# BILL ANALYSIS

C.S.S.B. 1052
By: Carona
Criminal Jurisprudence
Committee Report (Substituted)

## BACKGROUND AND PURPOSE

Internet communications companies often hold information and data that may be vital in the prosecution of an offense, particularly Internet crimes. To obtain a search warrant for electronic communications, law enforcement officers must apply for a local search warrant in an Internet company's jurisdiction, which is often located in a different state than the state in which the communications are held by a service provider. Interested parties contend that this limitation hampers law enforcement efforts to obtain evidence on Internet criminals, who are able to remove or change identifying data much faster than law enforcement can obtain warrants. In response to this problem, several states have enacted laws providing for the issuance of computer data warrants that address out-of-state jurisdiction when dealing with Internet data. In an effort to bring Texas laws regarding electronic data search warrants in line with other states and allow Texas to serve such warrants directly to out-of-state companies, C.S.S.B. 1052 seeks to provide for the issuance of a search warrant for certain electronic information held in electronic storage, regardless of whether the data or information is held at a location in Texas or in another state.

## RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

## ANALYSIS

C.S.S.B. 1052 amends the Code of Criminal Procedure to authorize a district judge to issue a search warrant for 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, by a provider of an electronic communications service or a provider of a remote computing service, regardless of whether the customer data is held at a location in Texas or at a location in another state. The bill requires an application for such a warrant to demonstrate probable cause for the issuance of the warrant and to be supported by the oath or affirmation of an authorized peace officer. The bill prohibits the issuance of such a warrant unless the required sworn affidavit sets forth sufficient and substantial facts to establish probable cause that a specific offense has been committed and the electronic customer data sought constitutes evidence of that offense or evidence that a particular person committed that offense and is held in electronic storage by the service provider on which the warrant is served. The bill limits the data that may be seized under the warrant to the electronic customer data described in the sworn affidavit, requires such a warrant to run in the name of "The State of Texas," and provides for such a warrant to be sealed.

C.S.S.B. 1052 requires the authorized peace officer to execute the warrant not later than the 11th day after the date of issuance, unless directed in the warrant by the district judge to execute the warrant within a shorter period. The bill authorizes such a warrant to be served only on a service provider that is a domestic entity or a company or entity otherwise doing business in Texas under a contract or a terms of service agreement with a Texas resident, if any part of that contract or agreement is to be performed in Texas. The bill requires the service provider to produce all

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. The bill authorizes a court to find any officer, director, or owner of a company or entity in contempt of court if the person by act or omission is responsible for the failure of the company or entity to comply with the warrant within the period allowed for compliance and establishes that the failure of a company or entity to timely deliver the information sought in the warrant does not affect the admissibility of that evidence in a criminal proceeding. The bill establishes that the warrant is served when the authorized peace officer delivers the warrant by hand, by facsimile transmission, or, in a manner allowing proof of delivery, by means of the United States mail or a private delivery service to a person considered an agent of the entity for service of process, notice, or demand as a matter of law, to the secretary of state if the secretary of state is acting as the entity's agent, or to any other person or entity designated to receive the service of process.

C.S.S.B. 1052 requires a district judge to indicate in the warrant that the deadline for compliance by the provider of an electronic communications service or the provider of a remote computing service is the 15th business day after the date the warrant is served if the warrant is to be served on a domestic entity or a company or entity otherwise doing business in Texas. The bill authorizes the extension of the deadline for compliance with a warrant served to the secretary of state acting as an entity's agent to a date that is not later than the 30th day after the date the warrant is served. The bill authorizes the judge to indicate in a warrant that the deadline for compliance is earlier than the 15th business day after the date the warrant is served if the officer makes a showing and the judge finds that failure to comply with the warrant by the earlier deadline would cause serious jeopardy to an investigation or undue delay of a trial or create a material risk of danger to the life or physical safety of any person, a material risk of flight from prosecution, a material risk of the tampering with or destruction of evidence, or a material risk of intimidation of potential witnesses. The bill requires the provider of an electronic communications service or remote computing service responding to such a warrant, if the authorized peace officer serving the warrant also delivers an affidavit form to the provider and notifies the provider in writing that an executed affidavit is required, to verify the authenticity of the customer data, contents of communications, and other information produced in compliance with the warrant by including with the information the affidavit form that is completed and sworn to by a person who is a custodian of the information or a person otherwise qualified to attest to its authenticity and states that the information was stored in the course of regularly conducted business of the provider and specifies whether it is the regular practice of the provider to store that information.

