SENATE BILL 1501

By Green

AN ACT to amend Tennessee Code Annotated, Title 40, Chapter 6, Part 1, relative to obtaining certain information by use of a search warrant.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. Tennessee Code Annotated, Section 40-6-102, is amended by adding the following language as a new subdivision (4) and by renumbering the existing subdivision (4) accordingly:

(4)

(A) Where the property is 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) For purposes of this subdivision, the definitions used in part 3 of this chapter shall be used for the definitions in this subdivision (4).

SECTION 2. Tennessee Code Annotated, Section 40-6-107, is amended by adding the following language as a new subsection (b) and by redesignating the existing subsection (b) accordingly:

(b) A search warrant issued pursuant to § 40-6-109, shall be executed and returned in the manner provided in that section, not later than the eleventh day after the date of issuance. In all other cases, a search warrant shall be executed and returned as provided in subsection (a).

SECTION 3. Tennessee Code Annotated, Title 40, Chapter 6, Part 1, is amended by adding the following new sections:

40-6-109.

(a) This section applies to a warrant required under § 40-6-102(4) and by Rule 41 of the Tennessee Rules of Criminal Procedure 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 law enforcement officer, a magistrate 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 a provider of a remote computing service described in 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 law enforcement officer.

(c) A search warrant may not be issued under this section unless the sworn affidavit required by § 40-6-103 and Rule 41 of the Tennessee Rules of Criminal Procedure 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 § 40-6-103 and Rule 41 of the Tennessee Rules of Criminal Procedure may be seized under the warrant.

(e) A warrant issued under this section shall run in the name of “The State of Tennessee.”

(f) Rule 41 of the Tennessee Rules of Criminal Procedure and this part apply to an affidavit presented under Rule 41 or this part for the issuance of a warrant under this section, and the affidavit may be sealed in the manner provided by law or rule.

(g) The law enforcement officer shall execute the warrant not later than the eleventh day after the date of issuance, except that the officer shall execute the warrant within a shorter period of time if so directed in the warrant by the magistrate. For purposes of this subsection, a warrant is executed when the warrant is served in the manner described by subsection (i)

(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 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 designated officer, designated director, or designated 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 the person designated by Rule 4 of the Tennessee Rules of Civil Procedure to receive process.

(j) The magistrate 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 fifteenth 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 may be extended to a date that is not later than the thirtieth day after the date the warrant is served in the discretion of the magistrate. The magistrate may indicate in a warrant that the deadline for compliance is earlier than the fifteenth business day after the date the warrant is served if the officer makes a showing and the magistrate 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 law enforcement 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 law enforcement 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 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.

(l) On a service provider's compliance with a warrant under this section, an authorized law enforcement officer shall file a return of the warrant and a copy of the inventory of the seized property as required under this part and Rule 41 of the Rules of Criminal Procedure.

(m) The judge with criminal jurisdiction where the warrant was issued shall hear and decide any motion to invalidate 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 judge with criminal jurisdiction where the warrant was issued shall grant a request for an extension based on those circumstances if:

(1) The authorized law enforcement officer who applied for the warrant or another appropriate authorized officer agrees to the extension; or

(2) The judge finds that the need for the extension outweighs the likelihood that the extension will cause an adverse circumstance described by subsection (j).

40-6-110.

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 § 40-6-109, if the warrant is served on the entity in a manner equivalent to the service of process requirements provided in § 40-6-109.

40-6-111.

(a) A warrant for disclosure of certain electronic customer data held in electronic storage by a provider of an electronic communications service or a provider of a remote computing service under § 40-6-109 may require the provider to create a copy of the customer data sought by the warrant for the purpose of preserving that data. The provider may not inform the subscriber or customer whose data is being sought that the warrant has been issued. The provider shall create the copy within a reasonable time as determined by the magistrate issuing the warrant.

(b) The provider of an electronic communications service or the provider of a remote computing service shall immediately notify the authorized law enforcement officer who presented the warrant requesting the copy when the copy has been created.

(c) The authorized law enforcement officer shall notify the subscriber or customer whose electronic customer data is the subject of the warrant of the creation of the copy not later than three (3) days after the date of the receipt of the notification from the applicable provider that the copy was created.

