By: Hughes S.B. No. 2093

A BILL TO BE ENTITLED

AN ACT

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; creating a criminal offense.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Article 18.02, Code of Criminal Procedure, is amended to read as follows:

Art. 18.02. GROUNDS FOR ISSUANCE. (a) A search warrant may be issued to search for and seize:

(1) property acquired by theft or in any other manner which makes its acquisition a penal offense;

(2) property specially designed, made, or adapted for or commonly used in the commission of an offense;

(3) arms and munitions kept or prepared for the purposes of insurrection or riot;

(4) weapons prohibited by the Penal Code;

(5) gambling devices or equipment, altered gambling equipment, or gambling paraphernalia;

(6) obscene materials kept or prepared for commercial distribution or exhibition, subject to the additional rules set forth by law;

(7) a drug, controlled substance, immediate

precursor, chemical precursor, or other controlled substance property, including an apparatus or paraphernalia kept, prepared, or manufactured in violation of the laws of this state;

(8) any property the possession of which is prohibited by law;

(9) implements or instruments used in the commission of a crime;

(10) property or items, except the personal writings by the accused, constituting evidence of an offense or constituting evidence tending to show that a particular person committed an offense;

(11) persons;

(12) contraband subject to forfeiture under Chapter 59 of this code;

(13) electronic customer communications records and 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~~]; [~~or~~]

(14) a cellular telephone or other wireless communications device, subject to Article 18.0215; or

(15) location information.

(b) For purposes of this article [~~Subsection (a)(13)~~]:

(1) "Electronic communication" and "wire communication" have the meanings assigned by Article 18A.001.

(2) "Electronic customer communications records," "electronic customer data," [~~and~~] "electronic storage," and

"location information" [~~storage"~~] have the meanings assigned by Article 18B.001.

SECTION 2. Article 18.06(a), Code of Criminal Procedure, is amended to read as follows:

(a) A peace officer to whom a search warrant is delivered shall execute the warrant without delay and forthwith return the warrant to the proper magistrate. A search warrant issued under Article 18B.354, and Articles 18B.222 and 18B.223 if requiring the disclosure of location information, as defined by Article 18B.001, must be executed in the manner provided by Article 18B.355 not later than the 30th [~~11th~~] day after the date of issuance. In all other cases, a search warrant must be executed within three days from the time of its issuance. A warrant issued under this chapter, Chapter 18A, or Chapter 18B shall be executed within a shorter period if so directed in the warrant by the magistrate.

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

(1-a) "Cell site simulator" means a device that:

(A) locates or identifies a wireless communications device in the immediate vicinity of the simulator by simulating the functions of a wireless telecommunications network transceiver; and

(B) is designed to collect location information from the wireless communications device.

(4) "Designated law enforcement office or agency" means:

(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; [~~or~~]

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

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

(i) apprehending a person charged with an offense under Article 18B.222(b)(2); or

(ii) resolving an emergency situation involving:

(a) an immediate life-threatening situation;

(b) conspiratorial activities characteristic of an imminent threat from violent organized crime;

(c) 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

(d) 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, assistant prosecutor, or a

peace officer who is an investigator of a prosecutor's office in a county with a population of more than 800,000.

(6-a) "Electronic customer communications records" means data or records, other than location information or electronic customer data, that:

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

(B) contain:

(i) the content of a wire or electronic communication sent to or by the customer, including:

(a) information that identifies by name the recipient or destination of a wire or electronic communication;

(b) the draft form of a wire or electronic communication, regardless of whether the communication was sent; or

(c) a summary description of the content of a wire or electronic communication, such as file name, subject line, or uniform resource locator; or

(ii) the content of files or records owned or possessed by a customer that are stored by the applicable service provider by or on behalf of the customer.

(7) "Electronic customer data" means 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; or

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

[~~(iv) the content of a wire or electronic communication sent to or by a customer; and~~

[~~(v) any data stored with the applicable service provider by or on behalf of a customer~~].

(8) "Electronic storage" means 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. The term includes storage of a wire or electronic communication by an electronic communications service or a remote computing service.

(9-a) "Immediate life-threatening situation" has the meaning assigned by Article 18A.201.