C.S.S.B. 1052 requires an authorized peace officer, on a service provider's compliance with such a warrant, to file a return of the warrant and a copy of the inventory of the seized property as required by statutory provisions relating to search warrant returns. The bill requires the district judge to hear and decide any motion to quash the warrant not later than the fifth business day after the date the service provider files the motion and authorizes the judge to allow the service provider to appear at the hearing by teleconference. The bill authorizes a provider of an electronic communications service or remote computing service responding to a warrant to request an extension of the compliance period if extenuating circumstances exist to justify the extension. The bill requires the district judge to grant a request for an extension based on those circumstances if the authorized peace officer who applied for the warrant or another appropriate authorized peace officer agrees to the extension or the district judge finds that the need for the extension outweighs the likelihood that the extension will cause an adverse circumstance described by the bill's provisions. The bill 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 information held in electronic storage if the warrant is served on the entity in a manner equivalent to the service of process requirements provided by the bill's provisions. The bill specifies that a search warrant required to be obtained under statutory provisions relating to a warrant for government access to stored communications is a search warrant issued under the bill's provisions.

C.S.S.B. 1052 redefines "electronic storage" to mean any storage of electronic customer data in a computer, computer network, or computer system, regardless of whether the data is subject to recall, further manipulation, deletion, or transmission, including any storage of a wire or electronic communication by an electronic communications service or a remote computing service, rather than a temporary, intermediate storage of a wire or electronic communication that is incidental to the electronic transmission of the communication or storage of a wire or electronic communication by an electronic communications service for purposes of backup protection of the communication. The bill defines "electronic customer data" to mean data or records that are acquired by or stored with the provider of an electronic communications service or a remote computing service and contain information revealing the identity of customers of the applicable service, information about a customer's use of the applicable service, information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the customer, the content of a wire communication or electronic communication sent to or by the customer, and any data stored by or on behalf of the customer with the applicable service provider.

**EFFECTIVE DATE**

On passage, or, if the bill does not receive the necessary vote, September 1, 2013.

**COMPARISON OF ORIGINAL AND SUBSTITUTE**

While C.S.S.B. 1052 may differ from the engrossed version in minor or nonsubstantive ways, the following comparison is organized and highlighted in a manner that indicates the substantial differences between the engrossed and committee substitute versions of the bill.

| SENATE ENGROSSED | HOUSE COMMITTEE SUBSTITUTE |
|---|---|
| SECTION 1. Article 18.02, Code of Criminal Procedure, is amended. | SECTION 1. Substantially the same as engrossed version. |
| SECTION 2. Subsection (a), Article 18.06, Code of Criminal Procedure, is amended. | SECTION 2. Same as engrossed version. |
| SECTION 3. Subsection (a), Article 18.07, Code of Criminal Procedure, is amended. | SECTION 3. Same as engrossed version. |
| SECTION 4. Subdivision (20), Section 1, Article 18.20, Code of Criminal Procedure, is amended. | SECTION 4. Same as engrossed version. |
| SECTION 5. Section 1, Article 18.21, Code of Criminal Procedure, is amended. | SECTION 5. Same as engrossed version. |
| SECTION 6. Subsections (a), (b), (c), and (d), Section 4, Article 18.21, Code of Criminal Procedure, are amended. | SECTION 6. Same as engrossed version. |
| SECTION 7. Article 18.21, Code of Criminal Procedure, is amended by adding Sections 5A and 5B to read as follows:<br>Sec. 5A. WARRANT ISSUED IN THIS STATE FOR STORED CUSTOMER DATA OR COMMUNICATIONS. (a) This section applies to a warrant required | SECTION 7. Article 18.21, Code of Criminal Procedure, is amended by adding Sections 5A and 5B to read as follows:<br>Sec. 5A. WARRANT ISSUED IN THIS STATE FOR STORED CUSTOMER DATA OR COMMUNICATIONS. (a) This section applies to a warrant required |

under Section 4 to obtain electronic customer data, including the contents of a wire communication or electronic communication.

