14100125D

HOUSE BILL NO. 17

Offered January 8, 2014

Prefiled November 20, 2013

A BILL to amend and reenact §§ 18.2-152.17, 19.2-56.2, and 19.2-70.3 of the Code of Virginia, relating to warrant requirement for cellular telephone, etc., as tracking device and obtaining location data.

Patrons—Marshall, R.G., Carr, Cline and LaRock

Referred to Committee for Courts of Justice

Be it enacted by the General Assembly of Virginia:

1. That §§ 18.2-152.17, 19.2-56.2, and 19.2-70.3 of the Code of Virginia are amended and reenacted as follows:

§ 18.2-152.17. Fraudulent procurement, sale, or receipt of telephone records.

A. Whoever (i) knowingly procures, attempts to procure, solicits, or conspires with another to procure a telephone record by fraudulent means; (ii) knowingly sells, or attempts to sell, a telephone record without the authorization of the customer to whom the record pertains; or (iii) receives a telephone record knowing that such record has been obtained by fraudulent means is guilty of a Class 1 misdemeanor.

B. As used in this section:

"Procure" in regard to such a telephone record means to obtain by any means, whether electronically, in writing, or in oral form, with or without consideration.

"Telecommunications carrier" means any person that provides commercial telephone services to a customer, irrespective of the communications technology used to provide such service, including, but not limited to, traditional wireline or cable telephone service; cellular, broadband PCS, or other wireless telephone service; microwave, satellite, or other terrestrial telephone service; and voice over Internet telephone service.

"Telephone record" means information retained by a telecommunications carrier that relates to the telephone number dialed by the customer or the incoming number of a call directed to a customer, or other data related to such calls typically contained on a customer telephone bill such as the time the call started and ended, the duration of the call, the time of day the call was made, and any charges applied. For purposes of this section, any information collected and retained by customers utilizing Caller I.D., or other similar technology, does not constitute a telephone record.

C. Nothing in this section shall be construed to prevent any action by a law-enforcement agency, or any officer or employee of such agency, from obtaining telephone records in connection with the performance of the official duties of the agency *when such records are obtained pursuant to § 19.2-70.3*.

D. Nothing in this section shall be construed to prohibit a telecommunications carrier from obtaining, using, disclosing, or permitting access to any telephone record, either directly or indirectly through its agents (i) in compliance with a subpoena ~~or subpoena duces tecum or as otherwise~~ authorized by ~~law~~ *§ 19.2-70.3*; (ii) with the lawful consent of the customer or subscriber; (iii) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, subscription to, such services; (iv) to a governmental entity, if the telecommunications carrier reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or (v) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under the Victims of Child Abuse Act of 1990.

E. Venue for the trial of any person charged with an offense under this section may be in the locality in which:

1. Any act was performed in furtherance of any course of conduct in violation of this section;

2. The accused has his principal place of business in the Commonwealth;

3. Any accused had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, telephone record, or other material or objects that were used in furtherance of the violation;

4. From which, to which, or through which any access to a telecommunication carrier was made whether by wires, electromagnetic waves, microwaves, optics or any other means of communication; or

5. The accused resides, or resided at the time of the offense.

§ 19.2-56.2. Application for and issuance of search warrant for a tracking device; installation

and use.

A. As used in this section, unless the context requires a different meaning:

"Judicial officer" means a judge, magistrate, or other person authorized to issue criminal warrants.

"Law-enforcement officer" shall have the same meaning as in § 9.1-101.

"Tracking device" means an electronic or mechanical device that permits a person to remotely determine or track the position or movement of a person or object. "Tracking device" includes *(i)* devices that store geographic data for subsequent access or analysis ~~and~~, *(ii)* devices that allow for the real-time monitoring of movement, *and (iii) cellular telephones or other wireless telecommunications devices*.

"Use of a tracking device" includes the installation, maintenance, and monitoring of a tracking device but does not include the interception of wire, electronic, or oral communications or the capture, collection, monitoring, or viewing of images.

B. A law-enforcement officer may apply for a search warrant from a judicial officer to permit the use of a tracking device. Each application for a search warrant authorizing the use of a tracking device shall be made in writing, upon oath or affirmation, to a judicial officer for the circuit in which the tracking device is to be installed, or where there is probable cause to believe the offense for which the tracking device is sought has been committed, is being committed, or will be committed.

The law-enforcement officer shall submit an affidavit, which may be filed by electronically transmitted (i) facsimile process or (ii) electronic record as defined in § 59.1-480, and shall include:

1. The identity of the applicant and the identity of the law-enforcement agency conducting the investigation;

2. The identity of *(i) the person, when the tracking device used is a cellular telephone or other wireless telecommunications device, or (ii)* the vehicle, container, item, or object to which, in which, or on which the tracking device is to be attached, placed, or otherwise installed; the name of the owner or possessor of the vehicle, container, item, or object described, if known; and the jurisdictional area in which the *person,* vehicle, container, item, or object described is expected to be found, if known;

3. Material facts constituting the probable cause for the issuance of the search warrant and alleging substantially the offense in relation to which such tracking device is to be used and a showing that probable cause exists that the information likely to be obtained will be evidence of the commission of such offense; and

4. The name of the county or city where there is probable cause to believe the offense for which the tracking device is sought has been committed, is being committed, or will be committed.

