⁵ by an applicant³⁶ 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.³⁷ 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

³² The "Stored Communications Act" is a term used to describe Title II of the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986), 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 Jan. 13, 2018). Title II of the ECPA is codified at 18 U.S.C. ss. 2701-2712.

³³ *Id.*

³⁴ Section 92.605(2), F.S.

³⁵ "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.

³⁶ "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.

³⁷ 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.

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.³⁸

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.³⁹

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.;⁴⁰
- Requires verification of the authenticity of produced records upon written request from the applicant or if ordered by the court;⁴¹
- 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.;⁴² and
- Provides for admissibility in evidence in a criminal proceeding of records produced in compliance with s. 92.605, F.S.⁴³

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

Major Features of Section 934.23, F.S.

Section 934.23, F.S., is patterned after the federal SCA. It closely tracks 18 U.S.C. s. 2703. “The SCA protects communications held by two defined classes of network service providers[.]”⁴⁴ Those classes are electronic communication service (ECS) providers and remote computing service (RCS) providers.⁴⁵

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, a wire or electronic communication held or maintained on a remote computing service, and a record or other information pertaining to a subscriber or customer of such service, not including the contents of a communication.

³⁸ Section 92.605(2)(b), F.S.

³⁹ 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.

⁴⁰ Section 92.605(2)(d), F.S.

⁴¹ Section 92.605(2)(e), F.S.

⁴² Section 92.605(4), F.S.

⁴³ Section 92.605(5)-(8), F.S. A Florida electronic communication service provider or remote computing service 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.

⁴⁴ *Supra*, n. 9, at p. 117.

⁴⁵ *Id.*

Section 934.23, F.S., also provides procedures for retention of records and other evidence pending issuance of process⁴⁶ and provides legal protections⁴⁷ and reasonable compensation for those providing assistance.⁴⁸

Terminology Relevant to Section 934.23, F.S.

Essential to an understanding of s. 934.23, F.S., is an understanding of the following terminology used in the section, most of which is patterned on terminology used in the SCA:

- “Contents,” when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.⁴⁹
- “Electronic communication” means the transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate, interstate, or foreign commerce. The definition does not include: any wire or oral communication; any communication made through a tone-only paging device; any communication from an electronic or mechanical device which permits the tracking of the movement of a person or an object; or electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.⁵⁰
- “Electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications.⁵¹
- “Electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.⁵²
- “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.⁵³

⁴⁶ 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.

⁴⁷ 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.

⁴⁸ 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.

⁴⁹ Section 934.02(7), F.S. This definition is identical to the definition in 18 U.S.C. s. 2510(8). “The contents of a network account are the actual files (including email) stored in the account.... For example, stored emails or voice mails are ‘contents,’ as are word processing files stored in employee network accounts. The subject lines of emails are also contents.” *Supra*, n. 9, at p. 122-123.

⁵⁰ Section 934.02(12), F.S. This definition is very similar to the definition in 18 U.S.C. s. 2510(12).

⁵¹ Section 934.02(15), F.S. This definition is identical to the definition in 18 U.S.C. s. 2510(15).

⁵² Section 934.02(14), F.S. This definition is identical to the definition in 18 U.S.C. s. 2510(14). Telephone companies and electronic mail companies are examples of “electronic communications service” providers. *Supra*, n. 9, at p. 117.

⁵³ Section 934.02(17), F.S. This definition is identical to the definition in 18 U.S.C. s. 2510(17). According to the U.S. Department of Justice (DOJ), “‘electronic storage’ refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system

- “Investigative or law enforcement officer” means any officer of the State of Florida or political subdivision thereof, of the United States, or of any other state or political subdivision thereof, who is empowered by law to conduct on behalf of the Government investigations of, or to make arrests for, offenses enumerated in this chapter or similar federal offenses, any attorney authorized by law to prosecute or participate in the prosecution of such offenses, or any other attorney representing the state or political subdivision thereof in any civil, regulatory, disciplinary, or forfeiture action relating to, based upon, or derived from such offenses.⁵⁴
- “Remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.⁵⁵
- “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.⁵⁶
- “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.⁵⁷

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 of provider possessing it.”⁵⁸ Section 934.23, F.S., mirrors this approach. The types of evidence obtainable by different means are discussed in detail below.⁵⁹

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

integrity. It does not include post-transmission storage of communications.” *Supra*, n. 9, at p. 123. Under the DOJ interpretation, an e-mail is only in “electronic storage” if not accessed by the recipient. *Id.* However, the federal Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), rejected this interpretation and “held that email messages were in ‘electronic storage’ regardless of whether they had been previously accessed[.]” *Supra*, n. 9, at p. 124-25, citing *Theofel*, 359 F.3d at 1075-77.

