BILL ANALYSIS

Senate Research Center
86R4850 JCG-F

S.B. 2093
By: Hughes
Criminal Justice
4/29/2019
As Filed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

In 2018, the United States Supreme Court issued *Carpenter v. United States* and held that a warrant must be issued prior to cell phone service-provided historical location data being accessed and used by law enforcement in the course of a criminal investigation. Similarly, in 2012, the United States Supreme Court issued a decision in *United States v. Jones*, which found that covert warrantless installation of a GPS tracking device on a suspect's vehicle that enabled police to remotely monitor the suspect's movements was a violation of privacy.

S.B. 2093 requires probable cause-based warrants for law enforcement to use cell site simulators or obtain cell site location records from cell phone service providers, and implements the warrant requirement for mobile tracking devices mandated by *Jones*. Additionally, the bill resolves inconsistencies between state and federal law related to warrant standards and durations and other issues and establishes additional public interest safeguards that surpass baselines articulated in judicial decisions or federal requirements.

As proposed, S.B. 2093 amends current law relating to subpoenas, orders, and warrants for the disclosure of location information, electronic customer communications records, and electronic customer data and for the use of pen registers, ESN readers, cell site simulators, and mobile tracking devices; and creates a criminal offense.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Article 18.02, Code of Criminal Procedure, as follows:

> Art. 18.02. GROUNDS FOR ISSUANCE. (a) Authorizes a search warrant to be issued to search for and seize:
>
> > (1)–(12) makes no changes to these subdivisions;
> >
> > (13) electronic customer communications records and electronic customer data held in electronic storage, rather than electronic customer data held in electronic storage, including the contents of and records and other information related to a wire communication or electronic communication held in electronic storage;
> >
> > (14) makes a nonsubstantive change to this subdivision; or
> >
> > (l5) location information.
>
> (b) Provides that for purposes of this article, rather than for purposes of Subsection (a)(13):
>
> > (1) makes no changes to this subdivision.

(2) "Electronic customer communications records," "electronic customer data," "electronic storage," and "location information," rather than "electronic customer data" and "electronic storage," have the meanings assigned by Article 18B.001 (Definitions)

SECTION 2. Amends Article 18.06(a), Code of Criminal Procedure, to require a search warrant issued under Article 18B.354 (Warrant Issued in This State: Application and Issuance of Warrant), and Articles 18B.221 and 18B.222 if requiring the disclosure of location information as defined by Article 18B.001, to be executed in the manner provided by Article 18B.355 (Warrant Issued in This State: Execution of Warrant) not later than the 11th day after the date of issuance, rather than to require a search warrant issued under Article 18B.354 to be executed in the manner provided by Article 18B.355 not later than the 11th day after the date of issuance.

SECTION 3. Amends Article 18B.001, Code of Criminal Procedure, by adding Subdivisions (1-a), (6-a), (9-a), and (9-b) and amending Subdivisions (4), (7), and (8), as follows:

(1-a) Defines "cell site simulator."

(4) Redefines "designated law enforcement office or agency" to mean:

(A) the sheriff's department of a county with a population of 3.3 million or more;

(B) a police department in a municipality with a population of 500,000 or more;

(C) the office of inspector general of the Texas Department of Criminal Justice;

(D) a special investigator under Article 2.122 (Special Investigations) when assisting a peace officer of this state in:

(i) apprehending a fugitive from justice charged with an offense under Article 18B.221(b)(2); or

(ii) resolving an emergency involving:

(a) an immediate life-threatening situation;

(b) conspiratorial activities characteristic of violent organized crime;

(c) an immediate threat to a national security interest;

(d) an ongoing attack on a protected computer, as defined by 18 U.S.C. Section 1030, that constitutes an offense under Section 33.02 (Breach of Computer Security), Penal Code, or an equivalent offense under federal law; or

(e) the report of the disappearance of an individual, including the report of a runaway individual younger than 18 years of age, or a report of a suicidal individual, where the report indicates the individual may be in danger based on the circumstances of the disappearance, including circumstances such as the age and mental or physical condition of the individual; or

(E) a prosecutor or assistant prosecutor in a county with a population of more than 800,000.

