18107405D

SENATE BILL NO. 833

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the House Committee for Courts of Justice on February 23, 2018)

(Patron Prior to Substitute—Senator Carrico)

A BILL to amend and reenact §§ 19.2-70.2 and 19.2-70.3 of the Code of Virginia, relating to installation of a pen register or trap and trace device; emergency circumstances.

Be it enacted by the General Assembly of Virginia:

1. That §§ 19.2-70.2 and 19.2-70.3 of the Code of Virginia are amended and reenacted as follows:

§ 19.2-70.2. Application for and issuance of order for a pen register or trap and trace device; assistance in installation and use.

A. An investigative or law-enforcement officer may make application for an order or an extension of an order authorizing or approving the installation and use of a pen register or a trap and trace device, in writing under oath or equivalent affirmation, to a court of competent jurisdiction. The application shall include:

1. The identity of the officer making the application and the identity of the law-enforcement agency conducting the investigation; and

2. A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

The application may include a request that the order require information, facilities and technical assistance necessary to accomplish the installation be furnished.

B. An application for an ex parte order authorizing the installation and use of a pen register or trap and trace device may be filed in the jurisdiction where the ongoing criminal investigation is being conducted; where there is probable cause to believe that an offense was committed, is being committed, or will be committed; or where the person or persons who subscribe to the wire or electronic communication system live, work, or maintain an address or a post office box. For the purposes of an order entered pursuant to this section for the installation and use of a pen register or trap and trace device, such installation shall be deemed to occur in the jurisdiction where the order is entered, regardless of the physical location or the method by which the information is captured or routed to the law-enforcement officer that made the application. Upon application, the court shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device if the court finds that the investigative or law-enforcement officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

The order shall specify:

1. The identity, if known, of the person in whose name the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied is listed or to whom the line or other facility is leased;

2. The identity, if known, of the person who is the subject of the criminal investigation;

3. The attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and

4. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

C. Installation and use of a pen register or a trap and trace device shall be authorized for a period not to exceed 60 days. Extensions of the order may be granted, but only upon application made and order issued in accordance with this section. The period of an extension shall not exceed 60 days.

D. An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that:

1. The order and application be sealed until otherwise ordered by the court;

2. Information, facilities and technical assistance necessary to accomplish the installation be furnished if requested in the application; and

3. The person owning or leasing the line or other facility to which the pen register or trap and trace device is attached or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

E. Upon request of an investigative or a law-enforcement officer authorized by the court to install and use a pen register, a provider of wire or electronic communication service, a landlord, custodian or any other person so ordered by the court shall, as soon as practicable, furnish the officer with all information, facilities, and technical assistance necessary to accomplish the installation of the pen

register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place.

F. Upon request of an investigative or law-enforcement officer authorized by the court to receive the results of a trap and trace device under this section, a provider of wire or electronic communication service, a landlord, custodian or any other person so ordered by the court shall, as soon as practicable, install the device on the appropriate line and furnish the officer with all additional information, facilities and technical assistance, including installation and operation of the device, unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the investigative or law-enforcement officer designated by the court at reasonable intervals during regular business hours for the duration of the order. Where the law-enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained that will identify (i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network; (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and (iv) any information that has been collected by the device. To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device. The record maintained hereunder shall be provided ex parte and under seal of the court that entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order, including any extensions thereof.

G. A provider of a wire or electronic communication service, a landlord, custodian or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for reasonable and actual expenses incurred in providing such facilities and assistance. The expenses shall be paid out of the criminal fund.

H. *When disclosure of real-time location data is not prohibited by federal law, an investigative or law-enforcement officer may obtain a pen register or trap and trace device installation without a court order, in addition to any real-time location data obtained pursuant to subsection E of § 19.2-70.3, in the following circumstances:*

1. To respond to a user's call for emergency services;

2. With the informed, affirmative consent of the owner or user of the electronic device concerned if (i) the device is in his possession, (ii) the owner or user knows or believes that the device is in the possession of an employee or agent of the owner or user with the owner's or user's consent, or (iii) the owner or user knows or believes that the device has been taken by a third party without the consent of the owner or user;

3. With the informed, affirmative consent of the legal guardian or next of kin of the owner or user, if reasonably available, if the owner or user is reasonably believed to be deceased, is reported missing, or is unable to be contacted;

4. To locate a child who is reasonably believed to have been abducted or to be missing and endangered; or

5. If the investigative or law-enforcement officer reasonably believes that an emergency involving the immediate danger to a person requires the disclosure, without delay, of pen register and trap and trace data, or real-time location data pursuant to subsection E of § 19.2-70.3, concerning a specific person and that a court order cannot be obtained in time to prevent the identified danger.

No later than three business days after seeking the installation of a pen register or trap and trace device pursuant to this subsection, the investigative or law-enforcement officer seeking the installation shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency and the reasons why the installation of the pen register or trap and trace device was believed to be important in addressing the emergency.