⁵⁴ Section 934.02(6), F.S. The definition in 18 U.S.C. 2510(7) refers to federal law enforcement officers and prosecutors.

⁵⁵ Section 934.02(19), F.S. This definition is identical to the definition in 18 U.S.C. s. 2711(2). “Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer.” *Supra*, n. 9, at p. 119.

⁵⁶ Section 934.02(23), F.S.

⁵⁷ Section 934.02(1), F.S. This definition is very similar to the definition in 18 U.S.C. s. 2510(1).

⁵⁸ *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. 9, 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 116.

⁵⁹ This analysis follows the format provided by the DOJ in its discussion of the SCA. *Supra*, n. 9.

including the contents of a communication, if the officer has the consent of the subscriber or customer to such disclosure.⁶⁰

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.⁶¹ 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.⁶²

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;⁶³
- 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 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.⁶⁴

⁶⁰ Section 934.23(4)(a)3., F.S. (similar to 18 U.S.C. s. 2703(c)(1)(C)).

⁶¹ Section 934.23(4)(a)4. and (4)(b), F.S.

⁶² 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. 9, at p. 121.

⁶³ Section 934.23(1) and (2)(b)1., F.S. (similar to 18 U.S.C. s. 2703(a) and (b)(1)(B)(i)).

⁶⁴ 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. 9, at p. 129.

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.⁶⁵

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.⁶⁶

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;⁶⁷ and
- Contents of an electronic communication that is held or maintained on a RCS as described in s. 934.23(3), F.S.⁶⁸

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
- Contents of a wire or electronic communication that has been held in electronic storage in an electronic communication system for 180 days or less.⁶⁹

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 evidence from an RCS provider under s. 934.23(2), F.S. (contents of communications in a RCS)

⁶⁵ 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. 9, at p. 130.

⁶⁶ 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. 9, at p. 122.

⁶⁷ Section 934.23(1), F.S. (similar to 18 U.S.C. s. 2703(a)).

⁶⁸ 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. 9, at p. 132.

⁶⁹ 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. 9, at p. 133.

pursuant to a court order for disclosure or subpoena, the officer may delay required notice under s. 934.23(2), F.S., for a period not exceeding 90 days as provided:

- Where a court order 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.”⁷⁰
- 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 official⁷¹ that there is reason to believe that notification of the existence of the subpoena may have an “adverse result”⁷² described in subsection (2).⁷³

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”⁷⁴ under subsection (2)).⁷⁵

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:
 - 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.⁷⁶

⁷⁰ 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).

⁷¹ 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)).

⁷² See n. 46, *supra*.

⁷³ 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)).

⁷⁴ See n. 46, *supra*.

⁷⁵ Similar to 18 U.S.C. s. 2705(a)(4).

⁷⁶ Similar to 18 U.S.C. s. 2705(a)(5) and (b).

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. (subpoena or court order for disclosure), 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”).⁷⁷

III. Effect of Proposed Changes:

The bill creates s. 934.255, F.S., which relates to subpoenas obtained by an investigative or law enforcement officer conducting 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. Of particular significance, the bill enlarges the period of delayed notification to the customer of the existence of the subpoena from 90 days under ss. 934.23 and 934.25, F.S., to 180 days. This extension of delayed notification applies only when the subpoena is used to obtain the *contents* of a communication that has been in electronic storage for more than 180 days during the investigation of certain sex crimes.

