HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: CS/HB 1249 Search of the Content, Information, and Communications of Cellular Phones, Portable Electronic Communication Devices, and Microphone-Enabled Household Devices
SPONSOR(S): Criminal Justice Subcommittee; Grant
TIED BILLS: **IDEN./SIM. BILLS:** SB 1256

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR or BUDGET/POLICY CHIEF
1) Criminal Justice Subcommittee	10 Y, 0 N, As CS	Bruno	Sumner
2) Justice Appropriations Subcommittee	11 Y, 0 N	Welty	Gusky
3) Judiciary Committee			

SUMMARY ANALYSIS

Currently, unlawful access of stored communications only addresses accessing a facility where electronic communications are stored. CS/HB 1249 significantly broadens the scope of conduct constituting the unlawful access of stored communications by including accessing a cell phone, portable electronic communication device, or microphone-enabled household device when used to obtain wire, oral, or electronic communications stored within the device.

The bill amends Chapter 934, F.S., relating to security of communications and surveillance, to:

- Expand the types of location tracking methods available to law enforcement to include:
  - Cell-site location data;
  - Precise global positioning satellite location data; and
  - Historical global positioning satellite location data.
- Provide that a court may issue a warrant based upon probable cause for a law enforcement officer to obtain cellular-site location data, precise global positioning satellite location data, or historical global positioning satellite data. The bill:
  - Requires a law enforcement officer to install a mobile tracking device within 10 days of the warrant's issuance, and
  - Provides time constraints on how long a mobile tracking device may be used or the location data may be obtained and the timeframe must be specified in the warrant.
- Require the law enforcement officer who executed the warrant to serve a copy of the warrant to the person who, or whose property, was tracked within 10 days after the surveillance timeframe specified in the warrant has ended.
- Authorize the court to delay the notice requirement for up to 90 days upon request of the law enforcement agency.
- Provide a definition of a "mobile tracking device" and allow for emergency location tracking under certain circumstances.

To the extent that persons are arrested for, charged with, and convicted of, the criminal offenses modified in the bill, this bill will have an indeterminate fiscal impact on state and local governments as these cases are processed through the criminal justice system.

The Criminal Justice Impact Conference (CJIC) considered this bill on February 12, 2018, and determined that the bill would increase the prison population by an insignificant amount.

The bill provides an effective date of July 1, 2018.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. EFFECT OF PROPOSED CHANGES:

Background

Fourth Amendment, Generally

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 reasonable expectation of privacy.[2] A warrantless search is generally per se unreasonable,[3] unless an exception to the warrant requirement applies.[4]

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

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

Searches of Cell Phones

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

In *Riley v. California*,[7] the U.S. Supreme Court held that law enforcement must obtain a search warrant to search the digital contents of a cell phone seized incident to arrest. The Court considered the advanced capabilities of modern cell phones, which it further noted "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[8] It reasoned that a modern smartphone's immense storage capacity allows that phone to carry tremendous quantity and variety of records regarding a person's private life, such as photographs, prescriptions, bank records, contacts, and videos.[9]

[1] U.S. CONST. AMEND. IV.
[2] *Katz v. United States*, 389 U.S. 347 (1967).
[3] *United States v. Harrison*, 689 F.3d 301, 306 (3d Cir.2012)
[4] Examples of exceptions to the warrant requirement include exigent circumstances, searches of motor vehicles, and searches incident to arrest.
[5] Fla. Const. Art. 1, s. 12.
[6] *Chimel v. California*, 395 U.S. 752 (1969).
[7] 134 S.Ct. 2473 (2014).
[8] Id. at 2484.
[9] Id. at 2489.

Wiretapping and Stored Communications

By Law Enforcement

Wiretapping generally refers to electronic or mechanical eavesdropping on communications.[10] Law enforcement use of a wiretap is subject to Fourth Amendment protections under the United States Constitution.[11]

In Florida, law enforcement officers may apply for an order authorizing the interception of wire, oral or electronic communication.[12] The requirements to obtain an interception order include the standard requirements of probable cause, oath or affirmation, and particularity as required with a search warrant, but the statute imposes a number of heightened requirements in order for law enforcement to intercept private wire, oral, or electronic communications. The application for an interception order must include:

