SENATE BILL NO. 246–SENATOR SEEVERS GANSERT

MARCH 15, 2021

Referred to Committee on Judiciary

SUMMARY—Prohibits the collection of surveillance data by law enforcement agencies under certain circumstances. (BDR 14-828)

FISCAL NOTE: Effect on Local Government: No.
Effect on the State: No.

~

EXPLANATION – Matter in ***bolded italics*** is new; matter between brackets **[**~~omitted material~~**]** is material to be omitted.

AN ACT relating to criminal procedure; defining certain terms, including the term "surveillance data"; prohibiting law enforcement agencies from obtaining surveillance data except when authorized by a data warrant or in certain other circumstances; establishing provisions relating to applying for, issuing and executing a data warrant; establishing provisions relating to the disclosure, retention and admissibility of surveillance data; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law requires certain persons to obtain an order authorizing the interception of wire, electronic or oral communications before intercepting such communications. (NRS 179.410-179.515) **Sections 2-21** of this bill establish similar provisions relating to the collection of certain surveillance data. **Sections 3-12** of this bill define certain terms for the purposes of the procedures relating to data warrants, including the term "surveillance data."

Sections 13 and 14 of this bill prohibit a law enforcement agency from collecting surveillance data unless a data warrant is obtained by the law enforcement agency or certain other circumstances apply.

If the surveillance data sought by the law enforcement agency is location information from an electronic device, **section 13** of this bill authorizes the law enforcement agency to obtain the location information without a data warrant if: (1) the electronic device is reported stolen; (2) an owner or user of the electronic device gives informed consent for the collection of the location information; (3) the collection falls within a judicially recognized exception to the requirement to obtain a warrant; (4) the owner has voluntarily and publicly disclosed the location information; or (5) certain other circumstances apply relating to the voluntary disclosure of the location information by a provider of remote computing service.

If the surveillance data sought by the law enforcement agency is stored data or transmitted data from an electronic device, or electronic information or data from a provider of remote computing service, **section 13** authorizes the law enforcement agency to collect such data or information without a data warrant if: (1) the owner of the electronic device or electronic information or data gives informed consent to the collection of the data or information; (2) the collection falls within a judicially recognized exception to the requirement to obtain a warrant; (3) the collection is made in connection with a report from the National Center for Missing and Exploited Children; or (4) certain other circumstances apply relating to the voluntary disclosure of the data or information by a provider of remote computing service.

If the surveillance data is third-party data, **section 14** of this bill authorizes the law enforcement agency to obtain the third-party data without a data warrant if: (1) the law enforcement agency obtains the informed consent of the applicable subscriber or customer; (2) the collection falls within a judicially recognized exception to the requirement to obtain a warrant; (3) the applicable subscriber or customer voluntarily discloses the third-party data in a manner that is publicly accessible; or (4) certain other circumstances apply relating to the voluntary disclosure of the third-party data by the provider of electronic communication service or remote computing service.

Additionally, **sections 13 and 14** authorize a district judge to issue a data warrant if a complete application is: (1) submitted by the Attorney General or a district attorney; and (2) supported by probable cause to believe that a person is committing, has committed or is about to commit an offense and the surveillance data sought to be collected by the law enforcement agency concerns the described offense. **Section 15** of this bill requires an application for a data warrant to contain certain information. Similarly, **section 16** of this bill requires a data warrant to contain certain information.

Section 17 of this bill requires a law enforcement agency to destroy certain surveillance data that is incidentally collected in the execution of the data warrant under certain circumstances. Additionally, **section 18** of this bill: (1) authorizes the disclosure of surveillance data under certain circumstances; and (2) provides that privileged surveillance data maintains its privilege despite its collection pursuant to **sections 2-21**.

Section 19 of this bill requires notice of a data warrant to be provided to certain persons and sets forth various procedures concerning the provision of such notice.

Section 20 of this bill authorizes certain persons to move to suppress surveillance data under certain circumstances and provides various procedures relating to such motions to suppress.

Section 21 of this bill exempts a provider of electronic communication service, a provider of remote computing service and certain persons associated therewith from liability for the provision of information, facilities or assistance made in a good faith reliance on **sections 13 and 14**.