(9-b) "Location information" means data or records, other than information identifying the subscriber or customer or the account with which a wireless communications device is associated or information composed of network transactional access

records unrelated to the location of a wireless communications device, that:

(A) suggest the physical location of a wireless communications device by identifying the first, intermediate, or last point through which a wire or electronic communication enters or departs the physical infrastructure of an electronic communications system, including data or records commonly known as cell site location information;

(B) are created by or accessible to a provider of an electronic communications system and designed to identify the physical location of a wireless communications device, including information commonly known as E911 or precision location information derived through a global positioning system or multi-lateration measurement; or

(C) are created by or accessed through the use of a cell site simulator.

SECTION 4. Subchapter B, Chapter 18B, Code of Criminal Procedure, is amended by adding Article 18B.0505 to read as follows:

Art. 18B.0505. APPLICABILITY. This subchapter and Subchapters C and D do not apply to the use of a cell site simulator.

SECTION 5. Article 18B.151, Code of Criminal Procedure, is amended to read as follows:

Art. 18B.151. EMERGENCY INSTALLATION AND USE OF PEN REGISTER OR TRAP AND TRACE DEVICE. [~~(a) In this article, "immediate life-threatening situation" has the meaning assigned by Article 18A.201.~~

[~~(b)~~] A peace officer authorized to possess, install, operate, or monitor a device under Subchapter E, Chapter 18A, may install and use a pen register or trap and trace device if:

(1) another peace officer is designated to approve for the authorized peace 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:

(A) an emergency situation exists in the territorial jurisdiction of the authorized peace officer, or another officer the authorized officer is assisting, involving:

(i) an immediate life-threatening situation;

(ii) conspiratorial activities characteristic of an imminent threat from violent organized crime;

(iii) if the authorized peace officer is assisting an employee, officer, or agent of the federal government, an immediate threat to a national security interest;

(iv) 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

(v) 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;

(B) installing and using the pen register or trap and trace device may resolve the emergency situation; and

(C) [~~the peace officer reasonably believes:~~

[~~(1) an immediate life-threatening situation exists that:~~

[~~(A) is within the territorial jurisdiction of the peace officer or another officer the peace officer is assisting; and~~

[~~(B) 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~~

[~~(2)~~] 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. Article 18B.152, Code of Criminal Procedure, is amended by adding Subsection (c) to read as follows:

(c) In the event that at the time of the installation and use of a pen register or trap and trace device under this subchapter it is not readily apparent that any offense has been committed, the judge shall note the exact date and time at which the likelihood

that an offense was committed became apparent, if applicable. If, before the conclusion of the emergency or issuance of an order authorizing continued use of the device under Subchapter B it did not become apparent that any offense was committed, the judge shall 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. Article 18B.202(c), Code of Criminal Procedure, is amended to read as follows:

(c) The affidavit must:

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

(2) identify the vehicle, container, or item to which, in which, or on which the mobile tracking device is to be attached, placed, or otherwise installed;

(3) state the name of the owner or possessor of the vehicle, container, or item identified under Subdivision (2);

(4) state the judicial jurisdictional area in which the vehicle, container, or item identified under Subdivision (2) is expected to be found; and

(5) state the facts and circumstances that provide the applicant with probable cause to believe [~~a reasonable suspicion~~] that:

(A) criminal activity has been, is, or will be committed; and

(B) the installation and use of a mobile tracking

device will [~~is likely to~~] 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 or location of a person to be arrested; or

(v) the identity or location of a person being unlawfully restrained [~~information that is material to an ongoing criminal investigation of that criminal activity~~].

SECTION 8. Article 18B.205, Code of Criminal Procedure, is amended to read as follows:

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

(b) For good cause shown, the judge may grant an extension for an additional 45-day [~~90-day~~] period.

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

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

Art. 18B.221. APPLICABILITY. This subchapter does not apply to a device used by the Texas Department of Criminal Justice, or a person under contract with the department, to detect contraband in a correctional facility.