(6-a) Defines "electronic customer communications records."

(7) Redefines "electronic customer data" to mean data or records, other than location information or electronic customer communication records, that:

(A) are in the possession, care, custody, or control of a provider of an electronic communications service or provider of a remote computing service; and

(B) contain:

(i) information revealing the identity of customers of the applicable service;

(ii) information about a customer's use of the applicable service; and

(iii) information that identifies the recipient or destination of a wire or electronic communication sent to or by a customer.

Deletes existing Subparagraphs (iv) and (v) defining "electronic customer data" to include data or records, other than location information or electronic customer communication records, that contain the content of a wire or electronic communication sent to or by a customer and any data stored with the applicable service provider by or on behalf of a customer.

(8) Redefines "electronic storage" to mean storage of electronic customer data, electronic customer communications records, or location information in a computer, computer network, or computer system, regardless of whether the data is subject to recall, further manipulation, deletion, or transmission.

(9-a) Defines "immediate life-threatening situation."

(9-b) Defines "location information."

SECTION 4. Amends Subchapter B, Chapter 18B, Code of Criminal Procedure, by adding Article 18B.050, as follows:

Art. 18B.050. APPLICABILITY. Provides that this subchapter (Application For Order Authorizing Installation and Use of Equipment) and Subchapters C (Order Authorizing Installation and Use of Equipment) and D (Emergency Installation and Use of Certain Equipment) do not apply to a cell site simulator.

SECTION 5. Amends Section 18B.151, Code of Criminal Procedure, as follows:

Art. 18B.151. EMERGENCY INSTALLATION AND USE OF PEN REGISTER OR TRAP AND TRACE DEVICE. (a) Deletes existing Subsection (a) defining "immediate life-threatening situation" and redesignates existing Subsection (b) as this subsection. Authorizes a peace officer authorized to possess, install, operate, or monitor a device under Subchapter E (Emergency Installation and Use of Interception Device), Chapter 18A, to install and use a pen register or trap and trace device if:

(1) another peace officer is designated to approve for the authorized officer's agency the emergency required disclosure of location information by:

(A) the head of the agency; and

(B) a district attorney or criminal district attorney with jurisdiction over all or part of the other officer's jurisdiction; and

(2) the peace officer described by Subdivision (1) approves the installation and use of a pen register or trap and trace device by reasonably determining that an emergency exists in the territorial jurisdiction of the authorized officer, or another officer the authorized officer is assisting, involving:

(A) an immediate life-threatening situation;

(B) conspiratorial activities characteristic of violent organized crime;

(C) an immediate threat to a national security interest;

(D) an ongoing attack on a protected computer, as defined by 18 U.S.C. Section 1030, that constitutes an offense under Section 33.02, Penal Code, or an equivalent offense under federal law; or

(E) the report of the disappearance of an individual, including the report of a runaway individual younger than 18 years of age, or a report of a suicidal individual, where the report indicates the individual may be in danger based on the circumstances of the disappearance, including circumstances such as the age and mental or physical condition of the individual.

Deletes existing text authorizing a peace officer authorized to possess, install, operate, or monitor a device under Subchapter E, Chapter 18A, to install and use a pen register or trap and trace device if the peace officer reasonably believes an immediate life-threatening situation exists that is within the territorial jurisdiction of the peace officer or another officer the peace officer is assisting and that requires the installation of a pen register or trap and trace device before an order authorizing the installation and use can, with due diligence, be obtained under this chapter, and there are sufficient grounds under this chapter on which to obtain an order authorizing the installation and use of a pen register or trap and trace device.

SECTION 6. Amends Article 18B.152, Code of Criminal Procedure, by adding Subsection (c), as follows:

(c) Requires the judge, in the event that no offense was readily apparent at the time of the installation and use of a pen register or trap and trace device under this subchapter, to note the exact date and time at which the likelihood that an offense occurred became apparent, if applicable. Requires the judge, if no offense became apparent before the conclusion of the emergency or issuance of an order authorizing continued use of the device under Subchapter B, to annotate the order to reflect that: "No affirmative investigative or prosecutive use may be made of any pen register or trap and trace records obtained pursuant to the device's emergency installation or use."