Existing law authorizes the Nevada Supreme Court and the district courts of this State to issue orders requiring a provider of electronic communication service to disclose the contents of a wire or electronic communication or a record or other information pertaining to a subscriber to, or customer of, such service under certain circumstances. (NRS 179.467) **Section 22** of this bill removes the provisions concerning records or other information pertaining to a subscriber to, or customer of, a provider of electronic communication service because such records and information qualify as third-party data and are subject to the procedures contained in **sections 2-21** of this bill concerning data warrants.

THE PEOPLE OF THE STATE OF NEVADA, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. Chapter 179 of NRS is hereby amended by adding thereto the provisions set forth as sections 2 to 21, inclusive, of this act.

Sec. 2. ***As used in sections 2 to 21, inclusive, of this act, unless the context otherwise requires, the words and terms defined in sections 3 to 12, inclusive, of this act have the meanings ascribed to them in those sections.***

Sec. 3. ***"Electronic communication service" has the meaning ascribed to it in NRS 179.423.***

Sec. 4. ***1. "Electronic device" means a device that enables access to or use of an electronic communication service, a remote computing service or a location information service.***

2. As used in this section, "location information service" means the provision of a global positioning service or other service for mapping, location or directional information.

Sec. 5. ***1. "Electronic information or data" means information or data including, without limitation, a sign, a signal, a writing, an image, a sound or an item of intelligence of any nature transmitted or stored, in whole or in part, by a wire or radio or an electromagnetic, a photoelectronic or a photooptical system. The term includes, without limitation, the location information, stored data and transmitted data of an electronic device.***

2. The term does not include:

(a) A wire communication or an oral communication.

(b) A communication made through a tone-only paging device.

(c) Electronic funds transfer information stored by a financial institution in a communication system used for the electronic storage and transfer of funds.

3. As used in this section:

(a) "Oral communication" has the meaning ascribed to it in NRS 179.440.

(b) "Wire communication" has the meaning ascribed to it in NRS 179.455.

Sec. 6. ***"Location information" means information obtained by means of a tracking device which concerns the location of an electronic device, the information of which is generated, derived or obtained, in whole or in part, by the operation of the electronic device.***

Sec. 7. ***"Remote computing service" means the provision of computer storage or processing services to the public by means of an electronic communication system.***

Sec. 8. *"Sexual abuse" has the meaning ascribed to it in NRS 432B.100.*

Sec. 9. *"Surveillance data" means target data or third-party data, or both.*

Sec. 10. *"Target data" means:*

1. Location information, stored data or transmitted data of an electronic device; or

2. Electronic information or data transmitted by its owner to a provider of remote computing service.

Sec. 11. *1. "Third-party data" means:*

(a) A subscriber record; or

(b) Any other record or information of a provider of electronic communication service or remote computing service relating to a subscriber or customer of the provider.

2. As used in this section, "subscriber record" means a record or information of a provider of electronic communication service or remote computing service that reveals any of the following in relation to a subscriber or customer of the provider:

(a) A name;

(b) An address;

(c) A local or long distance telephone connection record, or a record of session time and duration;

(d) The length of service, including, without limitation, the start date of the service;

(e) A telephone number, instrument number or other subscriber or customer number or any other form of identification, including, without limitation, a temporarily assigned network address; or

(f) The means and source of payment for the service, including, without limitation a credit card or bank card number.

Sec. 12. *"Transmitted data" means electronic information or data that is transmitted wirelessly from an electronic device to:*

1. Another electronic device without the use of an intermediate connection relay; or

2. A nearby antenna.

Sec. 13. *1. Except as otherwise provided in this section and section 17 of this act, a law enforcement agency shall not obtain target data.*

2. The Attorney General or the district attorney of any county may apply to a district judge in the county where the target data is to be obtained, and the judge may grant a data warrant if the application is complete and supported by probable cause to believe that:

(a) A person is committing, has committed or is about to commit an offense; and

(b) The target data relates to the offense described in paragraph (a).

