BILL ANALYSIS

Senate Research Center
83R2938 GCB-F

S.B. 1052
By: Carona
Criminal Justice
4/5/2013
As Filed

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 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 California, Florida, 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 S.B. 1052 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 and provides a timeline for return of the data sought. In addition, S.B. 1052 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.

As proposed, S.B. 1052 amends current law relating to search warrants issued in this state and other states for certain customer data, communications, and other 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 Section 18.02, Code of Criminal Procedure, as follows:

> Sec. 18.02. GROUNDS FOR ISSUANCE. (a) Creates this subsection from existing text. Authorizes a search warrant to be issued to search for and seize electronic customer data held in electronic storage or the contents of and records and other information related to a wire communication or electronic communication held in electronic storage, in addition to certain other items and individuals.

(b) Defines "electronic communication," "electronic storage," "wire communication," and "electronic customer data."

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, Article 18.21, be executed in the manner provided by that section not later than the 10th day after the date of issuance. Requires that a search warrant, in all other cases, be executed within three days from the time of its issuance. Requires that a 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, rather than the time, allowed for the execution of a search warrant, exclusive of the day of its issuance and of the day of its execution, is:

(1) 15 whole days if the warrant is issued solely to search for and seize specimens from a specific person for DNA analysis and comparison, including blood and saliva samples;

(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).

SECTION 4. 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 5. Amends Sections 4(a), (b), (c), (d), and (e), Article 18.21, Code of Criminal Procedure, as follows:

(a) Authorizes an authorized peace officer to require a provider of electronic communications service to disclose the contents of a wire communication or an 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 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, in addition to certain other methods.

(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) of this subsection if notice is not being given to the subscriber or customer, by obtaining a warrant under Section 5A, in addition to certain other methods. Makes nonsubstantive changes.

(2) Makes no change to this subdivision.

(d) Authorizes 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 a warrant under Section 5A, in addition to certain other methods.

(e) Makes no change to this subsection.

SECTION 6. 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) Authorizes a district judge to issue, on the filing of an application by an authorized peace officer, a search warrant under this section for electronic customer data held in electronic storage or 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 (c), regardless of whether the customer data, contents of communications, or other information 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 be supported by the oath or affirmation of the authorized peace officer.

(b) Requires the peace officer to execute the warrant not later than the 10th 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 (d).

(c) 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 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 (e). 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.

(d) 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; or

(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.

(e) Requires the district judge to indicate in the warrant the deadline for compliance by the provider of an electronic communications service or the provider of a remote computing service, which is prohibited from being later than the 10th 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 period allowed for compliance is four business days or less after the date the warrant is served if the officer makes a showing and the judge finds that failure to comply with the

warrant in four business days or less 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.

(f) Requires the provider of an electronic communications service or a provider of a remote computing service responding to a warrant issued under this section 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 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.

(g) Requires an authorized peace officer 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), on a service provider's compliance with a warrant under this section.

(h) 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.

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(a), if the warrant is served on the entity in a manner equivalent to the service of process requirements provided in Section 5A(c).

SECTION 7. Effective date: upon passage or September 1, 2013.