- The identity of the investigative or law enforcement officer making the application and the officer authorizing the application.
- A full and complete statement of the facts and circumstances relied upon by the applicant to justify his or her belief that an order should be issued, including:
    - Details as to the particular offense that has been, is being, or is about to be committed.
    - A particular description of the nature and location of the facilities from which, or the place where, the communications are to be intercepted, with exceptions.
- A particular description of the type of communications sought to be intercepted.
- The identity of the person, if known, committing the offense and whose communications are to be intercepted.
- A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.
- A statement of the period of time for which the interception is required to be maintained and, if the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter.
- A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application.
- When the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception or a reasonable explanation of the failure to obtain such results.[13]

Additionally, the court may require an applicant to furnish additional testimony or documentary evidence in support of the application for an interception order. Only the Governor, the Attorney General, the statewide prosecutor, or any state attorney may authorize the application for an interception order, and the order must pertain to certain enumerated crimes.[14] Upon receiving such an order, a provider of wire, oral, or electronic communication service, or a landlord, custodian, or other person may not disclose the existence of any interception or the device used to accomplish the interception.[15]

[10] BLACK'S LAW DICTIONARY (10th ed. 2014), wiretapping.
[11] *Katz v. United States*, 389 U.S. 347 (1967).
[12] S. 934.09, F.S.
[13] Id.
[14] S. 934.07, F.S.
[15] S. 934.03(2)(a)3., F.S.

By the General Public

Wiretapping by the general public is prohibited under Florida law.[16] Subject to exceptions, it is a third degree felony[17] for a person to:

- Intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any wire, oral, or electronic communication;
- Intentionally use, endeavor to use, or procure any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:
    - Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
    - Such device transmits communications by radio or interferes with the transmission of such communication;
- Intentionally disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the illegal interception of a wire, oral, or electronic communication;
- Intentionally use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the illegal interception of a wire, oral, or electronic communication; or
- Intentionally disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication intercepted by authorized means when that person:
    - Knows or has reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation;
    - Has obtained or received the information in connection with a criminal investigation; and
    - Intends to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.[18]

The penalty for wiretapping may be decreased to a misdemeanor[19] under the following circumstances:

- The person has no prior wiretapping offenses;
- The conduct was not done for tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; and
- The intercepted communication was a radio communication that was not scrambled, encrypted, or transmitted using modulation techniques intended to preserve the privacy of such communication.[20]

Stored Communications

Separate from wiretapping, Florida law also criminally penalizes unlawful accessing stored communications by:

- Intentionally accessing without authorization a facility through which an electronic communication service is provided, or
- Intentionally exceeding an authorization to access such facility.[21]

The penalties for unlawfully accessing stored communications varies based on specific intent and number of offenses. If the offense is committed for the purpose of commercial advantage, malicious destruction or damage, or private commercial gain, it is a first degree misdemeanor for a first offense and a third degree felony for second and subsequent offenses.[22] If the offense was not committed for

[16] S. 934.03, F.S.
[17] A third degree felony is punishable by up to five years in prison and a $5,000 fine. SS. 775.082 & 775.083, F.S.
[18] S. 934.03(1), F.S.
[19] Misdemeanors are classified as either first- or second-degree. A first degree misdemeanor is punishable by up to 1 year in the county jail and a $1,000 fine. A second degree misdemeanor is punishable by up to 60 days in the county jail and a $500 fine. SS. 775.082 & 775.083, F.S. Under s. 934.03(4), F.S., wiretapping may be either a first- or second-degree misdemeanor, depending on the specific type of communication intercepted.
[20] S. 934.03(4), F.S.
[21] S. 934.21(1), F.S.
[22] S. 934.21(2)(a), F.S.

commercial advantage, malicious destruction or damage, or private commercial gain, it is a second degree misdemeanor.[23]

New Technologies

Several technologies now use microphone-enabled features. These devices may be activated in different ways. Some, such as many Smart TVs, require the user to manually activate the microphone by pressing a button.[24] Some respond to a trigger phrase that activates the device to begin transmitting information. These devices, which include many home assistant devices such as the Google Home and Amazon Echo, constantly "listen" for the trigger phrase in order to activate.[25] The devices record commands in order to fulfill the requests, and the recordings are stored remotely.[26] Other devices, such as baby-monitors and home security systems, are always recording.[27]

As these microphone-enabled devices grow in popularity, concerns mount about privacy. A security expert recently demonstrated how an Amazon Echo might be hacked.[28] Additionally, prosecutors in Arkansas requested to obtain recordings possibly made by an Amazon Echo in a murder case.[29]