SECTION 7. Amends Article 18B.202(c), Code of Criminal Procedure, as follows:

(c) Requires the affidavit for an order to install and use a mobile tracking device to:

(1)–(4) makes no changes to these subdivisions; and

(5) state the facts and circumstances that provide the applicant with probable cause to believe that:

(A) makes no changes to this paragraph; and

(B) the installation and use of a mobile tracking device will produce:

(i) evidence of the offense;

(ii) the location of contraband, fruits of the offense, or other items illegally possessed;

(iii) the location of criminal instruments;

(iv) the identity of a person to be arrested; or

(v) the identity of a person being unlawfully restrained.

Deletes existing text requiring the affidavit to state the facts and circumstances that provide the applicant with a reasonable suspicion that the installation and use of a mobile tracking device is likely to produce information that is material to an ongoing criminal investigation of that criminal activity.

SECTION 8. Amends Article 18B.205, Code of Criminal Procedure, as follows:

Art. 18B.205. DURATION OF ORDER. (a) Provides that an order under this subchapter (Mobile Tracking Devices) expires not later than the 45th day after, rather than the 90th day after, the date that the mobile tracking device was activated in place on or within the vehicle, container, or item.

(b) Authorizes the judge, for good cause shown, to grant an extension for an additional 45-day period, rather than 90-day period.

SECTION 9. Amends Chapter 18B, Code of Criminal Procedure, by adding Subchapter E-1, as follows:

SUBCHAPTER E-1. WARRANT FOR USE OF CELL SITE SIMULATOR OR REQUIRING DISCLOSURE OF LOCATION INFORMATION

Art. 18B.221. WARRANT FOR USE OF CELL SITE SIMULATOR OR DISCLOSURE OF CERTAIN LOCATION INFORMATION. (a) Authorizes a district judge to issue a warrant:

(1) authorizing the use of a cell site simulator to obtain location information from a cellular telephone or other wireless communications device; or

(2) requiring the disclosure of location information by a service provider who has possession, care, custody, or control of the information, regardless of whether the location information is held at a location in this state or another state.

(b) Authorizes a district judge to issue a warrant described by Subsection (a), only:

(1) except as provided by Article 18B.230, on application by:

(A) a prosecutor; or

(B) an assistant prosecutor, if applying on request of:

(i) an authorized peace officer commissioned by the Department of Public Safety of the State of Texas (DPS); or

(ii) an authorized peace officer of a designated law enforcement office or agency; and

(2) for the investigation of:

(A) an offense under certain sections and chapters of the Penal Code or the Health and Safety Code;

(B) a felony under Chapter 71 (Organized Crime), Penal Code;

(C) any sex offense for which a person is subject to registration under Chapter 62 (Sex Offender Registration Program) and in which the victim was younger than 18 years of age at the time the offense was committed;

(D) an offense of another jurisdiction in the United States equivalent to an offense under Paragraph (A), (B), or (C), committed by a fugitive from justice, regardless of whether the offense was committed in this state or another jurisdiction; or

(E) an emergency for which a judge is authorized to issue a warrant under Article 18B.230.

(c) Requires an application under this article to:

(1) be made in writing under oath; and

(2) include:

(A) the name, department, agency, and address of the applicant;

(B) the offense being investigated and for which the application is being made;

(C) the case number or unique identifier assigned by the law enforcement agency to the investigation of the offense for which the application is being made;

(D) the name of:

(i) the customer or subscriber whose data or device is the subject of the application, if the application seeks location information related to a particular subscriber or customer and the name of the customer or subscriber is known to the applicant; and

(ii) the person who is the subject of the application, if that person is not described by Subparagraph (i); and

(E) the account number or unique identifier that is the subject of the application.

(d) Requires the accompanying affidavit to contain a statement of facts and circumstances demonstrating certain conditions have been met.

