SENATE BILL NO. 213-SENATOR HANSEN

MARCH 11, 2021

Referred to Committee on Judiciary

SUMMARY—Establishes provisions relating to the use of surveillance devices. (BDR 14-678)

FISCAL NOTE: Effect on Local Government: May have Fiscal Impact. Effect on the State: Yes.

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 device"; prohibiting law enforcement officers from using surveillance devices except when authorized by surveillance warrants or in exigent circumstances; establishing provisions relating to applying, issuing and executing surveillance warrants; establishing provisions relating to the disclosure, retention, admissibility and reporting of information obtained through surveillance warrants; requiring the Attorney General to develop certain training protocols regarding surveillance devices; establishing certain additional reporting requirements relating to surveillance warrants; providing for a civil action under certain circumstances; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

Existing law requires certain persons to obtain a court order authorizing the interception of wire, electronic or oral communications before intercepting such communications. (NRS 179.410-179.515) Similarly, existing law provides that a district court may issue an order authorizing the use of a pen register or trap and trace device. (NRS 179.530) Sections 2 and 23 of this bill provide that, with certain exceptions, the provisions of sections 3-21 of this bill govern the collection of information by surveillance devices, regardless of the type of information sought to be collected by the device. Section 22 of this bill makes a conforming change to indicate the proper placement of section 2 in the Nevada Revised Statutes.

Section 9 of this bill prohibits a law enforcement officer from using a surveillance device unless: (1) a surveillance warrant is first obtained; or (2) in certain exigent circumstances. Additionally, **section 9** authorizes a district judge to





grant a surveillance warrant, initially or upon the cessation of an exigent circumstance, if a complete application is submitted by the Attorney General or the district attorney of any county and the application is supported by probable cause to believe that a person is committing, has committed or is about to commit an offense and the information sought to be collected by the surveillance device concerns the described offense.

Section 10 of this bill provides that an application for a surveillance warrant must contain certain information. **Section 11** of this bill requires a surveillance warrant to contain certain information and places certain timing and geographic limitations on the warrant.

Section 12 of this bill requires any law enforcement officer executing a surveillance warrant to: (1) limit the incidental collection of information that falls outside the scope of the surveillance warrant and immediately destroy such incidental information if so collected; and (2) destroy any information that is collected within the scope of the surveillance warrant that does not give rise to probable cause of the commission of an offense.

Section 13 of this bill requires the information collected through a surveillance warrant to be recorded, if possible. **Section 13** also requires such recordings to be retained for 10 years unless otherwise required to be destroyed before such time.

Section 14 of this bill: (1) authorizes the disclosure of information collected from a surveillance warrant under certain circumstances; and (2) provides that privileged information so collected remains privileged in character despite its collection by the surveillance device.

Section 15 of this bill requires notice of a surveillance warrant to be provided to certain persons. Similarly, section 16 of this bill prohibits any information collected through a surveillance warrant from being received into evidence or otherwise disclosed in court unless a copy of the warrant, its application and any information so collected is transmitted to certain persons at least 10 days before any trial, hearing or other proceeding. Additionally, section 17 of this bill authorizes certain persons to move to suppress information collected from a surveillance warrant under certain circumstances and sets forth the procedure for such a motion to suppress.

Existing law requires the Attorney General and the district attorney of each county to report certain information relating to the interception of wire, electronic and oral communications to the Administrative Office of the United States Courts. Existing law also requires every justice of the Nevada Supreme Court or district judge who grants or denies an order authorizing the interception of wire, electronic or oral communications to report similar information to the Investigation Division of the Department of Public Safety. (NRS 179.515) Section 18 of this bill requires the Attorney General or a district attorney who applies for a surveillance warrant, and any district judge who issues such warrants, respectively, to comply with the requirements for reporting, as applicable.

Section 19 of this bill: (1) requires the Attorney General to develop certain protocols for the training of law enforcement officers relating to the use of surveillance devices; (2) requires a law enforcement agency whose officers operate a surveillance device to conduct such training; and (3) prohibits a law enforcement officer from operating a surveillance device without first receiving such training.

Section 20 of this bill requires: (1) any district judge issuing or denying a surveillance warrant to report annually certain information to the Attorney General; and (2) the Attorney General to submit a report containing such information and certain additional information to the Legislature or Legislative Commission, as applicable, and to post the report to the Internet website of the Attorney General.