Pen Registers and Trap and Trace Devices

Pen registers and trap and trace devices can track incoming and outgoing phone calls in real time. Historically, a pen register was understood to record the telephone numbers dialed from the target telephone, and a trap and trace device to record the telephone numbers from incoming calls to the target telephone.[30]

Florida law defines a pen register as a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but such information does not include the contents of any communication.[31] A trap and trace device under the statute means a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but such information does not include the contents of any communication.[32] Florida's definition of these terms are substantially similar to the definitions in the federal Pen Register Act.[33] The broader statutory definitions draw more types of non-content information under the purview of a pen register or trap and trace device orders.[34]

Law enforcement may only install a pen register or trap and trace device pursuant to an order under s. 934.33, F.S. The application for such an order must include:

- The identity of the applicant specified in the section and the identity of the law enforcement agency conducting the investigation; and

[23] S. 934.21(2)(b), F.S.
[24] Future of Privacy Forum, *Microphones and the Internet of Things* (August 2017), available at: https://fpf.org/wp-content/uploads/2017/08/Microphones-Infographic-Final.pdf (last visited January 22, 2018).
[25] Id.
[26] Nicole Chavez, *Arkansas judge drops murder charge in Amazon Echo case*, CNN (Dec. 2, 2017), available at: http://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html (last visited January 22, 2018).
[27] Supra FN 24.
[28] Jay McGregor, *Listening-in on a Hacked Amazon Echo is Terrifying*, Forbes (Sept. 7, 2017), available at: https://www.forbes.com/sites/jaymcgregor/2017/09/07/listening-in-on-a-hacked-amazon-echo-is-terrifying/#32744f415c7f (last visited January 22, 2018).
[29] Supra FN 26.
[30] *Tracey v. State*, 152 So.3d 504, 506 (Fla. 2014).
[31] S. 934.02(20), F.S.
[32] S. 934.02(21), F.S.
[33] 18 USC § 3127.
[34] For example, the U.S. Department of Justice used pen register orders to track real-time locations of a cell-phone using a cell-site simulator until September 2015. U.S. Department of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology* (Sept. 3, 2015), available at: https://www.justice.gov/opa/file/767321/download (last visited January 22, 2018).

- 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.[35]

The statutory requirement of relevancy to an ongoing criminal investigation falls short of the probable cause standard, as required for the issuance of a search warrant.

Case Law

In *Smith v. Maryland*,[36] the U.S. Supreme Court considered whether Fourth Amendment protections applied where the government installed and used a pen register at a telephone company's offices without a warrant to record the telephone numbers a target phone dialed. Through the pen register, law enforcement discovered that a telephone in Smith's home had been used to place a telephone call to a robbery victim who had received threatening calls. The Court held that there was no expectation of privacy in dialed telephone numbers, as they were voluntarily transmitted to the telephone company.[37]

The Florida Supreme Court (FSC) considered a pen register and trap and trace order in *Tracey v. State*[38] in which law enforcement obtained not only numbers dialed but real-time location information. Officers in *Tracey* applied for the numbers associated with incoming and outgoing calls; however, the phone company also provided real-time cell-site location information, which officers used to track Tracey's location and movements.[39] The FSC held that the real-time location tracking of Tracey through his cell phone was a search under the Fourth Amendment and therefore required either a warrant or an exception to the warrant requirement.

Mobile Tracking Devices

A mobile tracking device is an electronic or mechanical device which permits the tracking of the movement of a person or object, such as a GPS tracker.[40] Law enforcement officers are authorized to install mobile tracking devices for the purpose of collecting tracking and location information after a court order is issued under s. 934.42(2), F.S. The statute requires law enforcement to provide a statement to the court that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the investigating agency.[41] A certification of relevance is a lower standard than probable cause standard required for obtaining a lawful warrant.

In 2012, the United States Supreme Court addressed mobile tracking devices in *United States v. Jones*.[42] The Court held that the installation of a GPS tracking device on a vehicle without a warrant violated the Fourth Amendment as an unlawful search.[43] Prior to the *Jones* decision, installation of a mobile tracking device was not considered a search when used to track a person's public movements.[44] As searches are generally per se unreasonable absent a warrant, it is likely that the *Jones* decision requires a warrant, supported by probable cause, for installation of a mobile tracking unit.

