16104636D

HOUSE BILL NO. 1332

Offered January 21, 2016

A BILL to amend the Code of Virginia by adding in Title 2.2 a chapter numbered 38.2, consisting of sections numbered 38.2.1 through 38.2.5, relating to the Virginia Electronic Communications Privacy Act; report.

Patrons—Dudenhefer and Anderson

Referred to Committee on Commerce and Labor

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 2.2 a chapter numbered 38.2, consisting of sections numbered 38.2.1 through 38.2.5, as follows:

Virginia Electronic Communications Privacy Act

Chapter 38.2

§ 38.2.1 Definitions.

For purposes of this chapter, unless the context requires a different meaning:

"Adverse result" shall mean any of the following:

1. Danger to the life or physical safety of an individual.

2. Flight from prosecution.

3. Destruction of or tampering with evidence.

4. Intimidation of potential witnesses.

5. Serious jeopardy to an investigation.

"Agency" means any agency, authority, board, department, division, commission, institution, bureau, or like governmental entity of the Commonwealth or of any unit of local government including counties, cities, towns, regional governments, and the departments thereof, and includes constitutional officers, except as otherwise expressly provided by law. "Agency" shall also include any entity, whether public or private, with which any of the foregoing has entered into a contractual relationship for the operation of a system of personal information to accomplish an agency function.

"Authorized possessor" shall mean the person in possession of an electronic device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

"Electronic communication" shall mean the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

"Electronic communication information" shall mean any information about an electronic communication or the use of an electronic communication service, including, but not limited to, the contents, sender, recipients, format, or precise or approximate location of the sender or recipients at any point during the communication, the time or date the communication was created, sent, or received, or any information pertaining to any individual or device participating in the communication, including, but not limited to, an IP address. Electronic communication information does not include subscriber information as defined in this Act.

"Electronic communication service" shall mean a service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.

"Electronic device" shall mean a device that stores, generates, or transmits information in electronic form.

"Electronic device information" shall mean any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device.

"Electronic information" shall mean electronic communication information or electronic device information.

"Service provider" shall mean a person or entity offering an electronic communication service.

"Specific consent" shall mean consent provided directly to the agency seeking information, including, but not limited to, when the agency is the addressee or intended recipient or a member of the intended audience of an electronic communication. Specific consent does not require that the originator of the communication have actual knowledge that an addressee, intended recipient, or member of the specific audience is an agency, except where a government employee or agent has taken deliberate steps to hide their government association.

"Subscriber information" shall mean the name, street address, telephone number, email address, or similar contact information provided by the subscriber to the provider to establish or maintain an

account or communication channel, a subscriber or account number or identifier, the length of service, and the types of services used by a user of or subscriber to a service provider.

§38.2.2 Access to electronic communication information and devices.

A. Except as provided in this Section, an agency shall not do any of the following:

1. Compel or incentivize the production of or access to electronic communication information from a service provider.

2. Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.

3. Access electronic device information by means of physical interaction or electronic communication with the electronic device.

B. An agency may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device only under the following circumstances:

1. Pursuant to a warrant issued pursuant to Section 19.2-70.3 of the Code of Virginia and subject to Section 38.2.2.D.

2. Pursuant to a wiretap order issued pursuant to Section 19.2-68 of the Code of Virginia.

C. An agency may access electronic device information by means of physical interaction or electronic communication with the device only as follows:

1. Pursuant to a warrant issued pursuant to Section 19.2-70.3 of the Code of Virginia and subject to Section 38.2.2.D.

2. Pursuant to a wiretap order issued pursuant to Section 19.2-68 of the Code of Virginia.

3. With the specific consent of the authorized possessor of the device.

4. With the specific consent of the owner of the device, only when the device has been reported as lost or stolen.

5. If the agency, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

D. Any warrant for electronic information shall comply with the following:

1. The warrant shall describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the applications or services covered, and the types of information sought.

2. The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be destroyed within thirty days and not subject to further review, use, or disclosure; provided that this section shall not apply when the information obtained is exculpatory with respect to the targeted individual.

3. The warrant shall comply with all other provisions of Virginia and federal law, including any provisions prohibiting, limiting, or imposing additional requirements on the use of search warrants.

E. When issuing any warrant or order for electronic information, or upon the petition from the target or recipient of the warrant or order, a court may, at its discretion, review the warrant or order to ensure that only information necessary to achieve the objective of the warrant or order is produced or accessed.

F. A service provider may voluntarily disclose electronic communication information or subscriber information when that disclosure is not otherwise prohibited by state or federal law.

G. If an agency receives electronic communication information voluntarily provided pursuant to Section 38.2.2.F., it shall destroy that information within 90 days unless one or more of the following circumstances apply:

1. The entity has or obtains the specific consent of the sender or recipient of the electronic communications about which information was disclosed.

2. The entity obtains a court order authorizing the retention of the information. A court shall issue a retention order upon a finding that the conditions justifying the initial voluntary disclosure persist, in which case the court shall authorize the retention of the information only for so long as those conditions persist, or there is probable cause to believe that the information constitutes evidence that a crime has been committed.

a) Information retained subject to this provision shall not be shared with:

(i) Any persons or entities that do not agree to limit their use of the provided information to those purposes contained in the court authorization; and

(ii) Any persons or entities that:

(A) Are not legally obligated to destroy the provided information upon the expiration or rescindment of the court's retention order; or

(B) Do not voluntarily agree to destroy the provided information upon the expiration or rescindment of the court's retention order.