Section 21 of this bill authorizes any person whose data is knowingly obtained, accessed, used, transmitted, copied, disclosed or retained in violation of



 $\dot{20}$



sections 3-21 to commence a civil action to recover certain damages from the person or entity that engaged in the violation.

Sections 4-8 of this bill define certain terms, including the term "surveillance device," for purposes of sections 3-21.

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. 1. The provisions of NRS 179.410 to 179.515, inclusive, do not apply to those situations in which a surveillance device is used to collect information that would otherwise qualify as a wire, electronic or oral communication.
- 2. As used in this section, "surveillance device" has the meaning ascribed to it in section 7 of this act.
 - Sec. 3. As used in sections 3 to 21, inclusive, of this act, unless the context otherwise requires, the words and terms defined in sections 4 to 8, inclusive, of this act have the meanings ascribed to them in those sections.
- Sec. 4. "Communications device" means a device that transmits or receives radio waves and is capable of sending or receiving communications, including, without limitation:
 - 1. A cellular telephone;
- 2. An aircard;

- 3. A tablet computer; or
- 4. A laptop computer.
- Sec. 5. 1. "Information" includes, without limitation:
 - (a) The location of a communications device;
- (b) Any identifying information of a subscriber or customer of a communications carrier; or
- (c) The contents of any communications, data or metadata sent or received by or stored on a communications device.
- 2. As used in this section, "communications carrier" means an individual or corporate undertaking to transport messages for compensation.
 - Sec. 6. "Offense" means any violation of state or local law.
- Sec. 7. "Surveillance device" means any cell-site simulator device that transmits or receives radio waves to or from a communications device and that can be used to intercept, collect, access, transfer or forward the data transmitted or received by the communications device, or stored on the communications device, including, without limitation:
 - 1. A Stingray;





2. A Triggerfish;

- 3. An IMSI catcher; or
- 4. A digital analyzer.
- Sec. 8. "Target device" means any communications device targeted by a surveillance device.
- Sec. 9. 1. Except as otherwise provided in subsections 2 and 3, a law enforcement officer shall not use a surveillance device.
- 2. The Attorney General or the district attorney of any county may apply to a district judge in the county in which the use of a surveillance device is to take place for a surveillance warrant authorizing the use of the surveillance device by a law enforcement officer, and the judge may grant the surveillance 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) A target device contains information that concerns the offense described in paragraph (a).
- 3. A law enforcement officer does not need to obtain a surveillance warrant before using a surveillance device if:
- (a) The law enforcement officer determines that an emergency exists that involves substantial bodily harm to a person; and
- (b) The emergency necessitates the use of the surveillance device.
- 4. A law enforcement officer who uses a surveillance device without obtaining a surveillance warrant as described in subsection 3 must, within 48 hours after first using the surveillance device, apply to a district judge in the county in which the surveillance device was used for a surveillance warrant. If the judge finds that an emergency did not occur or otherwise denies the surveillance warrant, any information, or evidence derived therefrom, is inadmissible in any proceeding.
- Sec. 10. 1. Each application for a surveillance 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 application. Each application must include the following information:
- (a) The identity 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 a surveillance 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) A particular description of the surveillance device;
- (3) The identity of the person, if known, who possesses the target device;
 - (4) A particular description of the target device;
- (5) The telephone number or the account number belonging to the service account used by the target device, and the identity of the person, if known, subscribed to such an account;

(6) The geographic area that will be covered by the

11 surveillance device;

(7) A particular description of the type of information sought to be collected from the target device;

(8) If the surveillance device may incidentally collect information from any person or device not specified in the surveillance warrant, a particular description of all such information that may be so incidentally collected by the surveillance device; and

(9) A particular description of any disruptions to access or use of a communications or Internet network that may be caused

by the use of the surveillance device;

- (c) A statement of the period of time for which the surveillance device will be used by the applicant and if the nature of the investigation is such that the authorization for the use of the surveillance device and the collection of information should not automatically terminate when the described information has been obtained, a particular description of the facts establishing probable cause to believe that additional information of the same type will occur thereafter;
- (d) A full and complete statement of the facts concerning all previous applications known to the applicant that were made to any judge for a surveillance warrant involving any of the same persons or target devices specified in the application, and the action taken by the judge on each such application; and

(e) Where the application is for the extension of a surveillance warrant, a statement setting forth the results obtained thus far from the use of the surveillance device, or a reasonable

explanation of 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 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. 11. 1. A surveillance warrant must specify:

- (a) The identity of the law enforcement officer authorized to use the surveillance device, and of the person authorizing the application;
- (b) The information described in subparagraphs (2) to (9), inclusive, of paragraph (b) of subsection 1 of section 10 of this act:
- (c) The period of time during which the use of the surveillance device is authorized, including a statement as to whether or not the authorized use will automatically terminate when the described information has been collected; and
- (d) A provision directing compliance with section 12 of this act.
- 2. A surveillance warrant must not authorize the use of a surveillance device:
- (a) Outside the territorial jurisdiction of the court in which the issuing judge sits; and
- (b) For any period longer than is necessary to achieve the objective of the authorization, and in no event longer than 14 days.
- 3. Extensions of a surveillance warrant may be granted, but only upon application for an extension made in accordance with the procedures provided in sections 3 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 any event not longer than 14 days.
- Sec. 12. Any law enforcement officer executing a surveillance warrant shall take any action necessary to:
- 1. Limit the incidental collection of information belonging to persons and devices other than those described in the surveillance warrant, and immediately destroy any information so incidentally collected; and
- 2. Destroy any information collected from the target device within 30 days after its collection if there is no longer probable cause to support the belief that such information is evidence of an offense.
- Sec. 13. Any information, must, if possible, be recorded on tape or wire device or by other comparable means. The recording of the information pursuant to this section must be done in a manner to protect the recording from editing or other alterations. Immediately upon the expiration of the period of the surveillance warrant, or extensions thereof, all such recordings must be made available to the judge issuing the surveillance warrant. Custody of





the recordings must be placed with whomever the judge directs. Except as otherwise provided in section 12 of this act, the recordings must not be destroyed except upon an order of the judge and in any event must be kept for 10 years.

Sec. 14. 1. The Attorney General, a district attorney or law enforcement officer, respectively, who, by any means authorized pursuant to sections 3 to 21, inclusive, of this act has obtained knowledge of the information derived from a surveillance warrant, may disclose the information to another official or officer, as applicable, or use the information 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 3 to 21, inclusive, of this act any information, or evidence derived therefrom, collected in accordance with sections 3 to 21, inclusive, of this act may disclose the contents of that communication, 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. Information that is otherwise privileged that is collected pursuant to sections 3 to 21, inclusive, of this act does not lose its

privileged character.

- Sec. 15. 1. Unless information collected pursuant to a surveillance warrant is required to be destroyed pursuant to section 12 of this act, within a reasonable time not later than 90 days after the termination of the period of a surveillance warrant, or any extension thereof, the judge who issued the surveillance warrant shall cause to be served on the chief of the Investigation Division of the Department of Public Safety, persons named in the order and any other parties of whom information was collected pursuant to the surveillance warrant, an inventory which must include notice of:
- (a) The fact of the entry and a copy of the surveillance warrant.
- (b) The fact that during the period information was or was not collected pursuant to the surveillance warrant.
- Except as otherwise provided in NRS 239.0115, the inventory filed pursuant to this section is confidential and must not be released for inspection unless subpoenaed by a court of competent jurisdiction.
- 2. The judge, upon receipt of a written request from any person who was a party to information collected pursuant to a surveillance warrant or from the person's counsel, shall make





available to the person or the person's counsel any information collected pursuant to the surveillance warrant that is relevant to the party. On an ex parte showing of good cause to a district judge, the serving of the inventory required by this section may be postponed for such time as the judge may provide.

Sec. 16. Any information collected pursuant to a surveillance warrant or evidence derived therefrom must not be received in evidence or otherwise disclosed in any trial, hearing or other proceeding in any court of this State unless each party, not less than 10 days before the trial, hearing or proceeding, has been furnished with a copy of the surveillance warrant, its application and a transcript or other document which accurately reflects the information collected pursuant to the surveillance warrant. The 10-day period may be waived by the judge if the judge finds that it was not possible to furnish the party with such information 10 days before the trial, hearing or proceeding and that the party will not be prejudiced by the delay in receiving such information.