Historical Cell Site Data

Cell phones connect to cell sites or base towers in order to make calls, send text messages, use data, and perform other functions.[45] These cell sites are located at fixed geographic locations. The phone

[35] S. 934.32(2), F.S.
[36] 442 U.S. 735 (1979).
[37] Id. at 742-44.
[38] 152 So.3d 504 (Fla. 2014).
[39] Id. at 507-508.
[40] S. 934.42, F.S.
[41] S. 934.42(2)(b), F.S.
[42] 565 U.S. 400 (2012).
[43] Id.
[44] *United States v. Knotts*, 460 U.S. 276 (1983).
[45] Center for the Advancement of Public Integrity, *Does Seeking Cell Site Location Information Require a Warrant? The Current State of Law in a Rapidly Changing Field* (August 1, 2016), available at: http://www.law.columbia.edu/sites/default/files/microsites/public-

connects to the cell site with the strongest available signal and may connect to different cell sites as it moves through a coverage area.[46] The phone company keeps a record of the cell sites that a phone connects to for certain actions.[47] This data can approximate a person's location, although it is possible for a cell site to have a coverage area of approximately 2,700 miles[48] and for a phone to connect to a tower other than the one closest to it.[49]

Under current Florida law, law enforcement may obtain historical cell site data without a warrant under s. 934.23, F.S., which allows an officer to seek a court order compelling an electronic communication service provider to release records other than the content of communications.[50] To obtain such an order, the officer must offer specific and articulable facts showing that there are reasonable grounds to believe the records are relevant and material to an ongoing criminal investigation,[51] which is a lower standard than probable cause.

Florida's Fourth District Court of Appeals (4th DCA) considered whether obtaining historical cell site data requires a finding of probable cause and warrant in *Johnson v. State*.[52] The 4th DCA held that there was no expectation of privacy in the data because:

- The data is not content based; and
- The data reveals only a person's past location, rather than pinpointing a current location.[53]

Under the *Johnson* holding, if there is no expectation of privacy in historical cell site data, then law enforcement does not conduct a search under the Fourth Amendment by obtaining it. However, more recently, the FSC noted a federal circuit split on the issue of requiring a probable cause determination to obtain historical cell site data in *Tracey v. State*.[54] Although the FSC discussed historical cell site data in its analysis, the issue in *Tracey* related to pen register and trap and trace devices; therefore the FSC did not decide whether historical cell site data requires more than the statutory criteria under s. 934.23, F.S.[55]

The Sixth Circuit Court of Appeals (6th Circuit) addressed the issue of requiring probable cause to obtain historical cell site information in *U.S. v. Carpenter.*[56] The 6th Circuit held that the Government did not conduct a search, for Fourth Amendment purposes, when it obtained historical cell site data, and thus, government could obtain the records pursuant to Stored Communications Act,[57] based on reasonable grounds for believing that the records were relevant and material to an ongoing investigation.[58] Carpenter appealed, and the case is now pending before the U.S. Supreme Court.[59]

---

integrity/files/does_seeking_cell_site_location_information_require_a_search_warrant_-_wesley_cheng_-_august_2016_update_0.pdf (last visiting January 22, 2018).
[46] Id.
[47] Id.
[48] Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 Richmond J.L. & Tech.3 (2011), available at: http://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1354&context=jolt (last visited Jan. 21, 2018).
[49] Supra FN 17.
[50] S. 934.23(4)(a)2., F.S.
[51] S. 934.23(5), F.S.
[52] 110 So.3d 954 (Fla. 4th DCA 2013).
[53] Id. at 958.
[54] 152 So.3d 504 (Fla. 2014).
[55] Id. at 516.
[56] 819 F.3d 880 (6th Cir. 2016).
[57] The federal Stored Communications Act, 18 USC. § 2703(d), requires the same standard as Florida's s. 934.23(5), F.S. to obtain historical cell site data through a court order.
[58] *Carpenter*, 819 F.3d at 886.
[59] *Carpenter v. U.S.*, Docket No. 16-402, available at: https://www.supremecourt.gov/docket/docketfiles/html/public/16-402.html (last visited January 22, 2018).