3. A law enforcement agency may obtain without a data warrant:

(a) Location information for an electronic device if:

(1) The electronic device is reported stolen;

(2) The law enforcement agency obtains the informed consent of an owner or user of the electronic device;

(3) The location information is obtained in accordance with a judicially recognized exception to the requirement to obtain a warrant;

(4) The owner of the electronic device has voluntarily and publicly disclosed the location information; or

(5) A provider of remote computing service voluntarily discloses the location information:

(I) Under the belief that an emergency exists involving a risk of substantial bodily harm, sexual abuse, kidnapping or trafficking in persons in violation of NRS 200.467 or 200.468; or

(II) After the location information was inadvertently discovered by the provider of remote computing service and it appears to relate to the commission of a misdemeanor involving the use or threatened use of force or violence against the victim, a misdemeanor involving dishonesty or a felony.

(b) Stored data or transmitted data from an electronic device or electronic information or data that is transmitted by its owner to a provider of remote computing service if:

(1) The law enforcement agency obtains the informed consent of the owner of the electronic device or electronic information or data;

(2) The stored data, electronic data or electronic information or data is obtained by the law enforcement agency:

(I) In accordance with a judicially recognized exception to the requirement to obtain a warrant; or

(II) In connection with a report forwarded by the National Center for Missing and Exploited Children pursuant to 18 U.S.C. § 2258A; or

(3) A provider of remote computing service voluntarily discloses the stored data, transmitted data or electronic information or data in accordance with 18 U.S.C. § 2702.

Sec. 14. ***1. Except as otherwise provided in subsections 2 and 3, a law enforcement agency shall not obtain third-party data.***

2. The Attorney General or the district attorney of any county may apply to the district judge in the county where the third-party data is to be obtained, and the judge may grant a data warrant if

the application is complete and supported by probable cause to believe that:

(a) A person is committing, has committed or is about to commit an offense; and

(b) The third-party data relates to the offense described in paragraph (a).

3. A law enforcement agency may obtain third-party data without a data warrant if:

(a) The law enforcement agency obtains the informed consent of the applicable subscriber or customer;

(b) In accordance with a judicially recognized exception to the requirement to obtain a warrant;

(c) The applicable subscriber or customer voluntarily discloses the third-party data in a manner that is publicly accessible; or

(d) A provider of electronic communication service or remote computing service voluntarily discloses the third-party data:

(1) Under the belief that an emergency exists involving risk of substantial bodily harm, sexual abuse, kidnapping or trafficking in persons in violation of NRS 200.467 or 200.468;

(2) After the third-party data was inadvertently discovered by the provider and it appears to relate to the commission of a misdemeanor involving the use or threatened use of force or violence against the victim, a misdemeanor involving dishonesty or a felony; or

(3) In accordance with 18 U.S.C. § 2702.

Sec. 15. *1. Each application for a data warrant must be made in writing upon oath or affirmation to a district judge and must state the authority of the applicant to make such an application. Each application must include the following information:*

(a) The identities of the person making the application and the person authorizing the application.

(b) A full and complete statement of the facts and circumstances relied upon by the applicant to justify his or her belief that the data warrant should be issued by the judge, including, without limitation:

(1) Details as to the particular offense that is being, has been or is about to be committed;

(2) The identity of the person, if known:

(I) Who is committing, has committed or is about to commit the offense; and

(II) Whose surveillance data is being sought by the law enforcement agency; and

(3) A particular description of:

(I) The type of the surveillance data;

(II) The electronic device, electronic communication service or remote computing service from which the surveillance data will be obtained by the law enforcement agency; and

(III) The means by which the law enforcement agency will obtain the surveillance data.

(c) A full and complete statement as to whether or not other investigative procedures have been tried and failed or why such procedures reasonably appear to be unlikely to succeed or too dangerous if tried.

(d) A statement of the period of time for which law enforcement agency seeks to obtain the surveillance data. If the nature of the investigation is such that the authorization for obtaining the surveillance data should not automatically terminate when the surveillance data has been obtained by the law enforcement agency, a particular description of the facts establishing probable cause to believe that additional surveillance data of the same type could be obtained thereafter.

(e) A full and complete statement of the facts concerning all previous applications known to the persons authorizing and making the application made to any judge for authorization to obtain surveillance data involving any of the same persons, devices or providers specified in the application, and the action taken by the judge on each such application.