Art. 18B.222. WARRANT FOR MASS, INDISCRIMINATE LOCATION INFORMATION. (a) Authorizes a district judge, in accordance with the requirements of this subchapter for the application and issuance of a warrant requiring the disclosure of location information by a service provider, other than Articles 18B.221(c)(2)(D) and (E), to issue a warrant requiring the disclosure of location information by a provider of an electronic communications service or a remote computing service based on the location where an offense occurred if the application includes the location where the offense occurred and each provider on whom the warrant will be served.

(b) Prohibits the location information disclosed pursuant to a warrant issued under this article from being used to further an investigation unrelated to the investigation of the offense for which the warrant application was made, unless an authorized peace officer, prosecutor, or assistant prosecutor makes an application,

other than the warrant application, to a district judge to use the location information to further an unrelated investigation and shows good cause for that use.

(c) Prohibits a law enforcement agency holding location information disclosed pursuant to a warrant issued under this article, unless authorized by a district judge, from commingling:

(1) the location information determined relevant to the investigation of the offense for which the warrant application was made;

(2) the location information determined to be irrelevant to that investigation; and

(3) other than the location information described by Subdivision (1), each set of location information disclosed by a different provider pursuant to a warrant issued under this article.

(d) Authorizes a district judge to review similar applications for a warrant under this article and instruct an agency holding separately the location information under Subsection (c) to compare the information to determine whether the information is relevant to the cases or to other locations identified in similar applications.

Art. 18B.223. JURISDICTION. Requires an application under this subchapter to be filed in a judicial district in which is located:

(1) the headquarters of:

(A) the office of the prosecutor filing an application under this subchapter;

(B) a law enforcement agency that requests the prosecutor to file an application for a warrant under this subchapter or that proposes to execute the warrant, if one is issued under this subchapter; or

(C) a service provider required to disclose location information held in electronic storage;

(2) the site of the proposed use of a cell site simulator; or

(3) the billing, residential, or business address of the subscriber or customer of a provider of an electronic communications service or remote computing service who is the subject of the application.

Art. 18B.224. DURATION OF WARRANT. (a) Provides that a warrant issued under this subchapter authorizing the use of a cell site simulator is valid for a period not to exceed 30 days.

(b) Provides that a warrant issued under this subchapter requiring the ongoing disclosure of prospective location information is valid for a period not to exceed 60 days.

Art. 18B.225. USE OF LOCATION INFORMATION IN UNRELATED INVESTIGATION PROHIBITED. (a) Provides that, except as provided by Article 18B.222(b) or (d), location information obtained pursuant to a warrant issued under this subchapter:

(1) is prohibited from being used to further an investigation unrelated to the investigation of the offense for which the warrant application was made; and

(2) is authorized to be used to investigate or prosecute offenses and defendants related to the offense for which the warrant application was made.

Art. 18B.226. CERTAIN RESTRICTIONS ON USE OF CELL SITE SIMULATOR. (a) Provides that under a warrant issued under this subchapter authorizing the use of a cell site simulator:

(1) if the cell site simulator is used to locate a known person's wireless communications device, location information that is derived from the simulator's use and is irrelevant to locating the device is required to be deleted on the date the information was collected; and

(2) unless granted an exception by a district judge to the requirement described in this subdivision, if the cell site simulator is used to locate an unknown wireless communications device, location information that is derived from the simulator's use and is irrelevant to locating the device is required to be deleted not later than the 30th day after the date the simulator is first used, and not later than the earlier of the following:

(A) at the end of each 30-day period following the initial 30-day period described by this subdivision; or

(B) the expiration of the warrant.

(b) Authorizes the district judge who issues a warrant under this subchapter for the use of a cell site simulator to extend a period described by Subsection (a) if the applicant for the warrant shows good cause for the extension. Authorizes the judge to grant a subsequent extension only if the applicant shows good cause for the subsequent extension. Prohibits an extension granted under this subsection from exceeding 90 days, unless the judge makes a finding in the record that the circumstances of the investigation justify an extension longer than 90 days.