Art. 18B.222. WARRANT FOR USE OF CELL SITE SIMULATOR OR

DISCLOSURE OF CERTAIN LOCATION INFORMATION. (a) A district judge may 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 provider of an electronic communications service or a provider of a remote computing service 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) A district judge may issue a warrant described by Subsection (a) only:

(1) except as provided by Article 18B.231, 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; or

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

(2) for the investigation of:

(A) an offense under:

(i) Section 19.02, Penal Code;

(ii) Section 19.03, Penal Code;

(iii) Section 20.03, Penal Code;

(iv) Section 20.04, Penal Code;

(v) Chapter 20A, Penal Code;

(vi) Section 21.02, Penal Code;

(vii) Section 21.11, Penal Code;

(viii) Section 22.01, Penal Code, if the offense is punishable as a felony;

(ix) Section 22.011, Penal Code;

(x) Section 22.02, Penal Code;

(xi) Section 22.021, Penal Code;

(xii) Section 22.04, Penal Code;

(xiii) Section 22.041, Penal Code;

(xiv) Section 28.02, Penal Code;

(xv) Section 29.02, Penal Code;

(xvi) Section 29.03, Penal Code;

(xvii) Section 30.02, Penal Code;

(xviii) Chapter 34, Penal Code;

(xix) Title 8, Penal Code;

(xx) Chapter 43, Penal Code;

(xxi) Chapter 481, Health and Safety Code, other than an offense under:

(a) Section 481.115(b), 481.1151(b)(1), 481.116(b), 481.1161(b)(1), (2), or (3), 481.117(b), 481.118(b), or 481.125(d) of that code; or

(b) Section 481.121(b) of that code, if the offense involves not more than one pound of marihuana;

(xxii) notwithstanding Subparagraph (xxi), any offense under Chapter 481, Health and Safety Code, involving fentanyl, alpha-methylfentanyl, or carfentanyl, or any derivative

of those substances, including any isomer, ester, ether, salt, or salt of an isomer, ester, or ether of those substances;

(xxiii) Chapter 483, Health and Safety Code; or

(xxiv) Chapter 485, Health and Safety Code;

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

(C) any sex offense for which a person is subject to registration under Chapter 62 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), regardless of whether the offense was committed in this state or another jurisdiction; or

(E) an emergency situation described by Article 18B.231(a)(2)(A).

(c) An application under this article must:

(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);

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

(F) if the application is requesting authorization to use a cell site simulator, a description of the manner and method of deploying the cell site simulator device, including:

(i) whether the use of the device is likely to result in the device collecting from a cellular telephone or other wireless communications device data that is not the subject of the application; and

(ii) procedures for mitigating the collection of extraneous data as described by Subparagraph (i).

(d) The accompanying affidavit must contain a statement of facts and circumstances demonstrating:

(1) probable cause that:

(A) an offense listed in Subsection (b)(2)(A), (B), (C), or (D) has been, is being, or will be committed; and

(B) the location information being sought or the use of a cell site simulator will reveal the location of:

(i) evidence of the offense;

(ii) contraband, fruits of the offense, or

other items illegally possessed;

(iii) criminal instruments;

(iv) a person to be arrested; or

(v) a person being unlawfully restrained; or

(2) that the use of a cell site simulator or the required disclosure of location information will resolve an emergency situation described by Article 18B.231(a)(2)(A).

Art. 18B.223. WARRANT FOR CERTAIN LOCATION INFORMATION. (a) The judge may issue a warrant requiring a provider of an electronic communications service or a provider of a remote computing service to disclose location information related to the commission of an offense based on an application for a warrant submitted without specifying any customer information required under Articles 18B.222(c)(2)(D) and (E), provided that the application:

(1) meets all other requirements of this subchapter; and

(2) includes:

(A) the location where the offense is alleged to have been committed; and

(B) each provider on whom the warrant will be served.

(b) The location information disclosed pursuant to a warrant issued under this article may not be 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:

(1) makes a separate application to a district judge to authorize the use of the location information to further an unrelated investigation; and

(2) states in the application described by Subdivision (1) specific and articulable facts showing good cause for that use.

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

(1) may not commingle:

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

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

(2) must keep separated by the criminal episode or location each set of location information described by Subdivision (1)(B).

(d) A district judge may 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.224. JURISDICTION. An application under this subchapter must 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 provider of an electronic communications service or a provider of a remote computing service holding in electronic storage location information for which the warrant is sought;

(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 a provider of a remote computing service who is the subject of the application.