(f) If the application is for the extension of a data warrant, a statement setting forth the results thus far obtained from the collection of the surveillance data or a reasonable explanation for the failure to obtain such results.

2. The judge may require the applicant to furnish additional testimony or documentary evidence under oath or affirmation in support of the application. Oral testimony must be reduced to writing.

3. The judge may accept a facsimile or an electronic copy of the signature of any person required to give an oath or affirmation as part of an application submitted pursuant to this section as an original signature to the application.

Sec. 16. *1. A data warrant must specify:*

(a) The identities of the law enforcement agency authorized to execute the data warrant and the person authorizing the application.

(b) The identity of the person, if known:

(1) Who is committing, has committed or is about to commit the offense; and

(2) Whose surveillance data is being sought by the law enforcement agency;

(c) A particular description of:

(1) The type of surveillance data;

(2) The electronic device, electronic communication service or remote computing service from which the surveillance data will be obtained by the law enforcement agency; and

(3) The means by which the law enforcement agency will obtain the surveillance data; and

(d) The period of time during which the law enforcement agency is authorized to obtain the surveillance data, including a statement as to whether or not the authorization will automatically terminate when the surveillance data has been obtained by the law enforcement agency.

2. A data warrant must, upon request of the applicant, direct that a provider of electronic communication service or remote computing service furnish the applicant forthwith with all information, facilities and technical assistance necessary to accomplish the collection unobtrusively and with a minimum of interference with the services being provided to the person whose surveillance data is to be obtained. Any provider of electronic communication service or remote computing service furnishing such information, facilities or technical assistance must be compensated therefor by the applicant at the prevailing rates.

3. Extensions of a data warrant may be granted, but only upon application for an extension made in accordance with the procedures provided in sections 2 to 21, inclusive, of this act. The period of extension must not be longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than 30 days.

Sec. 17. *1. Except as otherwise provided in subsection 2, a law enforcement agency may not use, copy or disclose any target data that is incidentally collected from devices or providers other than those described in the data warrant. The law enforcement agency shall destroy any target data so incidentally collected within 60 days of its incidental collection.*

2. A law enforcement agency may use, copy or disclose transmitted data of an electronic device used to communicate with the electronic device that is the subject of a data warrant if the law enforcement agency reasonably believes that the transmitted data is necessary to achieve the objectives of the data warrant.

Sec. 18. *1. The Attorney General, a district attorney or law enforcement officer who, by any means authorized pursuant to sections 2 to 21, inclusive, of this act, has obtained surveillance data, may disclose the surveillance data to another official or officer or use the surveillance data to the extent that the disclosure or use is appropriate to the proper performance of the official duties of the official or officer making or receiving the disclosure.*

2. Any person who has received, by any means authorized pursuant to sections 2 to 21, inclusive, of this act, any surveillance data, or evidence derived therefrom, obtained in accordance with sections 2 to 21, inclusive of this act, may disclose the surveillance data, or the evidence derived therefrom, while giving testimony under oath or affirmation in any criminal proceeding in any court or before any grand jury in this State, or in any court of the United States or of any state or in any federal or state grand jury proceeding.

3. Otherwise privileged surveillance data collected in accordance with, or in violation of, the provisions of sections 2 to 21, inclusive, of this act, does not thereby lose its privileged character.

Sec. 19. ***1. Except as otherwise provided in this section, not later than 14 days after the termination of the period of execution described in the data warrant, or any extension thereof, as applicable, the law enforcement agency who executed the data warrant shall issue a notice to any person specified in the data warrant as the owner of the electronic device or the owner of the surveillance data, as applicable. The notice must include, without limitation:***

(a) A statement relaying that a data warrant was applied for and granted by a court of competent jurisdiction;

(b) The period of time during which the law enforcement agency was authorized by the court to execute the data warrant;

(c) The offense specified in the application for the data warrant;

(d) The identity of the law enforcement agency executing the data warrant; and

(e) The identity of the judge who issued the data warrant.