(c) Prohibits a district judge from issuing a warrant to authorize using or configuring a cell site simulator for, and prohibits a person acting under a warrant issued under this subchapter from using or configuring a cell site simulator for, intercepting, capturing, or collecting the content of any electronic communication or collecting information on the attendees of a public gathering.

Art. 18B.227. PRESERVATION OF CERTAIN LOCATION INFORMATION. (a) Provides that location information disclosed by a service provider pursuant to a warrant issued under this subchapter:

(1) is required to be preserved; and

(2) except as provided by 18B.222(b) or (d), is prohibited from being used in the investigation or prosecution of an offense unrelated to the offense for which the warrant application was made.

(b) Requires the attorney representing the state, as soon as practicable after receiving a timely request from a defendant, to produce and permit inspection and electronic and print duplication of the location information described by Subsection (a) by or on behalf of the defendant.

Art. 18B.228. WARRANTS SEALED. (a) Requires a district judge issuing a warrant under this subchapter to, notwithstanding any other law, other than Subsections (b) and (c), seal the warrant and applicable affidavit.

(b) Requires a judge to authorize the disclosure of the warrant and applicable affidavit to a defendant, or the attorney representing the defendant, in a criminal action, if the defendant or attorney makes a timely request for disclosure, or to the

public, if at an in camera hearing the judge finds that the warrant application or affidavit does not substantially comply with requirements for the issuance of a warrant under this subchapter.

(c) Requires a judge authorizing disclosure under Subsection (b) to redact information tending to reveal the identity of cooperating witnesses, informants, or undercover peace officers.

Art. 18B.229. NOTICE TO SUBSCRIBER OR CUSTOMER. Authorizes an authorized peace officer to require a provider of an electronic communications service or a provider of a remote computing service to disclose location information without giving the subscriber or customer notice if the officer obtains a warrant under this subchapter or the consent of the subscriber or customer.

Art. 18B.230. EMERGENCY USE OF CELL SITE SIMULATOR OR REQUIRED DISCLOSURE OF LOCATION INFORMATION. (a) Authorizes an authorized peace officer, subject to Subsections (c) and (d), to without a warrant require a service provider who has possession, care, custody, or control of location information to disclose the information, if certain conditions are met.

(b) Authorizes an authorized peace officer of DPS or a designated law enforcement office or agency, subject to Subsections (c) and (d), to without a warrant use a cell site simulator if the head of the authorized officer's agency or that person's designee approves the authorized officer's use of the cell site simulator by reasonably determining that certain conditions are met.

(c) Requires an authorized officer who requires disclosure of location information or uses a cell site simulator under Subsection (a) or (b) to:

(1) promptly report the required disclosure of location information or the use of the simulator to, as applicable:

(A) if using a cell site simulator, the prosecutor in the county in which the simulator is used; or

(B) if requiring the disclosure of location information, the prosecutor in the county where the peace officer's agency is headquartered; and

(2) within 48 hours after providing notice of the required disclosure or within 48 hours after the use of the simulator begins, as applicable, obtain a warrant under this subchapter authorizing the required disclosure or the use of the simulator.

(d) Requires the peace officer, if a warrant application is denied or is not issued within the 48-hour period, to delete the disclosed location information or terminate use of the cell site simulator promptly on the earlier of the denial of the warrant application or the expiration of 48 hours.

Art. 18B.231. EXECUTION OF WARRANT. Provides that Article 18B.355 (Warrant Issued in This State: Execution of Warrant) applies to the execution of a warrant issued under this subchapter in the same manner as the article applies to the execution of a warrant for electronic customer communications records.

Art. 18B.232. WARRANT ISSUED IN ANOTHER STATE. Requires any domestic entity that provides electronic communications services or remote computing services to the public to comply with a warrant issued in another state and seeking location information described by Article 18B.221, if the warrant is served on the entity in a manner equivalent to the service of process requirements provided by Article 18B.355(b) (relating to authorizing certain warrants to be served only to certain communications

services and providers doing business in this state under a contract or agreement with a resident of this state if any part of the contract or agreement is to be performed in this state).