Definitions

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

- “Child” means a person under 18 years of age.
- “Deliver” is construed in accordance with completed delivery, as provided for in Rule 1.080(b) of the Florida Rules of Civil Procedure.
- “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 or Other Information

The bill authorizes use of a subpoena 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 crimes⁷⁸ to compel the production of records, documents, or other tangible objects and the testimony of the subpoena recipient to authenticate such information. This investigative subpoena does not apply

⁷⁷ See n. 46, *supra*. Similar to 18 U.S.C. s. 2705(b).

⁷⁸ 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.

to information held or maintained by an electronic communication service (ECS) provider or remote computing service (RCS) provider, 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, without notice to the subscriber or customer of an ECS provider or RCS provider, obtain records or other information pertaining to the subscriber or customer, not including the contents of a communication. This information consists of the basic subscriber identity and session information described in s. 934.23(4)(b), F.S.:

- 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.

In an investigation involving sexual abuse of a child, an investigative or law enforcement officer may, with notice to the subscriber or customer of a RCS provider or with delayed notice (see discussion, *infra*), obtain the contents of any wire or electronic communication that has been in electronic storage in an electronic communication system for more than 180 days. This information, which is the same information obtainable with a subpoena and prior notice as provided in s. 934.23(2)(b) and (3), F.S., consists of any electronic communication that is held or maintained on a remote computing service:

- On behalf of a subscriber or customer of such service and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of such service.
- 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.

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.

Petition for an Order Modifying or Setting Aside a Subpoena or Disclosure Prohibition

At any time before the date prescribed in the subpoena by which records, documents, or other tangible objects must be produced, a person or entity receiving a subpoena may, before a judge of competent jurisdiction, petition for an order modifying or setting aside the subpoena or 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.

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.⁷⁹ 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.

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.

Delay of Required Notification

For the contents of a communication that has been in electronic storage in an electronic communications system for more than 180 days, the bill authorizes an investigative or law enforcement officer to delay giving the notification required for a subpoena to obtain such content for 180 days, if the subpoena is accompanied by a written certification of a supervisory official stating that there is reason to believe that notification of the existence of the subpoena *may* have an adverse result. The investigator or law enforcement officer must maintain a true copy of the written certification.

⁷⁹ The bill defines an "adverse result" in conformity with section 934.25(2) and (6), F.S., as any of the following acts by a subpoena recipient: 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.

Extension of the Nondisclosure Period or Delay of Notification

A court may grant extensions of the nondisclosure period or period of delay of notification for up to 90 days each. An extension must be consistent with another provision of the bill authorizing an investigative or law enforcement officer to 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. Under this provision, 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.

Compelling Compliance with a Subpoena and Sanctioning Noncompliance

In the case of contumacy⁸⁰ 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 or delay of notification is in effect 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 by the officer of 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).

⁸⁰ 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 Jan. 13, 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 effective date of the bill is October 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:

The bill is substantially patterned after current law and does not appear to obligate the recipient of a subpoena to provide records or information beyond what the recipient is required to provide under current law. However, 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 bill is substantially patterned after current law and does not appear to authorize an investigative or law enforcement officer to obtain records or information beyond what may be obtained under current law. However, there may be a workload impact in regard to preparing and submitting written certifications relevant to nondisclosure or delay of notification, but that impact, if any, is 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:

None.

VIII. Statutes Affected:

This bill creates section 934.255 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 by Judiciary on January 18, 2018:

The Committee Substitute:

- Corrects a grammatical error in the bill's title; and
- Removes wording in subsection (7) to clarify that the customer or subscriber, not the subpoena recipient, causes the enumerated adverse results.

CS by Criminal Justice on January 9, 2018:

The Committee Substitute:

- Makes technical changes to correct referencing errors and remove inapplicable language.
- Removes references and terminology relating to investigations involving a child sexual offender's failure to register as a sexual predator or sexual offender.
- Makes conforming changes to further model the bill after provisions of ss. 943.23 and 934.25, F.S., which include: authorizing multiple 90-day court-ordered extensions of delay of notification and the nondisclosure period; incorporating procedures for retention of records and other evidence pending issuance of a court order or other process; and providing legal protections and reasonable compensation for those providing assistance with subpoena compliance.
- Removes a provision relating to service of process.
- Removes a provision that states that a subpoena may not compel the production of a record, etc., that would otherwise be protected from production.

- B. **Amendments:**

None.