C. 1. If the judicial officer finds, based on the affidavit submitted, that there is probable cause to believe that a crime has been committed, is being committed, or will be committed and that there is probable cause to believe the information likely to be obtained from the use of the tracking device will be evidence of the commission of such offense, the judicial officer shall issue a search warrant authorizing the use of the tracking device. The search warrant shall authorize the use of the tracking device from within the Commonwealth to track a person or property for a reasonable period of time, not to exceed 30 days from the issuance of the search warrant. The search warrant shall authorize the collection of the tracking data contained in or obtained from the tracking device but shall not authorize the interception of wire, electronic, or oral communications or the capture, collection, monitoring, or viewing of images.

2. The affidavit shall be certified by the judicial officer who issues the search warrant and shall be delivered to and preserved as a record by the clerk of the circuit court of the county or city where there is probable cause to believe the offense for which the tracking device has been sought has been committed, is being committed, or will be committed. The affidavit shall be delivered by the judicial officer in person; mailed by certified mail, return receipt requested; or delivered by electronically transmitted facsimile process or by use of filing and security procedures as defined in the Uniform Electronic Transactions Act (§ 59.1-479 et seq.) for transmitting signed documents.

3. By operation of law, the affidavit, search warrant, return, and any other related materials or pleadings shall be sealed. Upon motion of the Commonwealth or the owner or possessor of the vehicle, container, item, or object that was tracked, the circuit court may unseal such documents if it appears that the unsealing is consistent with the ends of justice or is necessary to reasonably inform such person of the nature of the evidence to be presented against him or to adequately prepare for his defense.

4. The circuit court may, for good cause shown, grant one or more extensions, not to exceed 30 days each.

D. 1. ~~The~~ *For tracking devices requiring installation, the* search warrant shall command the law-enforcement officer to complete the installation authorized by the search warrant within 15 days after issuance of the search warrant.

2. The law-enforcement officer executing the search warrant shall enter on it the exact date and time the device was installed and the period during which it was used *or, in the case of a cellular telephone or other wireless telecommunications device, the exact date and time the tracking was initiated and the*

period during which it was used.

3. Law-enforcement officers shall be permitted to monitor the tracking device during the period authorized in the search warrant, unless the period is extended as provided for in this section.

4. ~~Law-enforcement~~ *For tracking devices requiring installation, law-enforcement* officers shall remove the tracking device as soon as practical, but not later than 10 days after the use of the tracking device has ended. Upon request, and for good cause shown, the circuit court may grant one or more extensions for such removal for a period not to exceed 10 days each.

5. In the event that law-enforcement officers are unable to remove the tracking device as required by subdivision 4, the law-enforcement officers shall disable the device, if possible, and all use of the tracking device shall cease.

6. Within 10 days after the use of the tracking device has ended, the executed search warrant shall be returned to the circuit court of the county or city where there is probable cause to believe the offense for which the tracking device has been sought has been committed, is being committed, or will be committed, as designated in the search warrant, where it shall be preserved as a record by the clerk of the circuit court.

E. Within 10 days after the use of the tracking device has ended, a copy of the executed search warrant shall be served on the person who was tracked and the person whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked or by leaving a copy with any individual found at the person's usual place of abode who is a member of the person's family, other than a temporary sojourner or guest, and who is 16 years of age or older and by mailing a copy to the person's last known address. Upon request, and for good cause shown, the circuit court may grant one or more extensions for such service for a period not to exceed 30 days each. Good cause shall include, but not be limited to, a continuing criminal investigation, the potential for intimidation, the endangerment of an individual, or the preservation of evidence.

F. The disclosure or publication, without authorization of a circuit court, by a court officer, law-enforcement officer, or other person responsible for the administration of this section of the existence of a search warrant issued pursuant to this section, application for such search warrant, any affidavit filed in support of such warrant, or any return or data obtained as a result of such search warrant that is sealed by operation of law is punishable as a Class 1 misdemeanor.

§ 19.2-70.3. Obtaining records concerning electronic communication service or remote computing service.

A. A provider of electronic communication service or remote computing service, which, for purposes of subdivisions ~~A~~ 2 through ~~A~~ 4, includes a foreign corporation that provides such services, shall disclose a record or other information pertaining to a subscriber to or customer of such service, excluding the contents of electronic communications *and location data*, to an investigative or law-enforcement officer only pursuant to:

1. A subpoena issued by a grand jury of a court of ~~this~~ *the* Commonwealth;

2. A search warrant issued by a magistrate, general district court, or ~~a~~ circuit court;

3. A court order for such disclosure issued as provided in ~~this section~~ *subsection B*; or

4. ~~The consent of the subscriber or customer to such disclosure~~ *An administrative subpoena issued pursuant to § 19.2-10.2.*

However, a subscriber or customer may consent to disclosure of a record or other information pertaining to him, including the contents of electronic communications or location data, or both.