I. 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 issued pursuant to this section. Good faith reliance on a court order, a legislative authorization or a statutory authorization is a complete defense against any civil or criminal action based upon a violation of this chapter.

§ 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 2, 3, and 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 real-time location data, to an investigative or law-enforcement officer only pursuant to:

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

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

3. A court order issued by a circuit court for such disclosure issued as provided in subsection B; or

4. The consent of the subscriber or customer to such disclosure.

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. Except as provided in subsection D or E, 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 real-time 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 G. 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. A search warrant for real-time location data shall be issued if the magistrate, the juvenile and domestic relations district court, the general district court, or the circuit court is satisfied that probable cause has been established that the real-time location data sought is relevant to a crime that is being committed or has been committed or that an arrest warrant exists for the person whose real-time location data is sought.

D. A provider of electronic communication service or remote computing service, including a foreign corporation that provides such services, shall disclose a record or other information pertaining to a subscriber to or customer of such service, including real-time location data but excluding the contents of electronic communications, to an investigative or law-enforcement officer pursuant to an administrative subpoena issued pursuant to § 19.2-10.2 concerning a violation of § 18.2-374.1 or 18.2-374.1:1, former § 18.2-374.1:2, or § 18.2-374.3 when the information sought is relevant and material to an ongoing criminal investigation.

E. When disclosure of real-time location data is not prohibited by federal law, an investigative or law-enforcement officer may obtain real-time location data without a warrant in the following circumstances:

1. To respond to the user's call for emergency services;

2. With the informed, affirmative consent of the owner or user of the electronic device concerned if (i) the device is in his possession; (ii) the owner or user knows or believes that the device is in the possession of an employee or agent of the owner or user with the owner's or user's consent; or (iii) the owner or user knows or believes that the device has been taken by a third party without the consent of the owner or user;

3. With the informed, affirmative consent of the legal guardian or next of kin of the owner or user, if reasonably available, if the owner or user is reasonably believed to be deceased, is reported missing, or is unable to be contacted; ~~or~~

4. *To locate a child who is reasonably believed to have been abducted or to be missing and endangered; or*

5. If the investigative or law-enforcement officer reasonably believes that an emergency involving the immediate danger to a person requires the disclosure, without delay, of real-time location data

concerning a specific person and that a warrant cannot be obtained in time to prevent the identified danger.

No later than three business days after seeking disclosure of real-time location data pursuant to this subsection, the investigative or law-enforcement officer seeking the information shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency and the facts as to why the person whose real-time location data was sought is believed to be important in addressing the emergency.

F. 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.

G. 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 real-time location data, or the contents of electronic communications, or both, shall produce the record or other information, including real-time 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 real-time 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.

H. 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 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 copies of reports or records and that they are prepared in the regular course of business. When so authenticated, no other evidence of authenticity shall be necessary. The written reports and records, excluding the contents of electronic communications, shall be considered business records for purposes of the business records exception to the hearsay rule.

I. No cause of action shall lie in any court against a provider of a wire or electronic communication service or remote computing service or such provider's officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, administrative subpoena, or subpoena under this section or the provisions of subsection E.

J. A search warrant or administrative subpoena for the disclosure of real-time location data pursuant to this section shall require the provider to provide ongoing disclosure of such data for a reasonable period of time, not to exceed 30 days. A court may, for good cause shown, grant one or more extensions, not to exceed 30 days each.

K. An investigative or law-enforcement officer shall not use any device to obtain electronic communications or collect real-time location data from an electronic device without first obtaining a search warrant authorizing the use of the device if, in order to obtain the contents of such electronic communications or such real-time location data from the provider of electronic communication service or remote computing service, such officer would be required to obtain a search warrant pursuant to this section. However, an investigative or law-enforcement officer may use such a device without first obtaining a search warrant under the circumstances set forth in subsection E. For purposes of subdivision E **4** 5, the investigative or law-enforcement officer using such a device shall be considered to be the possessor of the real-time location data.

L. Upon issuance of any subpoena, search warrant, or order for disclosure issued under this section, upon written certification by the attorney for the Commonwealth that there is a reason to believe that the victim is under the age of 18 and that notification or disclosure of the existence of the subpoena, search warrant, or order will endanger the life or physical safety of an individual, or lead to flight from prosecution, the destruction of or tampering with evidence, the intimidation of potential witnesses, or otherwise seriously jeopardize an investigation, the court may in an ex parte proceeding order a provider of electronic communication service or remote computing service not to disclose for a period of 90 days the existence of the subpoena, search warrant, or order and written application or statement of facts to another person, other than an attorney to obtain legal advice. The nondisclosure order may be renewed 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 for disclosure 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.

M. For the purposes of this section:

"Electronic device" means a device that enables access to, or use of, an electronic communication service, remote computing service, or location information service, including a global positioning service or other mapping, locational, or directional information service.

"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.

"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.

"Real-time location data" means any data or information concerning the current location of an electronic device that, in whole or in part, is generated, derived from, or obtained by the operation of the device.