SUBJECT: Search warrants issued in Texas and other states for certain electronic data

COMMITTEE: Criminal Jurisprudence — committee substitute recommended

VOTE: 6 ayes — Herrero, Carter, Burnam, Hughes, Schaefer, Toth

0 nays

2 absent — Leach, Moody

1 present, not voting — Canales

WITNESSES: For — Lori Burks, Tarrant County District Attorney's Office; Anne Olson, Texas Baptist Christian Life Commission; (*Registered, but did not testify:* Jessica Anderson, Houston Police Department; David Boatright, National Center for Missing and Exploited Children; Lon Craft, Texas Municipal Police Association; Robert Flores, Texas Association of Mexican-American Chambers of Commerce; Clifford Herberg, Bexar County Criminal District Attorney's Office; Jason Sabo, Children at Risk; Ballard C. Shapleigh, District Attorney 34th Judicial District; Gary Tittle, Dallas Police Department; Ana Yanez Correa, Texas Criminal Justice Coalition)

Against — Chris Howe

On — Scott McCollough, Data Foundry; (*Registered, but did not testify:* Andy MacFarlane, Data Foundry)

BACKGROUND: Code of Criminal Procedure, ch. 18 governs search warrants. Art. 18.02 enumerates property, information, and other items for which a search warrant may be issued.

Art. 18.06 and art. 18.07 govern the time within which a warrant must be executed. Unless a warrant is issued solely for specimens for DNA analysis, it must be executed within three days.

Art. 18.20 governs detection, interception, and use of wire, oral, or electronic communications. It defines "electronic storage" as:

- 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.

Art. 18.21, sec. 4, governs the procedures for a peace officer to require disclosure of a stored wire communication or electronic communication, including circumstances in which a warrant is required. Art. 18.21, sec. 4(d) governs requirements for a peace officer to require disclosure of records or other information pertaining to a subscriber or customer of a remote computing service.

DIGEST:

CSHB 2268 would allow search warrants for certain electronic data to be issued in Texas and executed in other states. It would define terms, provide procedures and standards for these search warrants, and allow for state reciprocity of similar warrants issued in other states.

Definitions. The bill would define terms relating to electronic communication and customer data.

The current definition of "electronic storage" would be replaced with a new definition. Under the bill, "electronic storage" would mean any storage of electronic customer data in a computer, computer network, or computer system, regardless of whether the data was subject to recall, further manipulation, deletion, or transmission and would include any storage of a wire or electronic communication by an electronic communications service or a remote computing service.

"Electronic customer data" would mean data or records that were acquired by or stored with the provider of an electronic communications service or a remote computing service and contained:

- information revealing the identity of customers of the applicable service;
- information about a customer's use of the applicable service;
- information that identified 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.

Search warrants for stored customer data or communications. CSHB 2268 would amend the list of items for which a search warrant could be issued under Code of Criminal Procedure, art. 18.21 to add electronic customer data held in electronic storage, including the contents of records and other information related to a wire communication or electronic communication held in electronic storage.

The bill would add Code of Criminal Procedure, art. 18.21, sec. 5A and sec. 5B to govern the issuance of warrants for stored customer data or communications.

Warrants issued in Texas. Sec. 5A would govern warrants for stored customer data or communications issued in Texas.

Under sec. 5A a district judge would be able to issue a search warrant for electronic customer data held in electronic storage. The warrant could be issued regardless of whether the customer data was held at a location in Texas or in another state. The warrant could only be served on an electronic communications provider or a remote computing service provider that was a domestic entity or was doing business in this state under a contract or a terms-of-service agreement with a resident of Texas if any part of that contract or agreement were performed in Texas.

A warrant under sec. 5A would be served when the authorized peace officer delivered the warrant by hand, by fax, or, in a manner allowing proof of delivery by U.S. mail or private delivery service. The warrant would need to be served on a person designated or allowed by law to receive process for the entity.

A warrant under sec. 5A would need to be executed not later than the 11th day after the date of issuance unless the judge issuing the warrant directed a shorter period within the warrant. A warrant under sec. 5A would be considered executed when proper service was completed. The bill would amend arts. 18.06 and 18.07 to reflect the 11-day time limit for a warrant issued under sec. 5A.

The service provider receiving the warrant would be required to produce

all electronic customer data, contents of communications, and other information sought, regardless of where the information was held. Any officer, director, or owner of an entity who was responsible for the failure of the entity to comply with the warrant could be held in contempt of court. Failure of an entity to timely deliver the information sought would not affect the admissibility of that evidence in a criminal proceeding.