SECTION 10. Amends Article 18B.351, Code of Criminal Procedure, as follows:

Art. 18B.351. New heading: GOVERNMENT ACCESS TO ELECTRONIC CUSTOMER COMMUNICATIONS RECORDS AND ELECTRONIC CUSTOMER DATA. (a) Authorizes an authorized peace officer to require a provider of an electronic communications service or a provider of a remote computing service to disclose electronic customer communications records or electronic customer data, rather than to disclose electronic customer data, that is in electronic storage by obtaining a warrant under Article 18B.354.

(b) Authorizes an authorized peace officer to require a provider of an electronic communications service or a provider of a remote computing service to disclose electronic customer data without giving the subscriber or customer notice in a certain manner, rather than authorizing an authorized peace officer to require a provider of an electronic communications service or a provider of a remote computing service to disclose only electronic customer data that is information revealing the identity of customers of the applicable service or information about a customer's use of the applicable service, without giving the subscriber or customer notice in a certain manner.

SECTION 11. Amends Article 18B.352(a), Code of Criminal Procedure, as follows:

(a) Requires a court to issue an order authorizing disclosure of electronic customer data related to a wire or electronic communication held in electronic storage, rather than disclosure of contents, records, or other information of a wire or electronic communication held in electronic storage, if the court determines that there is a reasonable belief that the information sought is relevant and material to an ongoing criminal investigation, rather than to a legitimate law enforcement inquiry.

SECTION 12. Amends Article 18B.353, Code of Criminal Procedure, as follows:

Art. 18B.353. WARRANT ISSUED IN THIS STATE: APPLICABILITY. Provides that Articles 18B.354–18B.357 apply to a warrant required under Article 18B.351 to obtain electronic customer communications records or electronic customer data, rather than to obtain electronic customer data, including the contents of a wire or electronic communication.

SECTION 13. Amends Articles 18B.354(a), (b), and (c), Code of Criminal Procedure, as follows:

(a) Authorizes a district judge, on the filing of an application by an authorized peace officer, to issue a search warrant under this article for electronic customer communications records or electronic customer data held in electronic storage by a provider of an electronic communications service or a provider of a remote computing service described by Article 18B.355(b), regardless of whether the electronic customer communications records or electronic customer data is held at a location in this state or another state, rather than authorizing a district judge, on the filing of an application by an authorized peace officer, to issue a search warrant under this article for electronic customer data held in electronic storage, including the contents of and records and other information related to a wire or electronic communication held in electronic storage, by a provider of an electronic communications service or a provider of a remote computing service described by Article 18B.355(b), regardless of whether the customer data is held at a location in this state or another state.

(b) Prohibits a search warrant from being issued under this article (Warrant Issued in This State: Application and Issuance of Warrant) unless the sworn affidavit required by Article

18.01(b) (relating to requiring search warrants to demonstrate probable cause in order to be issued) provides sufficient and substantial facts to establish probable cause that:

(1) makes no changes to this subdivision; and

(2) the electronic customer communications records or electronic customer data sought, rather than the electronic customer data sought:

(A) constitutes evidence of that offense or evidence that a particular person committed that offense, or reveals the location of a fugitive from justice charged with a felony offense described by Article 18B.221(b)(2)(A), (B), (C), or (D), rather than constitutes evidence of that offense or evidence that a particular person committed that offense; and

(B) makes no changes to this paragraph.

(c) Authorizes only the electronic customer communications records or electronic customer data described in the sworn affidavit required by Article 18.01(b), rather than electronic customer data described in the sworn affidavit required by Article 18.01(b), to be seized under the warrant.

