

VIRGINIA ACTS OF ASSEMBLY — CHAPTER

An Act to amend and reenact § 19.2-70.3 of the Code of Virginia, relating to obtaining electronic communication service or remote computing service records.

[H 326]

Approved

**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 *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, 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

57 criminal investigation.

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

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

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

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

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

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

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

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

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

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

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

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

118 subdivision E 4, the investigative or law-enforcement officer using such a device shall be considered to  
119 be the possessor of the real-time location data.

120 L. *Upon issuance of any subpoena, search warrant, or order for disclosure issued under this section,*  
121 *upon written certification by the attorney for the Commonwealth that there is a reason to believe that*  
122 *the victim is under the age of 18 and that notification or disclosure of the existence of the subpoena,*  
123 *search warrant, or order will endanger the life or physical safety of an individual, or lead to flight from*  
124 *prosecution, the destruction of or tampering with evidence, the intimidation of potential witnesses, or*  
125 *otherwise seriously jeopardize an investigation, the court may in an ex parte proceeding order a*  
126 *provider of electronic communication service or remote computing service not to disclose for a period of*  
127 *90 days the existence of the subpoena, search warrant, or order and written application or statement of*  
128 *facts to another person, other than an attorney to obtain legal advice. The nondisclosure order may be*  
129 *renewed for additional 90-day periods for good cause shown upon subsequent application of the*  
130 *attorney for the Commonwealth in an ex parte proceeding. A court issuing an order for disclosure*  
131 *pursuant to this section, on a motion made promptly by the service provider, may quash or modify the*  
132 *order if the information or records requested are unusually voluminous in nature or compliance with*  
133 *such order would otherwise cause an undue burden on such provider.*

134 M. For the purposes of this section:

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

138 "Foreign corporation" means any corporation or other entity, whose primary place of business is  
139 located outside of the boundaries of the Commonwealth, that makes a contract or engages in a terms of  
140 service agreement with a resident of the Commonwealth to be performed in whole or in part by either  
141 party in the Commonwealth, or a corporation that has been issued a certificate of authority pursuant to  
142 § 13.1-759 to transact business in the Commonwealth. The making of the contract or terms of service  
143 agreement or the issuance of a certificate of authority shall be considered to be the agreement of the  
144 foreign corporation or entity that a search warrant or subpoena, which has been properly served on it,  
145 has the same legal force and effect as if served personally within the Commonwealth.

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

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