

15102300D

SENATE BILL NO. 1189

Offered January 14, 2015

Prefiled January 13, 2015

A *BILL to amend and reenact § 19.2-70.3 of the Code of Virginia, relating to records concerning electronic communication service or remote computing service; authentication of contents of communications.*

Patron—Lewis

Referred to Committee on General Laws and Technology

Be it enacted by the General Assembly of Virginia:**1. That § 19.2-70.3 of the Code of Virginia is amended and reenacted as follows:****§ 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 through 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 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, 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.

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.

INTRODUCED

SB1189

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

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

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

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

71 4. If the investigative or law-enforcement officer reasonably believes that an emergency involving the
72 immediate danger to a person requires the disclosure, without delay, of real-time location data
73 concerning a specific person and that a warrant cannot be obtained in time to prevent the identified
74 danger, and the possessor of the real-time location data believes, in good faith, that an emergency
75 involving danger to a person requires disclosure without delay.

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

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

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

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

104 I. *For contents of communications obtained pursuant to this section, the provider of electronic*
105 *communication service or remote computing service may verify the authenticity of such records by*
106 *providing an affidavit from the custodian of the records or from a person to whom such custodian*
107 *reports certifying that they are accurate and complete and prepared in the regular course of business.*

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

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

116 L. For the purposes of this section:

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

120 "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.