BILL ANALYSIS

Senate Research Center
83R28777 GCB-D

C.S.H.B. 2268
By: Frullo et al. (Carona)
Criminal Justice
5/15/2013
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Internet communications companies often hold information and data vital to prosecute an offense under state law, particularly relating to internet crimes. Although the certain electronic communications may take place within a state, law enforcement officers must apply for a local search warrant in an internet company's jurisdiction, often found out of state. This limitation hampers law enforcement's 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 other states including Florida, California, and Minnesota have enacted computer data warrant statutes that take advantage of "long-arm," or out-of-state, jurisdiction when dealing with internet data.

There are limited purposes for which traditional search warrants may be obtained, and C.S.H.B. 2268 adds customer data, transactional data, and content of communications related to electronic or wire communication providers to the list of grounds for issuance of a search warrant found in Article 18 of the Code of Criminal Procedure. The bill also creates a data search warrant which operates differently from a traditional search warrant in three ways. First, a data search warrant allows employees of the electronic communication company that is subject of the warrant to perform the search rather than a peace officer. Second, the data search warrant extends the time allowed to serve the warrant on the company's representative. The bill also provides a timeline for return of the data sought. In addition, C.S.H.B. 2268 extends the jurisdiction of district judges by granting them privileges to issue data search warrants beyond the physical boundaries of the state for computer data searches only.

The bill also reciprocates the electronic data search warrant process with other states already implementing similar statutes, which would allow Texas to serve data search warrants directly to out of state companies as well.

C.S.H.B. 2268 amends current law relating to search warrants issued in this state and other states for certain customer data, communications, and other related information held in electronic storage in this state and other states by providers of electronic communications services and remote computing services.

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) Creates this subsection from existing text. Authorizes a search warrant to be issued to search for and seize:
>
> (1)-(10) Makes no change to these subdivisions;
>
> (11)-(12) Makes nonsubstantive changes; or

(13) 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.

(b) Defines "electronic communication," "electronic storage," and "wire communication" for purposes of Subsection (a)(13).

SECTION 2. Amends Article 18.06(a), Code of Criminal Procedure, as follows:

(a) Requires a peace officer to whom a search warrant is delivered to execute the warrant without delay and forthwith return the warrant to the proper magistrate. Requires that a search warrant issued under Section 5A (relating to requiring a court to issue an order authorizing disclosure of certain information of a wire or electronic communication held in electronic storage), Article 18.21, be executed in the manner provided by that section not later than the 11th day after the date of issuance. Requires that a search warrant be executed within three days from the time of its issuance in all other cases. Requires that warrant issued under this chapter be executed within a shorter period if so directed in the warrant by the magistrate. Makes nonsubstantive changes.

SECTION 3. Amends Article 18.07(a), Code of Criminal Procedure, as follows:

(a) Provides that the period allowed for the execution of a search warrant, exclusive of the day of its issuance and of the day of its execution, is:

(1) Makes no change to this subdivision;

(2) 10 whole days if the warrant is issued under Section 5A, Article 18.21; or

(3) three whole days if the warrant is issued for a purpose other than that described by Subdivision (1) or (2).

Makes nonsubstantive changes.

SECTION 4. Amends Section 1(20), Article 18.02, Code of Criminal Procedure, to redefine "electronic storage."

SECTION 5. Amends Section 1, Article 18.21, Code of Criminal Procedure, by adding Subdivisions (3-b) and (3-c), to define "domestic entity" and "electronic customer data."

SECTION 6. Amends Sections 4(a), (b), (c), and (d), Article 18.21, Code of Criminal Procedure, as follows:

(a) Authorizes an authorized peace officer to require a provider of an electronic communications service to disclose the contents of a wire communication or electronic communication that has been in electronic storage for not longer than 180 days by obtaining a warrant under Section 5A.

(b) Authorizes an authorized peace officer to require a provider of an electronic communications service to disclose the contents of a wire communication or an electronic communication that has been in electronic storage for longer than 180 days if notice is not being given to the subscriber or customer, by obtaining a warrant under Section 5A; if notice is being given to the subscriber or customer, by obtaining an administrative subpoena authorized by statute, a grand jury subpoena, or a court order issued under Section 5 (Court Order to Obtain Access to Stored Communications); or as otherwise permitted by applicable federal law. Makes a nonsubstantive change.

(c) (1) Authorizes an authorized peace officer to require a provider of a remote computing service to disclose the contents of a wire communication or an electronic communication as described in Subdivision (2) (providing that

Subdivision (1) of this subsection applies only to a wire communication or an electronic communication that is in electronic storage) of this subsection:

(A) if notice is not being given to the subscriber or customer, by obtaining a warrant under Section 5A;

(B) Makes a nonsubstantive change; or

(C) Makes no change to this paragrph.

(2) Makes no change to this subdivision.

Makes nonsubstantive changes.

(d) 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 not otherwise described by this section without giving the applicable subscriber or customer notice:

(1)-(2) Makes no change to these subdivisions;

(3) by obtaining a warrant under Section 5A;

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

(5) Makes a nonsubstantive change; or

(6) Makes no change to this subdivision.