Art. 18B.225. DURATION OF WARRANT. (a) 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) A warrant issued under this subchapter requiring the ongoing disclosure of prospective location information by a provider of an electronic communications service or a provider of a remote computing service is valid for a period not to exceed 60 days.

Art. 18B.226. USE OF LOCATION INFORMATION IN UNRELATED INVESTIGATION PROHIBITED. Except as provided by Article 18B.223(b) or (d), location information obtained pursuant to a warrant issued under this subchapter:

(1) may not be used to further an investigation unrelated to the investigation of the offense for which the warrant application was made; and

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

Art. 18B.227. CERTAIN RESTRICTIONS ON USE OF CELL SITE SIMULATOR. (a) 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 must 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 must 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) The district judge who issues a warrant under this subchapter for the use of a cell site simulator may extend a period described by Subsection (a) if the applicant for the warrant shows

good cause for the extension. The judge may grant a subsequent extension only if the applicant shows good cause for the subsequent extension. An extension granted under this subsection may not exceed 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) A district judge may not issue a warrant to authorize using or configuring a cell site simulator for the purpose of, and a person acting under a warrant issued under this subchapter may not use or configure a cell site simulator for the purpose of:

(1) intercepting, capturing, or collecting the content of any electronic communication; or

(2) collecting information on the attendees of a public gathering who are exercising any right under the First Amendment to the United States Constitution, including as part of a protest, demonstration, rally, political meeting, or religious gathering.

Art. 18B.228. PRESERVATION OF CERTAIN LOCATION INFORMATION. (a) Location information disclosed by a provider of an electronic communications service or a provider of a remote computing service pursuant to a warrant issued under this subchapter must be preserved by the attorney representing the state.

(b) As soon as practicable after receiving a timely request from a defendant, the attorney representing the state shall produce the location information described by Subsection (a) and permit inspection and electronic and print duplication of that information

by or on behalf of the defendant.

Art. 18B.229. WARRANTS AND AFFIDAVITS SEALED. (a) Notwithstanding any other law, other than Subsections (b) and (c), a district judge issuing a warrant under this subchapter shall seal the warrant and applicable affidavit.

(b) A judge shall authorize the disclosure of the warrant and applicable affidavit to:

(1) a defendant, or the attorney representing the defendant, in a criminal action, if the defendant or attorney makes a timely request for disclosure; or

(2) the public, if a criminal action has been filed based on evidence obtained as part of the investigation conducted under the case number or unique identifier included in the warrant application and each defendant in that criminal action has been convicted or acquitted.

(c) A judge authorizing disclosure under Subsection (b) shall redact all information revealing the identity of cooperating witnesses, informants, or undercover peace officers.

(d) This article may not be construed to affect any other right of access to public records or proceedings granted under any other law.

Art. 18B.230. NOTICE TO SUBSCRIBER OR CUSTOMER. An authorized peace officer may 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:

(1) a warrant under this subchapter and the court

issuing the warrant makes a finding that there is reason to believe that giving notice under this section may result in:

(A) endangering the life or physical safety of an individual;

(B) a suspect or defendant fleeing from prosecution;

(C) the destruction of or tampering with evidence;

(D) the intimidation of potential witnesses who may assist an investigation of an offense or testify at a legal proceeding; or

(E) otherwise jeopardizing an investigation or unduly delaying a trial; or

(2) the consent of the subscriber or customer.

Art. 18B.231. EMERGENCY USE OF CELL SITE SIMULATOR OR REQUIRED DISCLOSURE OF LOCATION INFORMATION. (a) Subject to Subsections (c) and (d), an authorized peace officer may without a warrant require a provider of an electronic communications service or a provider of a remote computing service who has possession, care, custody, or control of location information to disclose the information, if:

(1) a peace officer in the authorized peace officer's agency is designated to approve for the 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 agency's

jurisdiction; and

(2) the peace officer described by Subdivision (1) approves the authorized peace officer's requiring the disclosure of the information by reasonably determining that:

(A) an emergency situation exists in the territorial jurisdiction of the authorized peace officer, or another officer the authorized peace officer is assisting, involving:

(i) an immediate life-threatening situation;

(ii) conspiratorial activities characteristic of an imminent threat from violent organized crime;

(iii) if the authorized peace officer is assisting an employee, officer, or agent of the federal government, an immediate threat to a national security interest;

(iv) 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

(v) 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; and

(B) requiring the information may resolve the emergency situation.