SECTION 14. Amends Article 18B.356(c), Code of Criminal Procedure, as follows:

(c) Requires the service provider to produce all electronic customer communications records, electronic customer data, and other information sought, rather than all electronic customer data, contents of communication, and other information sought, regardless of where the information is held and within the period allowed for compliance with the warrant, as provided by Subsection (a) (relating to requiring a district judge to indicate certain information in a warrant for electronic communications including a deadline or compliance) or (b) (relating to authorizing a district judge to indicate an earlier deadline for providers of electronic communications under certain circumstances)

SECTION 15. Amends Articles 18B.406(a) and (d), Code of Criminal Procedure, as follows:

(a) Requires the motion to quash the subpoena to contain an affidavit or other sworn statement stating:

(1) makes no changes to this subdivision; and

(2) the applicant's reasons for believing that the electronic customer data sought is not relevant and material to an ongoing criminal investigation, rather than that the customer data sought is not relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(d) Makes conforming changes to this subsection.

SECTION 16. Amends Article 18B.451, Code of Criminal Procedure, as follows:

Art. 18B.451. SUBPOENA AUTHORITY. (a) Creates an exception under Subsection (b) to the authority of the director of DPS or the director's designee, the inspector general of the Texas Department of Criminal Justice or the inspector general's designee, or the sheriff or chief of a designated law enforcement agency or the sheriff's or chief's designee to issue an administrative subpoena to a communication common carrier or a provider of an electronic communications service to compel the production of any carrier's or service provider's business records that meet certain criteria.

(b) Prohibits a person described by Subsection (a) from compelling the production of business records containing location information or electronic customer

communications records by issuing an administrative subpoena under Subsection (a).

SECTION 17. Amends Article 18B.501(a), Code of Criminal Procedure, to authorize an authorized peace officer seeking electronic customer communications records or electronic customer data, rather than electronic customer data, under Article 18B.351 to apply to the court for an order commanding the service provider to whom a warrant, subpoena, or court order is directed not to disclose to any person the existence of the warrant, subpoena, or court order.

SECTION 18. Amends Articles 18B.503(a) and (b), Code of Criminal Procedure, as follows:

(a) Requires an authorized peace officer who obtains electronic customer communications records or electronic customer data under Article 18B.351 or 18B.359 (Government Access to Certain Stored Customer Data Without Legal Process) or other information under this chapter, except as provided by Subsection (c) (relating to Subsection (a) not applying to records or other information maintained by a communication common carrier and that relates to certain telephone toll records or certain telephone listings), to reimburse the person assembling or providing the records, data, or information for all costs that are reasonably necessary and that have been directly incurred in searching for, assembling, reproducing, or otherwise providing the records, data, or information, including costs arising from necessary disruption of normal operations of a provider of an electronic communications service or a provider of a remote computing service in which the electronic customer communications records or electronic customer data may be held in electronic storage or in which the other information may be stored, rather than requiring an authorized peace officer who obtains electronic customer data under Article 18B.351 or 18B.359 or other information under this chapter, except as provided by Subsection (c), to reimburse the person assembling or providing the data or information for all costs that are reasonably necessary and that have been directly incurred in searching for, assembling, reproducing, or otherwise providing the data or information, including costs arising from necessary disruption of normal operations of a provider of an electronic communications service or a provider of a remote computing service in which the electronic customer data may be held in electronic storage or in which the other information may be stored.

(b) Authorizes the authorized peace officer and the person providing the electronic customer communications records, electronic customer data or other information, rather than electronic customer data, or other information to agree on the amount of reimbursement. Requires the court that issued the order for production of the records, data, or information, rather than the court that issued the order for production of the data or information, if there is not an agreement, to determine the amount. Makes conforming changes.

SECTION 19. Amends Chapter 16, Penal Code, by adding Section 16.07, as follows:

Sec. 16.07. UNLAWFUL USE OF CELL SITE SIMULATOR. (a) Defines "cell site simulator," "communication common carrier," and "electronic communication" for purposes of this section.

(b) Provides that a person commits an offense if the person knowingly uses a cell site simulator to locate or identify a wireless communications device or intercept the content of an electronic communication.

(c) Provides that an offense under this section is a state jail felony.

(d) Provides that it is an affirmative defense to prosecution under this section that the actor meets certain criteria.

SECTION 20. Makes application of Chapter 18B, Code of Criminal Procedure, as amended by this Act, prospective.

SECTION 21. Effective date: September 1, 2019.