

18103489D

HOUSE BILL NO. 604

Offered January 10, 2018

Prefiled January 8, 2018

A BILL to amend and reenact §§ 19.2-10.2, 19.2-56, and 19.2-70.3 of the Code of Virginia, relating to warrant requirement for telecommunications records; location data.

 Patron—Carr

Referred to Committee for Courts of Justice

Be it enacted by the General Assembly of Virginia:

1. That §§ 19.2-10.2, 19.2-56, and 19.2-70.3 of the Code of Virginia are amended and reenacted as follows:

§ 19.2-10.2. Administrative subpoena issued for record from provider of electronic communication service or remote computing service.

A. A provider of electronic communication service or remote computing service that is transacting or has transacted any business in the Commonwealth 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* as required by § 19.2-70.3, to an attorney for the Commonwealth or the Attorney General pursuant to an administrative subpoena issued under this section.

1. In order to obtain such records or other information, the attorney for the Commonwealth or the Attorney General shall certify on the face of the subpoena that there is reason to believe that the records or other information being sought are relevant to a legitimate law-enforcement investigation concerning violations of §§ 18.2-47, 18.2-48, 18.2-49, 18.2-346, 18.2-347, 18.2-348, 18.2-349, 18.2-355, 18.2-356, 18.2-357, 18.2-374.1, and 18.2-374.1:1, former § 18.2-374.1:2, and § 18.2-374.3.

2. Upon written certification by the attorney for the Commonwealth or the Attorney General 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 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 subpoena shall include a provision ordering the service provider not to notify or disclose the existence of the subpoena to another person, other than an attorney to obtain legal advice, for a period of 30 days after the date on which the service provider responds to the subpoena.

3. On a motion made promptly by the electronic communication service or remote computing service provider, a court of competent jurisdiction may quash or modify the administrative subpoena if the records or other information requested are unusually voluminous in nature or if compliance with the subpoena would otherwise cause an undue burden on the service provider.

B. All records or other information received by an attorney for the Commonwealth or the Attorney General pursuant to an administrative subpoena issued under this section shall be used only for a reasonable length of time not to exceed 30 days and only for a legitimate law-enforcement purpose. Upon completion of the investigation, the records or other information held by the attorney for the Commonwealth or the Attorney General shall be destroyed if no prosecution is initiated. The existence of such a subpoena shall be disclosed upon motion of an accused.

C. No cause of action shall lie in any court against an electronic communication service or remote computing service provider, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of an administrative subpoena issued under this section.

D. Records or other information pertaining to a subscriber to or customer of such service means name, address, local and long distance telephone connection records, or records of session times and durations, length of service, including start date, and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service.

E. Nothing in this section shall require the disclosure of information in violation of any federal law.

§ 19.2-56. To whom search warrant directed; what it shall command; warrant to show date and time of issuance; copy of affidavit to be part of warrant and served therewith; warrants not executed within 15 days.

The judge, magistrate or other official authorized to issue criminal warrants, shall issue a search warrant if he finds from the facts or circumstances recited in the affidavit that there is probable cause for the issuance thereof.

INTRODUCED

HB604

59 Every search warrant shall be directed to (i) the sheriff, sergeant, or any policeman of the county,
60 city or town in which the place to be searched is located, (ii) any law-enforcement officer or agent
61 employed by the Commonwealth and vested with the powers of sheriffs and police, or (iii) jointly to
62 any such sheriff, sergeant, policeman or law-enforcement officer or agent and an agent, special agent or
63 officer of the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco and Firearms of the
64 United States Treasury, the United States Naval Criminal Investigative Service, the United States
65 Department of Homeland Security, any inspector, law-enforcement official or police personnel of the
66 United States Postal Service, or the Drug Enforcement Administration. The warrant shall (a) name the
67 affiant, (b) recite the offense or the identity of the person to be arrested for whom a warrant or process
68 for arrest has been issued in relation to which the search is to be made, (c) name or describe the place
69 to be searched, (d) describe the property or person to be searched for, and (e) recite that the magistrate
70 has found probable cause to believe that the property or person constitutes evidence of a crime
71 (identified in the warrant) or tends to show that a person (named or described therein) has committed or
72 is committing a crime or that the person to be arrested for whom a warrant or process for arrest has
73 been issued is located at the place to be searched.

74 The warrant shall command that the place be forthwith searched, either in day or night, and that the
75 objects or persons described in the warrant, if found there, be seized. An inventory shall be produced
76 before a court having jurisdiction of the offense or over the person to be arrested for whom a warrant or
77 process for arrest has been issued in relation to which the warrant was issued as provided in § 19.2-57.

78 Any such warrant as provided in this section shall be executed by the policeman or other
79 law-enforcement officer or agent into whose hands it shall come or be delivered. If the warrant is
80 directed jointly to a sheriff, sergeant, policeman or law-enforcement officer or agent of the
81 Commonwealth and a federal agent or officer as otherwise provided in this section, the warrant may be
82 executed jointly or by the policeman, law-enforcement officer or agent into whose hands it is delivered.
83 No other person may be permitted to be present during or participate in the execution of a warrant to
84 search a place except (1) the owners and occupants of the place to be searched when permitted to be
85 present by the officer in charge of the conduct of the search and (2) persons designated by the officer in
86 charge of the conduct of the search to assist or provide expertise in the conduct of the search.