2. If the identity of the owner of the electronic device or the owner of the surveillance data, as applicable, is not known on the date that notice is required to be issued pursuant to subsection 1, the notice must be served on the applicable person not later than 14 days after his or her identity becomes known to the law enforcement agency who executed the data warrant.

3. The law enforcement agency who executed the data warrant may apply to the court that issued the data warrant for permission to delay the issuance of the notice described in subsection 1 for a period not to exceed 30 days. The application must demonstrate probable cause to believe that the issuance of the notice may:

(a) Endanger the life or safety of a person;

(b) Cause a person to flee from prosecution;

(c) Lead to the destruction or tampering of evidence;

(d) Intimidate a potential witness;

(e) Seriously jeopardize an investigation; or

(f) Unduly delay a trial.

4. If the issuance of the notice is delayed pursuant to subsection 3, the law enforcement agency may again apply to the court who issued the data warrant for permission to delay the issuance of the notice for:

(a) An additional period not to exceed 30 days; or

(b) An additional period not to exceed 60 days, if the application demonstrates that the investigation relating to the data warrant is:

(1) Interstate in nature and sufficiently complex; or

(2) Likely to extend up to or beyond an additional 60 days.

5. Upon the expiration of the period of delay described in subsection 3 or 4, as applicable, the law enforcement agency must serve or send by first-class mail a notice and a copy of the data warrant to the person specified in the data warrant as the owner of the electronic device or the owner of the surveillance data, as applicable. The notice must include, without limitation:

(a) A statement detailing with reasonable specificity the nature of the investigation by the law enforcement agency;

(b) The information described in subsection 1;

(c) A statement that the notice was delayed;

(d) The name of the court that authorized the notice to be delayed; and

(e) A reference to this section.

6. A law enforcement agency is not required to send notice pursuant to this section to a person who is located outside of the United States.

Sec. 20. *1. Any aggrieved person in any trial, hearing or proceeding in or before any court, department, officer, agency or other authority of this State, or a political subdivision thereof, may move to suppress surveillance data, or evidence derived therefrom, on the grounds that:*

(a) The surveillance data was unlawfully obtained;

(b) The data warrant under which the surveillance data was obtained is insufficient on its face;

(c) The collection of the surveillance data was not made in conformity with the data warrant; or

(d) The period of execution for the data warrant and any extension thereof had expired.

2. A motion pursuant to subsection 1 must be made before the trial, hearing or proceeding unless there was not an opportunity to make such a motion or the person was not aware of the grounds for the motion. If the motion is granted, the surveillance data, or

evidence derived therefrom, must be treated as having been obtained in violation of sections 2 to 21, inclusive, of this act. The judge, upon the filing of such motion by the aggrieved person, may in the judge's discretion make available to the aggrieved person or the aggrieved person's counsel for inspection such portions of the surveillance data, or evidence derived therefrom, as the judge determines to be in the interest of justice.

3. As used in this section, "aggrieved person" means any person whose information was collected pursuant to a data warrant.

Sec. 21. ***A provider of electronic communication service or remote computing service, or an officer, employee or agent thereof, or another person associated with any such provider is not liable for providing information, facilities or assistance in a good faith reliance on:***

1. The terms of a data warrant; or

2. An exception to the requirement to obtain a data warrant for the collection of:

(a) Target data pursuant to subsection 3 of section 13 of this act; or

(b) Third-party data pursuant to subsection 3 of section 14 of this act.

Sec. 22. NRS 179.467 is hereby amended to read as follows:

179.467 1. The Nevada Supreme Court and the district courts of this State may issue orders requiring a provider of electronic communication service to disclose the contents of a wire or electronic communication ~~[or a record or other information pertaining to a subscriber to, or customer of, such service]~~ upon the application of a district attorney or the Attorney General, or their deputies, supported by an affidavit of a peace officer under the circumstances and upon the conditions prescribed by 18 U.S.C. § 2703.

2. A provider of electronic communication service, an officer, employee or agent thereof or another person associated with the provider of electronic communication service who, pursuant to an order issued by a district court pursuant to subsection 1, discloses the contents of a wire or electronic communication or a record or other information pertaining to a subscriber to, or customer of, the electronic communication service is immune from any liability relating to any disclosure made pursuant to the order.

㉚