(b) On the filing of an application by an authorized peace officer, a district judge may issue a search warrant under this section for 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, by a provider of an electronic communications service or provider of a remote computing service described by Subsection (g), regardless of whether the customer data is held at a location in this state or at a location in 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 or affirmation of the authorized peace officer.

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

(1) a specific offense has been committed; and

(2) the electronic customer data sought:

(A) constitutes evidence of that offense or evidence that a particular person committed that offense; and

(B) is held in electronic storage by the service provider on which the warrant is served under Subsection (h).

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

(e) A warrant issued under this section shall run in the name of "The State of Texas."

(f) Article 18.011 applies to an affidavit presented under Article 18.01(b) for the issuance of a warrant under this section, and the affidavit may be sealed in the manner provided by that article.

under Section 4 to obtain electronic customer data, including the contents of a wire communication or electronic communication.

(b) On the filing of an application by an authorized peace officer, a district judge may issue a search warrant under this section for 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, by a provider of an electronic communications service or provider of a remote computing service described by Subsection (h), regardless of whether the customer data is held at a location in this state or at a location in 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 or affirmation of the authorized peace officer.

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

(1) a specific offense has been committed; and

(2) the electronic customer data sought:

(A) constitutes evidence of that offense or evidence that a particular person committed that offense; and

(B) is held in electronic storage by the service provider on which the warrant is served under Subsection (i).

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

(e) A warrant issued under this section shall run in the name of "The State of Texas."

(f) Article 18.011 applies to an affidavit presented under Article 18.01(b) for the issuance of a warrant under this section, and the affidavit may be sealed in the manner provided by that article.

(g) The authorized peace officer shall execute the warrant not later than the 11th day after the date of issuance, except that the officer shall execute the warrant within a shorter period if so directed in the warrant by the district judge. For purposes of this subsection, a warrant is executed when the

warrant is served in the manner described by Subsection (i).

(g) A warrant under this section may be served only on a service provider that is a domestic entity or a company or entity otherwise doing business in this state under a contract or a terms of service agreement with a resident of this state, if any part of that contract or agreement is to be performed in this state. The service provider shall produce all 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 (i). A court may find any officer, director, or owner of a company or entity in contempt of court if the person by act or omission is responsible for the failure of the company or entity to comply with the warrant within the period allowed for compliance. The failure of a company or entity to timely deliver the information sought in the warrant does not affect the admissibility of that evidence in a criminal proceeding.

(h) A search warrant issued under this section is served when the authorized peace officer delivers the warrant by hand, by facsimile transmission, or, in a manner allowing proof of delivery, by means of the United States mail or a private delivery service to:

(1) a person specified by Section 5.255, Business Organizations Code;

(2) the secretary of state in the case of a company or entity to which Section 5.251, Business Organizations Code, applies; or

(3) any other person or entity designated to receive the service of process.

(i) The district judge shall indicate in the warrant that the deadline for compliance by the provider of an electronic communications service or the provider of a remote computing service is the 15th business day after the date the warrant is served if the warrant is to be served on a domestic entity or a company or entity otherwise doing business in this state, except that the deadline for compliance with a warrant served in accordance with Section 5.251, Business Organizations Code, may be extended to a date that is not later than the 30th day after the date the warrant is served. The judge may indicate in a warrant

(h) A warrant under this section may be served only on a service provider that is a domestic entity or a company or entity otherwise doing business in this state under a contract or a terms of service agreement with a resident of this state, if any part of that contract or agreement is to be performed in this state. The service provider shall produce all 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 (j). A court may find any officer, director, or owner of a company or entity in contempt of court if the person by act or omission is responsible for the failure of the company or entity to comply with the warrant within the period allowed for compliance. The failure of a company or entity to timely deliver the information sought in the warrant does not affect the admissibility of that evidence in a criminal proceeding.

(i) A search warrant issued under this section is served when the authorized peace officer delivers the warrant by hand, by facsimile transmission, or, in a manner allowing proof of delivery, by means of the United States mail or a private delivery service to:

(1) a person specified by Section 5.255, Business Organizations Code;

(2) the secretary of state in the case of a company or entity to which Section 5.251, Business Organizations Code, applies; or

(3) any other person or entity designated to receive the service of process.