87 Any search warrant for records or other information pertaining to a subscriber to, or customer of, an
88 electronic communication service or remote computing service, whether a domestic corporation or
89 foreign corporation, that is transacting or has transacted any business in the Commonwealth, to be
90 executed upon such service provider may be executed within or without the Commonwealth by hand,
91 United States mail, commercial delivery service, facsimile, or other electronic means upon the service
92 provider. Notwithstanding the provisions of § 19.2-57, the officer executing a warrant pursuant to this
93 paragraph shall endorse the date of execution thereon and shall file the warrant, with the inventory
94 attached (or a notation that no property was seized) and the accompanying affidavit, unless such
95 affidavit was made by voice or videotape recording, within three days after the materials ordered to be
96 produced are received by the officer from the service provider. The return shall be made in the circuit
97 court clerk's office for the jurisdiction wherein the warrant was issued. Saturdays, Sundays, or any
98 federal or state legal holiday shall not be used in computing the three-day filing period.

99 Electronic communication service or remote computing service providers, whether a foreign or
100 domestic corporation, shall also provide the contents of electronic communications *and location data*
101 pursuant to a search warrant issued under this section and § 19.2-70.3 using the same process described
102 in the preceding paragraph.

103 Notwithstanding the provisions of § 19.2-57, any search warrant for records or other information
104 pertaining to a customer of a financial institution as defined in § 6.2-604, money transmitter as defined
105 in § 6.2-1900, commercial business providing credit history or credit reports, or issuer as defined in
106 § 6.2-424 may be executed within the Commonwealth by hand, United States mail, commercial delivery
107 service, facsimile, or other electronic means upon the financial institution, money transmitter,
108 commercial business providing credit history or credit reports, or issuer. The officer executing such
109 warrant shall endorse the date of execution thereon and shall file the warrant, with the inventory
110 attached (or a notation that no property was seized) and the accompanying affidavit, unless such
111 affidavit was made by voice or videotape recording, within three days after the materials ordered to be
112 produced are received by the officer from the financial institution, money transmitter, commercial
113 business providing credit history or credit reports, or issuer. The return shall be made in the circuit court
114 clerk's office for the jurisdiction wherein the warrant was executed. Saturdays, Sundays, or any federal
115 or state legal holiday shall not be used in computing the three-day filing period. For the purposes of this
116 section, the warrant will be considered executed in the jurisdiction where the entity on which the
117 warrant is served is located.

118 Every search warrant shall contain the date and time it was issued. However, the failure of any such
119 search warrant to contain the date and time it was issued shall not render the warrant void, provided that
120 the date and time of issuing of said warrant is established by competent evidence.

The judge, magistrate, or other official authorized to issue criminal warrants shall attach a copy of the affidavit required by § 19.2-54, which shall become a part of the search warrant and served therewith. However, this provision shall not be applicable in any case in which the affidavit is made by means of a voice or videotape recording or where the affidavit has been sealed pursuant to § 19.2-54.

Any search warrant not executed within 15 days after issuance thereof shall be returned to, and voided by, the officer who issued such search warrant.

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.

"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.

§ 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

182 data sought is relevant to a crime that is being committed or has been committed or that an arrest
183 warrant exists for the person whose ~~real-time~~ location data is sought.

184 D. A provider of electronic communication service or remote computing service, including a foreign
185 corporation that provides such services, shall disclose a record or other information pertaining to a
186 subscriber to or customer of such service, including ~~real-time~~ location data but excluding the contents of
187 electronic communications, to an investigative or law-enforcement officer pursuant to an administrative
188 subpoena issued pursuant to § 19.2-10.2 concerning a violation of § 18.2-374.1 or 18.2-374.1:1, former
189 § 18.2-374.1:2, or § 18.2-374.3 when the information sought is relevant and material to an ongoing
190 criminal investigation.

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

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

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

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

203 4. If the investigative or law-enforcement officer reasonably believes that an emergency involving the
204 immediate danger to a person requires the disclosure, without delay, of real-time location data
205 concerning a specific person and that a warrant cannot be obtained in time to prevent the identified
206 danger.

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

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

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

229 H. The provider of electronic communication service or remote computing service may verify the
230 authenticity of the written reports or records that it discloses pursuant to this section by providing an
231 affidavit from the custodian of those written reports or records or from a person to whom said custodian
232 reports certifying that they are true and complete copies of reports or records and that they are prepared
233 in the regular course of business. When so authenticated, no other evidence of authenticity shall be
234 necessary. The written reports and records, excluding the contents of electronic communications, shall be
235 considered business records for purposes of the business records exception to the hearsay rule.

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

240 J. A search warrant or administrative subpoena for the disclosure of real-time location data pursuant
241 to this section shall require the provider to provide ongoing disclosure of such data for a reasonable
242 period of time, not to exceed 30 days. A court may, for good cause shown, grant one or more
243 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 *to collect real-time location data* without first obtaining a search warrant under the circumstances set forth in subsection E. For purposes of subdivision E 4, 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.

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

"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 by, derived from, or obtained by the operation of the device.