Deletes existing text authorizing an authorized peace officer to require a provider of remote computing service to disclose records or other information pertaining to a subscriber or customer of the service, other than communications described in Subsection (c) of this section, without giving the subscriber or customer notice by obtaining the consent of the subscriber or customer to the disclosure of the records or information.

Makes nonsubstantive changes.

SECTION 7. Amends Article 18.21, Code of Criminal Procedure, by adding Sections 5A and 5B, as follows:

Sec. 5A. WARRANT ISSUED IN THIS STATE FOR STORED CUSTOMER DATA OR COMMUNICATIONS. (a) Provides that 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) Authorizes a district judge, on the filing of an application by an authorized peace officer, to 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 a 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. Requires that an application made under this subsection demonstrate probable cause for the issuance of the warrant and must be supported by the oath or affirmation of the authorized peace officer.

(c) Prohibits a search warrant from being issued under this section unless the sworn affidavit required by Article 18.01(b) (relating to prohibiting the issuing of

a search warrant unless sufficient facts are first presented to satisfy the issuing magistrate that probable cause does in fact exist for its issuance and requiring that a sworn affidavit setting forth substantial facts establishing probable cause be filed in every instance in which a search warrant is requested) 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) Authorizes the electronic customer data described in the sworn affidavit required by Article 18.01(b) to be seized under the warrant.

(e) Requires that a warrant issued under this section run in the name of "The State of Texas."

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

(g) Requires the peace officer to 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. Provides that, for purposes of this subsection, a warrant is executed when the warrant is served in the manner described by Subsection (i).

(h) Authorizes a warrant under this section to 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. 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, as provided by Subsection (j). 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. Provides 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.

(i) Provides that 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 (Agent for Service of Process, Notice, or Demand as Matter of Law), Business Organizations Code;

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

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

(j) Requires the 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 this state, except that the deadline for compliance with a warrant served in accordance with Section 5.251, Business Organizations Code, is authorized to be extended to a date that is not later than the 30th day after the date the warrant is served. 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, 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) Requires the provider 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 completed and sworn to by a person who is a custodian of the information or a person otherwise qualified to attest to its authenticity 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 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.

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

(m) 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. Authorizes the judge to allow the service provider to appear at the hearing by teleconference.

(n) Authorizes a provider of an electronic communications service or a provider of a remote computing service responding to a warrant issued under this section to request an extension of the period for compliance with the warrant if extenuating circumstances exist to justify the extension. 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 Subsection (j).

Sec. 5B. WARRANT ISSUED IN ANOTHER STATE FOR STORED CUSTOMER DATA OR COMMUNICATIONS. 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 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. Amends Sections 6(a), (b), (d), (e), (f), and (g), Article 18.21, Code of Criminal Procedure, as follows:

(a) Authorizes a subpoena or court order for disclosure of the contents of electronic communication held in electronic storage by a provider of an electronic communications service under Section 4(b) or a provider of a remote computing service under Section 4(c) to require that provider, rather than that service provider, to create a copy of the contents of the electronic communications sought by the subpoena or court order for the purpose of preserving those contents. Makes nonsubstantive and conforming changes.

(b) Requires the provider of an electronic communications service or the provider of remote computing service to immediately notify the authorized peace officer who presented the subpoena or court order requesting the copy when the copy has been created.

(d) Requires the provider of an electronic communications service or the provider of a remote computing service to release the copy to the requesting authorized peace officer not earlier than the 14th day after the date the peace officer's notice to the subscriber or customer if the provider has not initiated proceedings to challenge the request of the peace officer for the copy, or received notice from the subscriber or customer that the subscriber or customer has initiated proceedings to challenge the request. Makes a conforming change.

(e) Prohibits the provider of an electronic communications service or the provider of a remote computing service from destroying or permitting the destruction of the copy until the information has been delivered to the applicable law enforcement agency, rather than to the designated law enforcement office or agency, or until the resolution of any court proceedings, including appeals of any proceedings, relating to the subpoena or court order requesting the creation of the copy, whichever occurs last.

(f) Authorizes an authorized peace officer who reasonably believes that notification to the subscriber or customer of the subpoena or court order would result in the destruction of or tampering with information sought to request the creation of a copy of the information. Provides that the peace officer's belief is not subject to challenge by the subscriber or customer or the provider of an electronic communications service or the provider of a remote computing service.

(g)(1) Requires that a motion to quash the subpoena or vacate the court order contain an affidavit or a sworn statement stating:

(A) 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 contents of electronic communications stored for the subscriber or customer have been sought; and

(B) Makes no change to this paragraph.

(2) Requires the subscriber or customer to give written notice to the provider of an electronic communications service or the provider of a remote computing service of the challenge to the subpoena or court order. Requires the authorized peace officer, rather than the authorized peace officer or the designated law enforcement office or agency, requesting the subpoena or court order to be served a copy of the papers filed by personal delivery or by registered or certified mail.

Makes nonsubstantive changes.

SECTION 9. Effective date: upon passage or September 1, 2013.