(j) The district judge shall indicate in the warrant that the deadline for compliance by the provider of an electronic communications service or the provider of a remote computing service is the 15th business day after the date the warrant is served if the warrant is to be served on a domestic entity or a company or entity otherwise doing business in this state, except that the deadline for compliance with a warrant served in accordance with Section 5.251, Business Organizations Code, may be extended to a date that is not later than the 30th day after the date the warrant is served. The judge may indicate in a warrant

that the deadline for compliance is earlier than the 15th business day after the date the warrant is served if the officer makes a showing and the judge finds that failure to comply with the warrant by the earlier deadline would cause serious jeopardy to an investigation, cause undue delay of a trial, or create a risk of:

(1) danger to the life or physical safety of any person;

(2) flight from prosecution;

(3) the tampering with or destruction of evidence; or

(4) intimidation of potential witnesses.

(j) The provider of an electronic communications service or a provider of a remote computing service responding to a warrant issued under this section shall verify the authenticity of the customer data, contents of communications, and other information produced in compliance with the warrant by including with the information an affidavit that is given by a person who is a custodian of the information or a person otherwise qualified to attest to its authenticity and that

states that the information was stored in the course of regularly conducted business of the provider and specifies whether it is the regular practice of the provider to store that information.

(k) On a service provider's compliance with a warrant under this section, an authorized peace officer shall file a return of the warrant and a copy of the inventory of the seized property as required under Article 18.10.

(l) The district judge shall hear and decide any motion to quash the warrant not later than the fifth business day after the date the service provider files the motion. The judge may allow the service provider to appear at the hearing by teleconference.

that the deadline for compliance is earlier than the 15th business day after the date the warrant is served if the officer makes a showing and the judge finds that failure to comply with the warrant by the earlier deadline would cause serious jeopardy to an investigation, cause undue delay of a trial, or create a material risk of:

(1) danger to the life or physical safety of any person;

(2) flight from prosecution;

(3) the tampering with or destruction of evidence; or

(4) intimidation of potential witnesses.

(k) If the authorized peace officer serving the warrant under this section also delivers an affidavit form to the provider of an electronic communications service or the provider of a remote computing service responding to the warrant, and the peace officer also notifies the provider in writing that an executed affidavit is required, then the provider shall verify the authenticity of the customer data, contents of communications, and other information produced in compliance with the warrant by including with the information the affidavit form that:

(1) is completed and sworn to by a person who is a custodian of the information or a person otherwise qualified to attest to its authenticity; and

(2) states that the information was stored in the course of regularly conducted business of the provider and specifies whether it is the regular practice of the provider to store that information.

(l) On a service provider's compliance with a warrant under this section, an authorized peace officer shall file a return of the warrant and a copy of the inventory of the seized property as required under Article 18.10.

(m) The district judge shall hear and decide any motion to quash the warrant not later than the fifth business day after the date the service provider files the motion. The judge may allow the service provider to appear at the hearing by teleconference.

(n) A provider of an electronic communications service or a provider of a remote computing service responding to a warrant issued under this section may request an extension of the period for compliance with the warrant if extenuating

| | |
|---|---|
| | circumstances exist to justify the extension. The district judge shall grant a request for an extension based on those circumstances if:<br>(1) the authorized peace officer who applied for the warrant or another appropriate authorized peace officer agrees to the extension; or<br>(2) the district judge finds that the need for the extension outweighs the likelihood that the extension will cause an adverse circumstance described by Subsection (j). |
| Sec. 5B. WARRANT ISSUED IN ANOTHER STATE FOR STORED CUSTOMER DATA OR COMMUNICATIONS. Any domestic entity that provides electronic communications services or remote computing services to the public shall comply with a warrant issued in another state and seeking information described by Section 5A(b), if the warrant is served on the entity in a manner equivalent to the service of process requirements provided in Section 5A(g). | Sec. 5B. WARRANT ISSUED IN ANOTHER STATE FOR STORED CUSTOMER DATA OR COMMUNICATIONS. Any domestic entity that provides electronic communications services or remote computing services to the public shall comply with a warrant issued in another state and seeking information described by Section 5A(b), if the warrant is served on the entity in a manner equivalent to the service of process requirements provided in Section 5A(h). |
| SECTION 8. This Act takes effect immediately if it receives a vote of two-thirds of all the members elected to each house, as provided by Section 39, Article III, Texas Constitution. If this Act does not receive the vote necessary for immediate effect, this Act takes effect September 1, 2013. | SECTION 8. Same as engrossed version. |