INTRODUCED

H. If an agency obtains electronic information pursuant to an emergency involving danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the entity shall, within three days after obtaining the electronic information, file with the appropriate court an application for a warrant or order authorizing obtaining the electronic information or a motion seeking approval of the emergency disclosures that shall set forth the facts giving rise to the emergency, and if applicable, a request supported by a sworn affidavit for an order delaying notification under Section 38.2.3.B.1. The court shall promptly rule on the application or motion and shall order the immediate destruction of all information obtained, and immediate notification pursuant to Section 38.2.3.A if such notice has not already been given, upon a finding that the facts did not give rise to an emergency or upon rejecting the warrant or order application on any other ground.

I. This Section does not limit the authority of an agency to use an administrative, grand jury, trial, or civil discovery subpoena to do any of the following:

1. Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication.

2. Require an entity that provides electronic communications services to its officers, directors, employees, or agents for the purpose of carrying out their duties, to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee, or agent of the entity.

3. Require a service provider to provide subscriber information.

J. This Section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to an agency.

K. Nothing in this Section shall be construed to expand any authority of agencies to compel the production of or access to electronic information.

§38.2.3. Service; notice of service; delay in notice of service.

A. Except as otherwise provided in this Section, any agency that executes a warrant, or obtains electronic information in an emergency pursuant to 38.2.2, shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant or emergency request, a notice that informs the recipient that information about the recipient has been compelled or requested, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant or a written statement setting forth facts giving rise to the emergency. The notice shall be provided contemporaneously with the execution of a warrant, or, in the case of an emergency, within three days after obtaining the electronic information.

B. When a warrant is sought or electronic information is obtained in an emergency under Section 38.2.2.H, the agency may submit a request supported by a sworn affidavit for an order delaying notification and prohibiting any party providing information from notifying any other party that information has been sought. The court shall issue the order if the court determines that there is reason to believe that notification may have an adverse result, but only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days.

1. The court may grant extensions of the delay of up to 90 days each on the same grounds as provided in Section 38.2.2.H.

2. Upon expiration of the period of delay of the notification, the agency shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective as specified by the court issuing the order authorizing delayed notification, the identified targets of the warrant, a document that includes the information described in Section 38.2.3.A, a copy of all electronic information obtained or a summary of that information, including, at a minimum, the number and types of records disclosed, the date and time when the earliest and latest records were created, and a statement of the grounds for the court's determination to grant a delay in notifying the individual.

C. If there is no identified target of a warrant or emergency request at the time of its issuance, the agency shall submit to the Attorney General within three days of the execution of the warrant or issuance of the request all of the information required in Section 38.2.3.A.. If an order delaying notice is obtained pursuant to Section 32.8.B, the agency shall submit to the Attorney General upon the expiration of the period of delay of the notification all of the information required in Section 38.2.3.B.2.. The Attorney General's office shall publish all those reports on its Internet Web site within 90 days of receipt. The Attorney General shall redact names or other personal identifying information from the reports.

D. Except as otherwise provided in this Section, nothing in this Act shall prohibit or limit a service provider or any other party from disclosing information about any request or demand for electronic information.

§38.2.4. Electronic information unlawfully obtained or retained.

A. Any person in a trial, hearing, or proceeding may move to suppress any electronic information obtained or retained in violation of the United States Constitution, Constitution of Virginia, or of this Chapter.

B. The Attorney General may commence a civil action to compel any agency to comply with the provisions of this Act.

C. An individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with this Act, or the Constitution of Virginia or the United States Constitution, or a service provider or any other recipient of the warrant, order, or other legal process may petition the issuing court to void or modify the warrant, order, or process, or to order the destruction of any information obtained in violation of this Act, or the Constitution of Virginia, or the United States Constitution.

D. A Virginia or foreign corporation, and its officers, employees, and agents, are not subject to any cause of action for providing records, information, facilities, or assistance in accordance with the terms of a warrant, court order, statutory authorization, emergency certification, or wiretap order issued pursuant to this Act.

§Section 38.2.5. Reports.

A. An agency that obtains electronic communication information pursuant to this Act shall make an annual report to the Attorney General. The report shall be made on or before February 1, 2018, and each February 1 thereafter. To the extent it can be reasonably determined, the report shall include all of the following:

1.The total number of times electronic information was sought or obtained pursuant to this Act.

2. For each of the following types of information, the number of times such information was sought or obtained, and the number of records obtained:

a) Electronic communication content.

b) Location information.

c) Electronic device information (not including location information).

d) Other electronic communication information.

3. For each of the types of information listed in Section 38.2.5.A.2, all of the following:

e) The number of times that type of information was sought or obtained pursuant to:

(i) Wiretap orders obtained pursuant to this Act.

(ii) Search warrants obtained pursuant to this Act.

(iii) Emergency requests subject to Section 38.2.2.H.

f) The total number of individuals whose information was sought or obtained.

g) The total number of instances where information was sought or obtained that did not specify a target individual.

h) For demands or requests issued upon a service provider, the number of such demands or requests complied with in full, partially complied with, and refused.

i) The number of times notice to targeted individuals was delayed and the average length of the delay.

j) The number of times records were shared with other agencies or any department or agency of the federal government, and the agencies with which the records were shared.

k) For location information, the average period for which location information was obtained or received.

l) The number of times electronic information obtained pursuant to this Act led to a conviction, and the number of instances where electronic information was sought or obtained that were relevant to the criminal proceedings leading to those convictions.

B. On or before December 1, 2017, and each December 1 thereafter, the Attorney General's office shall publish on its Internet Web site both of the following:

1) The individual reports from each agency that requests or compels the production of contents or records pertaining to an electronic communication or location information.

2) A summary aggregating each of the items in Section 38.2.5.A.1.-3.

C. Nothing in this Act shall prohibit or restrict a service provider from producing an annual report summarizing the demands or requests it receives under this Act.