An entity upon which a warrant under 5A was served would have until the 15th business day after the date the warrant was served to comply, with certain exceptions:

- the deadline for a warrant served on the secretary of state as the agent of the entity would be the 30th day after the date the warrant was served; and
- the judge issuing the warrant could indicate an earlier compliance date in certain circumstances where failure to comply by the earlier deadline would cause serious jeopardy to an investigation or create certain risks.

The service provider would be required to verify the authenticity of the information produced by including an affidavit given by a person qualified to attest to its authenticity. The affidavit would have to state that the information was stored in the course of regularly conducted business of the provider and specify whether it was the regular practice of the provider to store that information.

A motion to quash filed by a service provider would need to be heard and decided by the judge issuing the warrant not later than the fifth business day after the date the motion was filed. This hearing could be conducted by teleconference.

Uniformity within ch. 18. The bill would ensure that references to warrants affected by this bill were updated and that sec. 5A mirrored several of the major provisions for search warrants throughout Code of Criminal Procedure, ch. 18.

The sworn affidavit required under art. 18.01(b) would be required for a warrant issued under sec. 5A and would need to establish probable cause that a specific offense had been committed and that the electronic customer data sought:

- constituted evidence of that offense or evidence that a particular person committed that offense; and
- was held in electronic storage by the service provider on which the warrant was served.

Other provisions similar to those elsewhere in ch. 18 would include:

- that an application for a warrant made under sec. 5A would need to demonstrate probable cause;
- that only the electronic customer data described in the sworn affidavit could be seized under the warrant;
- that the sworn affidavit could be sealed pursuant to art. 18.011;
- that a peace officer would need to file a return of the warrant and a copy of the inventory pursuant to art. 18.10; and
- that the warrant would run in the name of "The State of Texas"

The bill would specify that warrants required under Art. 18.21, sec. 4, would be warrants under sec. 5A. It would amend Art. 18.21, sec. 4(d) to apply to a provider of an electronic communications service or a remote computing service and only to disclosure of electronic customer data and not information pertaining to a subscriber.

Reciprocity. Under sec. 5B, a domestic entity that provided electronic communications services or remote computing services would be required to comply with a warrant issued in another state in a manner equivalent to the requirements under sec. 5A.

This bill would take immediate effect if finally passed by a two-thirds record vote of the membership of each house. Otherwise, it would take effect September 1, 2013.

SUPPORTERS SAY:

CSHB 2268 would simplify a needlessly complex process and keep Texas law enforcement in charge of Texas prosecutions. Currently, if an officer needs a search warrant for electronic data from a California company for someone in Texas, the officer has to create an affidavit and submit it to a California peace officer. The California peace officer must then create another affidavit and submit it to a California judge who will have discretion over whether to issue a search warrant. If the warrant is issued, California law enforcement must execute the warrant, collect the requested information, and then return it to Texas law enforcement. This process

could be simplified by allowing Texas judges and law enforcement to issue and execute warrants for certain electronic information held in other states. The entities upon which these warrants are commonly served have processes in place to streamline compliance and production of evidence. CSHB 2268 would expedite the investigation of Texas crimes and give Texas prosecutors the tools they need to successfully and timely prosecute these crimes, while alleviating the burden on courts in other states, and simplifying the process for the entities receiving these warrants.

The bill would allow Texas law enforcement to successfully investigate and prosecute criminals who engage in heinous crimes such as human trafficking and child sex exploitation. The Internet is the primary venue for traffickers to buy and sell women and children in the United States. The bulk of criminal activity and evidence in these crimes take place online, and the evidence may be held on a server or by a company housed in another state. It is often difficult in these cases to gather sufficient evidence because of the complex search warrant procedures, and some cases have to go forward without corroborating evidence because the evidence cannot be obtained in a timely manner. The bill would streamline these search warrants, allowing the state to be more successful in investigating and punishing trafficking crimes.

The bill would allow reciprocity only to the extent necessary for the bill to be effective. In order for Texas judges and law enforcement to use the tools provided by this bill, it would be necessary to grant the same ability to judges and law enforcement in other states who encounter the same problem. The reciprocity in the bill would be narrowly granted to apply only to warrants equivalent to those defined under the bill.

OPPONENTS SAY:

CSHB 2268 would allow judges who should have no jurisdiction in Texas to exercise judicial power within the state. The bill would allow for state reciprocity of warrants, meaning that Texas entities would be required to comply with warrants issued in another state. The judges whose warrants would be honored under this bill were not elected by Texans and should not have jurisdiction to issue warrants and enforce compliance within the state.