Cell-Site Simulators

A cell-site simulator functions like a cellular tower.[60] The simulator causes each cellular device within a certain radius to connect and transmit its standard unique identifying number to the simulator.[61] Law enforcement can use this capability to help locate a cell phone whose unique identifying number is known or to determine the unique identifier of a cell phone in the simulator's proximity.[62] A cell-site simulator provides only the relative signal strength and general direction of a target phone; it does not have the same capabilities as a GPS locator.[63]

In 2015, the U.S. Department of Justice (USDOJ) issued written guidance on the use of a cell-site simulator. In this memorandum, USDOJ began requiring federal agencies to obtain a search warrant supported by probable cause in order to use a cell-site simulator.[64] The District of Columbia Court of Appeals,[65] U.S. District Court for Northern California,[66] and U.S. District Court for Southern New York[67] have held that use of a cell-site simulator constitutes a search under the Fourth Amendment, requiring either probable cause and a warrant or that an exception to the warrant requirement.

Criminal Punishment Code

The Criminal Punishment Code (Code) applies to all felony offenses, except capital felonies, committed on or after October 1, 1998."[68] Noncapital felonies sentenced under the Code receive an offense severity level ranking (Levels 1-10), either by being specifically listed in the offense severity ranking chart[69] or by default.[70]Judges must use the Criminal Punishment Code worksheet to compute a sentence score for each felony offender.[71]

Sentence points are assigned and accrue based on the level ranking assigned to the primary offense, additional offenses and prior offenses.[72] Sentence points increase as the offense severity level increases from Level 1 (least severe) to Level 10 (most severe). Sentence points are added for victim injury, and increase based on the type of injury and severity.[73] Sentence points may also be added or multiplied for other factors including possession of a firearm or the commission of certain offenses, such as drug trafficking.[74]

If total sentence points equal or are less than 44 points, the lowest permissible sentence is any nonstate prison sanction, unless the court determines that a prison sentence is appropriate. If total sentence points exceed 44 points, the lowest permissible sentence in prison months is calculated by subtracting 28 points from the total sentence points and decreasing the remaining total by 25 percent.[75]

---

[60] U.S. Department of Justice, *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, at 1 (Sept. 3, 2015), available at: https://www.justice.gov/opa/file/767321/download (last visited January 22, 2018).
[61] Id. at 2
[62] Id.
[63] Id.
[64] Id. at 3.
[65] *Jones v. U.S.*, Case No. 15-CF-322 (Sept. 21, 2017), available at: https://www.dccourts.gov/sites/default/files/2017-09/15-CF-322.pdf (last visited January 22, 2018).
[66] *U.S. v. Ellis*, Case No. 13-CR-00818, Pretrial Order No. 3 Denying Motions to Suppress (Aug. 24, 2017), available at: https://www.documentcloud.org/documents/3962321-Gov-Uscourts-Cand-273044-337-0.html (last visited January 22, 2018).
[67] *U.S v. Lambis*, Case No. 15cr734, Opinion and Order (July 12, 2016), available at: https://www.documentcloud.org/documents/2992109-Pauley-Stingray-Opinion-7-12-16.html#document/p6/a307678 (last visited January 22, 2018).
[68] s. 921.002, F.S.
[69] s. 921.0022, F.S.
[70] s. 921.0023, F.S., addresses ranking unlisted felony offenses. For example, an unlisted felony of the third degree is ranked within offense level 1.
[71] s. 921.0024, F.S.
[72] Id.
[73] Id.
[74] Id.
[75] s. 921.0022(2), F.S.

Absent mitigation,[76] the permissible range under the Code is generally the lowest permissible sentence scored up to and including the maximum penalty provided under s. 775.082, F.S.[77]

Effect of Proposed Changes

Wiretapping and Stored Communications

CS/HB 1249 amends the definition of oral communication to explicitly include communication recorded by a microphone-enabled device. The bill defines microphone-enabled device 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;
- That communicates with, by any means, another entity or individual; and
- That contains a microphone designed to listen for and respond to environmental cues.

By including communication recorded by a microphone-enabled device in the definition of oral communication, the bill ensures that communication intercepted through a microphone-enabled device is subject to Florida's wiretapping protections, including criminal penalties for those who violate the wiretapping statute and stringent requirements for law enforcement interception of such communication.