(b) Subject to Subsections (c) and (d), an authorized peace officer of the department or a designated law enforcement office or agency may without a warrant use a cell site simulator if the head of the authorized peace officer's agency or that person's designee approves the authorized peace officer's use of the cell site simulator by reasonably determining that:

(1) an emergency situation described by Subsection (a)(2)(A) exists in the applicable judicial district under Article 18B.224; and

(2) use of the cell site simulator may resolve the emergency situation.

(c) An authorized peace officer who requires disclosure of location information or uses a cell site simulator under Subsection (a) or (b) shall:

(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) If a warrant application is denied or is not issued

within the 48-hour period, the peace officer shall 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 the 48-hour period.

Art. 18B.232. EXECUTION OF WARRANT. Article 18B.355 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.233. WARRANT ISSUED IN ANOTHER STATE. A provider of an electronic communications service or a provider of a remote computing service shall comply with a warrant issued in another state and seeking location information described by Article 18B.222, if the warrant is served on the service provider in a manner equivalent to the service of process requirements provided by Article 18B.355(b).

Art. 18B.234. REPORTING REQUIRED. Not later than April 1 of each year, each law enforcement office or agency employing a person who applies for a warrant under this subchapter shall annually post on the Internet website of the office or agency the following information:

(1) the number of warrants of all persons of the office or agency who applied for a warrant under this subchapter requesting authorization for use of a cell site simulator and the number of those warrants granted to those persons;

(2) the number of warrants of all persons of the office or agency who applied for a warrant under this subchapter requiring the disclosure of location information by a provider of an

electronic communications service or a provider of a remote computing service and the number of those warrants granted to those persons;

(3) the offense for which each warrant application under Subdivision (1) or (2) was made; and

(4) the number of persons who were located as a result of the location information obtained pursuant to a warrant issued under this subchapter and were charged with a felony.

SECTION 10. Article 18B.351, Code of Criminal Procedure, is amended to read as follows:

Art. 18B.351. GOVERNMENT ACCESS TO ELECTRONIC CUSTOMER COMMUNICATIONS RECORDS AND ELECTRONIC CUSTOMER DATA. (a) An authorized peace officer may 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 that is in electronic storage by obtaining a warrant under Article 18B.354.

(b) An authorized peace officer may 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:

(1) by obtaining an administrative subpoena authorized by statute;

(2) by obtaining a grand jury subpoena;

(3) by obtaining a court order under Article 18B.352;

(4) by obtaining a warrant under Article 18B.354;

(5) by obtaining the consent of the subscriber or customer to the disclosure of the data; or

(6) as otherwise permitted by applicable federal law.

SECTION 11. Article 18B.352(a), Code of Criminal Procedure, is amended to read as follows:

(a) A court shall issue an order authorizing disclosure of electronic customer data related to [~~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 [~~to a legitimate law enforcement inquiry~~].

SECTION 12. Article 18B.353, Code of Criminal Procedure, is amended to read as follows:

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

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

(a) On the filing of an application by an authorized peace officer, a district judge may issue a search warrant under this article for electronic customer communications records or 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 electronic customer communications records or electronic customer data is held at a location in this state or another state. An application made under this subsection must demonstrate probable cause for the issuance of the warrant and must be supported by the oath of the authorized peace officer.

(b) A search warrant may not be issued under this article unless the sworn affidavit required by Article 18.01(b) provides sufficient and substantial facts to establish probable cause that:

(1) a specific offense has been committed; and

(2) the electronic customer communications records or 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 person charged with a felony offense; and

(B) is held in electronic storage by the service provider on which the warrant is served under Article 18B.355(c).

(c) Only the electronic customer communications records or electronic customer data described in the sworn affidavit required by Article 18.01(b) may be seized under the warrant.

SECTION 14. Article 18B.356(c), Code of Criminal Procedure, is amended to read as follows:

(c) The service provider shall produce all electronic customer communications records, electronic customer data,

[~~contents of communications,~~] 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) or (b).