(d) The provider of an electronic communications service or the provider of a remote computing service shall release the copy to the requesting authorized law enforcement officer not earlier than the fourteenth day after the date of the officer's notice to the subscriber or customer if the provider has not:

(1) Initiated proceedings to challenge the request of the officer for the copy; or

(2) Received notice from the subscriber or customer that the subscriber or customer has initiated proceedings to challenge the request.

(e) The provider of an electronic communications service or the provider of a remote computing service may not destroy or permit the destruction of the copy until the

electronic customer data has been delivered to the applicable law enforcement agency or until the resolution of any court proceedings, including appeals of any proceedings, relating to the warrant requesting the creation of the copy, whichever occurs last.

(f) An authorized law enforcement officer, who reasonably believes that notification to the subscriber or customer of the warrant would result in the destruction of or tampering with electronic customer data sought, may request the creation of a copy of the data. The officer's belief is not subject to challenge by the subscriber or customer or by a provider of an electronic communications service or a provider of a remote computing service.

(g)

(1) A subscriber or customer who receives notification as described in subsection (c) may file a written motion to vacate the warrant in the court that with criminal jurisdiction in the district where the warrant was issued not later than the fourteenth day after the date of the receipt of the notice. The motion must contain an affidavit or 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 electronic customer data held in electronic storage for the subscriber or customer has been sought; and

(B) The applicant's reasons for believing that the customer data sought is not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this act in some other respect.

(2) The subscriber or customer shall give written notice to the provider of an electronic communications service or the provider of a remote computing

service of the challenge to the warrant. The authorized law enforcement officer requesting the warrant must be served a copy of the papers filed by personal delivery or by registered or certified mail.

(h)

(1) The court shall order the authorized law enforcement officer to file a sworn response to the motion filed by the subscriber or customer if the court determines that the subscriber or customer has complied with the requirements of subsection (g). On request of the law enforcement officer, the court may permit the response to be filed in camera. The court may conduct any additional proceedings the court considers appropriate if the court is unable to make a determination on the motion on the basis of the parties' initial allegations and response.

(2)

(A) The court shall rule on the motion as soon as practiced after the filing of the officer's response as practicable. The court shall deny the motion if the court finds that the applicant is not the subscriber or customer whose electronic customer data held in electronic storage is the subject of the warrant or that there is reason to believe that the law enforcement officer's inquiry is legitimate and that the customer data sought is relevant to that inquiry.

(B) The court shall invalidate the warrant 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 to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this act.

(3) A court order denying a motion or application under this section is not a final order and no interlocutory appeal may be taken from the denial.

40-6-112.

(a) An authorized law enforcement officer seeking electronic customer data under this act may apply to the court for an order commanding the service provider, to whom a warrant is directed, not to disclose to any person the existence of the warrant. The order is effective for the period the court considers appropriate. The court shall enter the order if the court determines that there is reason to believe that notification of the existence of the warrant will have an adverse result.

(b) As used in this section, an “adverse result” means:

(1) Endangering the life or physical safety of an individual;

(2) Flight from prosecution;

(3) Destruction of or tampering with evidence;

(4) Intimidation of a potential witness; or

(5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

40-6-113.

(a) An authorized law enforcement officer who obtains electronic customer data under this act or other information under this act shall reimburse the person assembling or providing the 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 data or information. These costs include 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 data may be held in electronic storage or in which the other information may be stored.

(b) The authorized law enforcement officer and the person providing the electronic customer data or other information may agree on the amount of reimbursement. If there is no agreement, the court before which the criminal prosecution relating to the data or information would be brought shall determine the amount.

40-6-114

A subscriber or customer of a provider of an electronic communications service or a provider of a remote computing service shall not have a cause of action against a provider or its officers, employees, or agents or against other specified persons for providing information, facilities, or assistance as required by warrant under this act.

40-6-115.

(a) Except as provided by § 40-6-114, a provider of an electronic communications service or a provider of a remote computing service, or a subscriber or customer of that provider, that is aggrieved by a violation of this act has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally and is entitled to:

(1) Injunctive relief;

(2) Reasonable attorneys' fees and other litigation costs reasonably incurred; and

(3) The sum of the actual damages suffered and any profits made by the violator as a result of the violation, or one thousand dollars ($1,000), whichever is more.

SECTION 4. This act shall take effect July 1, 2014, the public welfare requiring it, and shall apply to all law enforcement attempts to obtain electronic customer data occurring on or after such date.