B. A court shall issue an order for disclosure under this section only if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant and material to an ongoing criminal investigation, or the investigation of any missing child as defined in § 52-32, missing senior adult as defined in § 52-34.4, or an incapacitated person as defined in § 64.2-2000 who meets the definition of a missing senior adult except for the age requirement. Upon issuance of an order for disclosure under this section, the order and any written application or statement of facts may be sealed by the court for 90 days for good cause shown upon application of the attorney for the Commonwealth in an ex parte proceeding. The order and any written application or statement of facts may be sealed for additional 90-day periods for good cause shown upon subsequent application of the attorney for the Commonwealth in an ex parte proceeding. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify the order, if the information or records requested are unusually voluminous in nature or compliance with such order would otherwise cause an undue burden on such provider.

C. A provider of electronic communication service or remote computing service, including a foreign corporation that provides such services, shall disclose the contents of electronic communications *or location data* to an investigative or law-enforcement officer only pursuant to a search warrant issued by a magistrate, a juvenile and domestic relations district court, a general district court, or a circuit court, based upon complaint on oath supported by an affidavit as required in § 19.2-54, or judicial officer or

court of any of the several states of the United States or its territories, or the District of Columbia when the warrant issued by such officer or such court complies with the provisions of subsection E. In the case of a search warrant directed to a foreign corporation the affidavit shall state that the complainant believes that the records requested are actually or constructively possessed by a foreign corporation that provides electronic communication service or remote computing service within the Commonwealth of Virginia. If satisfied that probable cause has been established for such belief and as required by Chapter 5 (§ 19.2-52 et seq.), the magistrate, the juvenile and domestic relations district court, the general district court, or the circuit court shall issue a warrant identifying those records to be searched for and commanding the person seeking such warrant to properly serve the warrant upon the foreign corporation.

D. In order to comply with the requirements of § 19.2-54, any search of the records of a foreign corporation shall be deemed to have been made in the same place wherein the search warrant was issued.

E. A Virginia corporation or other entity that provides electronic communication services or remote computing services to the general public, when properly served with a search warrant and affidavit in support of the warrant, issued by a judicial officer or court of any of the several states of the United States or its territories, or the District of Columbia with jurisdiction over the matter, to produce a record or other information pertaining to a subscriber to or customer of such service, *including location data,* or the contents of electronic communications, or both, shall produce the record or other information, *including location data,* or the contents of electronic communications as if that warrant had been issued by a Virginia court. The provisions of this subsection shall only apply to a record or other information, *including location data,* or contents of electronic communications relating to the commission of a criminal offense that is substantially similar to (i) a violent felony as defined in § 17.1-805, (ii) an act of violence as defined in § 19.2-297.1, (iii) any offense for which registration is required pursuant to § 9.1-902, (iv) computer fraud pursuant to § 18.2-152.3, or (v) identity theft pursuant to § 18.2-186.3. The search warrant shall be enforced and executed in the Commonwealth as if it were a search warrant described in subsection C.

F. The provider of electronic communication service or remote computing service may verify the authenticity of the written reports or records that it discloses pursuant to this section, excluding the contents of electronic communications, by providing an affidavit from the custodian of those written reports or records or from a person to whom said custodian reports certifying that they are true and complete and that they are prepared in the regular course of business. When so authenticated, the written reports and records are admissible in evidence as a business records exception to the hearsay rule.

G. No cause of action shall lie in any court against a provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant or subpoena under this section.

H. For the purposes of this section:

"Foreign corporation" means any corporation or other entity, whose primary place of business is located outside of the boundaries of the Commonwealth, that makes a contract or engages in a terms of service agreement with a resident of the Commonwealth to be performed in whole or in part by either party in the Commonwealth, or a corporation that has been issued a certificate of authority pursuant to § 13.1-759 to transact business in the Commonwealth. The making of the contract or terms of service agreement or the issuance of a certificate of authority shall be considered to be the agreement of the foreign corporation or entity that a search warrant or subpoena, which has been properly served on it, has the same legal force and effect as if served personally within the Commonwealth.

"Location data" means any data or information that tracks, either at a point in time or over a period of time, the location of a subscriber to or customer of a provider of electronic communication service or a remote computing service as determined by the location of an electronic device to which the subscriber or customer has legal title, claim, right, custody, or ultimate control.

"Properly served" means delivery of a search warrant or subpoena by hand, by United States mail, by commercial delivery service, by facsimile or by any other manner to any officer of a corporation or its general manager in the Commonwealth, to any natural person designated by it as agent for the service of process, or if such corporation has designated a corporate agent, to any person named in the latest annual report filed pursuant to § 13.1-775.