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

(a) Not later than the 14th day after the date a subscriber or customer receives notice under Article 18B.402, the subscriber or customer may file a written motion to quash the subpoena or vacate the court order in the court that issued the subpoena or court order. The motion must contain an affidavit or other sworn statement stating:

(1) that the applicant is a subscriber or customer of the provider of an electronic communications service or the provider of a remote computing service from which the electronic customer data held in electronic storage for the subscriber or customer has been sought; and

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

(d) The court shall rule on the motion as soon as practicable after the filing of the peace officer's response. The court shall deny the motion if the court finds that the applicant is not the subscriber or customer whose data is the subject of the subpoena or court order or that there is reason to believe that the

peace officer's inquiry is legitimate and that the data sought is relevant to that inquiry. The court shall quash the subpoena or vacate the court order if the court finds that the applicant is the subscriber or customer whose data is the subject of the subpoena or court order and that there is not a reason to believe that the data is relevant and material to an ongoing criminal investigation [~~a legitimate law enforcement inquiry~~] or that there has not been substantial compliance with the provisions of this chapter.

SECTION 16. Article 18B.451, Code of Criminal Procedure, is amended to read as follows:

Art. 18B.451. SUBPOENA AUTHORITY. (a) Except as provided by Subsection (b), the [~~The~~] director of the department 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 may 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:

(1) that:

(A) [~~(1)~~] disclose information about:

(i) [~~(A)~~] the carrier's or service provider's customers; or

(ii) [~~(B)~~] users of the services offered by the carrier or service provider; or

(B) are electronic customer data described by Article 18B.001(7)(B)(iii); and

(2) are material to a criminal investigation.

(b) A person described by Subsection (a) may not compel the production of business records containing location information or electronic customer communications records by issuing an administrative subpoena under Subsection (a).

SECTION 17. Article 18B.501(a), Code of Criminal Procedure, is amended to read as follows:

(a) An authorized peace officer seeking electronic customer communications records or electronic customer data under Article 18B.351 may 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. The order is effective for the period the court considers appropriate.

SECTION 18. Articles 18B.503(a) and (b), Code of Criminal Procedure, are amended to read as follows:

(a) Except as provided by Subsection (c), an authorized peace officer who obtains electronic customer communications records or electronic customer data under Article 18B.351 or 18B.359 or other information under this chapter shall 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.

(b) The authorized peace officer and the person providing the electronic customer communications records, electronic customer data, or other information may agree on the amount of reimbursement. If there is not an agreement, the court that issued the order for production of the records, data, or information shall determine the amount. If a court order was not issued for production of the records, data, or information, the court before which any criminal prosecution relating to the records, data, or information would be brought shall determine the amount.

SECTION 19. Chapter 16, Penal Code, is amended by adding Section 16.07 to read as follows:

Sec. 16.07. UNLAWFUL USE OF CELL SITE SIMULATOR. (a) In this section:

(1) "Cell site simulator" has the meaning assigned by Article 18B.001, Code of Criminal Procedure.

(2) "Communication common carrier" and "electronic communication" have the meanings assigned by Article 18A.001, Code of Criminal Procedure.

(b) 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) An offense under this section is a state jail felony.

(d) It is an affirmative defense to prosecution under this section that the actor:

(1) is an officer, employee, or agent of a communication common carrier and the actor uses a cell site simulator in the regular course of business of the carrier for the purpose of:

(A) protecting property or services provided by the carrier; or

(B) assisting another whom the actor reasonably believes to be a peace officer authorized to use a cell site simulator under Article 18B.222, Code of Criminal Procedure;

(2) is a person authorized to use a cell site simulator under Article 18B.222, Code of Criminal Procedure, and acted within the scope of that authorization; or

(3) obtained the effective consent of the owner or renter of the wireless communications device and the simulator was not used to commit an offense or other prohibited act.

SECTION 20. Chapter 18B, Code of Criminal Procedure, as amended by this Act, applies to the disclosure of certain information by a provider of a wire or electronic communications service or remote computing service or by a communication common carrier under a warrant, order, or other legal process on or after the effective date of this Act.

SECTION 21. This Act takes effect September 1, 2019.