The bill significantly broadens the scope of conduct constituting unlawful access of stored communications by including accessing a cell phone, portable electronic communication device, or microphone-enabled household device when used to obtain wire, oral, or electronic communications stored within the device. Current law only covers accessing a facility where electronic communications are stored. The punishment scheme remains the same as current law:

- If the offense is committed for the purpose of commercial advantage, malicious destruction or damage, or private commercial gain, it is:
    - A first degree misdemeanor, punishable by up to 1 year in the county jail and a $1,000 fine, for a first offense; or
- An unranked third degree felony, punishable by up to 5 years in prison and a $5,000 fine, for second and subsequent offenses. An unranked third degree felony is a descriptive term for a noncapital felony that is not specifically ranked in the offense severity ranking chart in s. 921.0022, F.S. If the felony is not ranked in the chart, it is ranked pursuant to s. 921.0023, F.S., based on its felony degree. An unranked third degree felony is a Level 1 offense.
- If the offense was not committed for commercial advantage, malicious destruction or damage, or private commercial gain, it is a second degree misdemeanor, punishable by up to 60 days in the county jail and a $500 fine.

Location Tracking

The bill groups several types of location tracking methods available to law enforcement under s. 934.42, F.S., currently relating to mobile tracking devices. The bill expands the scope of this statute to also include:

- Cell-site location data;
- Precise global positioning satellite location data; or
- Historical global positioning satellite location data.

The bill requires the court to find probable cause and issue a warrant in order to authorize the use of any location tracking device. The officer must install the device within 10 days of the warrant's

[76] The court may "mitigate" or "depart downward" from the scored lowest permissible sentence if the court finds a mitigating circumstance. Section 921.0026, F.S., provides a list of mitigating circumstances.
[77] s. 921.0022(2), F.S.

issuance. Additionally, the bill places time constraints on how long such a device may be used; the timeframe in which the device is used must be specified in the warrant and may not exceed 45 days from when the warrant was issued. Upon a showing of good cause the court may grant one or more extensions. The extensions must also not exceed 45 days.

The bill imposes notice requirements for law enforcement use of a location tracking device. Within 10 days after the surveillance timeframe specified in the warrant, the officer executing the warrant must serve a copy on the person whom, or whose property, law enforcement tracked. The officer may serve this notice by delivering a copy to the person or leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who lives there and by mailing a copy to the person's last known address. The court may grant an extension of the notice requirement for up to 90 days upon law enforcement request.

The bill allows for the installation of a mobile tracking device before 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; and
- 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 the installation and use,

When tracking someone without a warrant under this provision of the bill, law enforcement must terminate the surveillance when the information sought is obtained, when the 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.

The bill provides an effective date of July 1, 2018.

B. SECTION DIRECTORY:

Section 1: Amends s. 934.01, F.S., relating to legislative findings.
Section 2: Amends s. 934.02, F.S., relating to definitions.
Section 3: Amends s. 934.21, F.S., relating to unlawful access to stored communications; penalties.
Section 4: Amends s. 934.42, F.S., relating to mobile tracking device authorization.
Section 5: Provides an effective date of July 1, 2018.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

   None.

2. Expenditures:

   The bill expands the scope of activity for which a person may be criminally liable for unlawfully accessing stored communications. To the extent that persons are arrested for, charged with and convicted of, the criminal offenses modified in the bill, this bill will have an indeterminate fiscal impact on state government.

   The Criminal Justice Impact Conference, which provides the final official estimate of a bill's prison bed impact, met on February 12, 2018, and determined the bill would have a "positive insignificant" prison bed impact (an increase of 10 or fewer prison beds).[78]

[78] Criminal Justice Impact Conference, Office of Economic and Demographic Research, Narrative Analysis of Adopted

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

None.

2. Expenditures:

The bill expands the scope of activity for which a person may be criminally liable for unlawfully accessing stored communications. To the extent that persons are arrested for, charged with and convicted of, the criminal offenses modified in the bill, this bill will have an indeterminate fiscal impact on local government.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

None.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

Not applicable. The does not appear to affect municipal or county governments.

2. Other:

None.

B. RULE-MAKING AUTHORITY:

Not applicable.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/ COMMITTEE SUBSTITUTE CHANGES

On January 24, 2018, the Criminal Justice Subcommittee adopted a strike-all amendment and reported the bill favorably as a committee substitute. The amendment:

- Removed all provisions changing the word “order” to “warrant” in the context of interception orders.
- Retained the requirement in current law that the prosecution must disclose the application and order authorizing interception of communications of intercepted communications at least 10 days before introducing the intercepted communications into evidence. The bill as originally filed had eliminated the 10 day component of this requirement.
- Removed other non-substantive provisions.

This analysis is drafted to the committee substitute as passed by the Criminal Justice Subcommittee.