- Sec. 17. 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 the information collected from a surveillance warrant, or evidence derived therefrom, on the grounds that:
 - (a) The information was unlawfully intercepted.
- (b) The surveillance warrant under which the information was collected is insufficient on its face.
- (c) The collection of information was not made in conformity with the surveillance warrant.
- (d) The period of the surveillance warrant and any extension had expired.
- 2. Such a motion must be made before the trial, hearing or proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion. If the motion is granted, the information collected from the surveillance warrant, or evidence derived therefrom, must be treated as having been obtained in violation of sections 3 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 collected information 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 surveillance warrant.
- Sec. 18. The Attorney General or a district attorney who applies for a surveillance warrant, and any district judge who





signs a surveillance warrant, respectively, shall comply with the reporting requirements set forth in NRS 179.515, to the extent that such requirements are applicable to the surveillance warrant.

- Sec. 19. 1. The Attorney General shall develop protocols for the training of law enforcement officers involved in the authorization, deployment and technical operation of surveillance devices. Such protocols must include instruction on privacy and civil liberties.
- 2. A law enforcement agency whose law enforcement officers operate a surveillance device shall conduct appropriate training based on the protocols developed pursuant to subsection 1.
- 3. A law enforcement officer shall not operate a surveillance device unless the officer has been authorized by his or her law enforcement agency to operate the device and has received training pursuant to this section.
- Sec. 20. 1. In addition to any report required pursuant to NRS 179.515, on or before March 15 of each calendar year, any district judge issuing or denying a surveillance warrant pursuant to section 9 of this act during the preceding calendar year shall report to the Attorney General:
- (a) The number of applications received for surveillance warrants.
- (b) The number of applications for surveillance warrants that were:
 - (1) Denied;

- (2) Modified; and
- (3) Granted.
- (c) The number of surveillance warrants that were granted and whose total duration, including extensions, were:
 - (1) At least 1 but not more than 14 days;
 - (2) At least 15 but not more than 28 days;
 - (3) At least 29 but not more than 42 days; and
 - (4) More than 43 days.
- 2. On or before March 15 of each calendar year, any law enforcement officer who used a surveillance device during the preceding calendar year shall report to the Attorney General:
- (a) The number of applications made for a surveillance warrant.
- (b) Separately, the number of applications for a surveillance warrant that were:
 - (1) Denied;
 - (2) Modified; and
 - (3) Granted.
- (c) With respect to any application for a surveillance warrant or use of a surveillance device without a warrant:





- (1) Whether the application was granted, modified or denied;
 - (2) The offenses specified in the application;
 - (3) The purposes for which the surveillance device was used or, if the application was denied, the proposed purposes for the application;
 - (4) Whether the surveillance device was:
 - (I) Used pursuant to a surveillance warrant;
 - (II) Used without a surveillance warrant; or
 - (III) Unauthorized pursuant to the provisions of sections 3 to 21, inclusive, of this act; or
 - (IV) Never used.

- (5) The geographic area where the surveillance device was used or, if the application was denied, the proposed location for such usage;
- (6) Whether monitoring software or applications were installed on any communications device during the use of the surveillance device and, if so, whether any of the devices on which they were installed were target devices;
- (7) The duration of the surveillance warrant, including any extensions granted, or, if the application was denied, the proposed duration; and
- (8) The number of communications devices from which data was obtained.
- 3. On or before June 30 of each calendar year, the Attorney General shall submit to the Director of the Legislative Counsel Bureau for transmittal to the Legislature if the Legislature is in session, or to the Legislative Commission, if the Legislature is not in session, a full and complete report concerning the number of applications for a surveillance warrant filed pursuant to subsection 2 of section 9 of this act, the number of times access to content, data or location information was obtained without a surveillance warrant pursuant to subsection 3 of section 9 of this act and the number of surveillance warrants granted and denied pursuant to section 9 of this act during the preceding calendar year.
 - 4. The report submitted pursuant to subsection 3 must:
- (a) Include a summary and analysis of the data required to be filed with the Attorney General pursuant to subsections 1 and 2.
- (b) Be made publicly available on the Internet website of the Attorney General.
- 5. If the Attorney General determines that a law enforcement officer violated any provision of sections 3 to 21, inclusive, of this act and the circumstances surrounding the violation raise serious questions about whether the violation was intentional, the





Attorney General shall initiate a proceeding to determine whether disciplinary action is warranted. If the Attorney General determines disciplinary action is not warranted, the reasons for such determination, including a summary of the incident and the reasons for declining disciplinary action, must be included in the report submitted pursuant to subsection 3.

6. If a court assesses punitive damages pursuant to section 21 of this act for intentional conduct, the Attorney General shall include such damages in the report submitted pursuant to subsection 3.

7. The Attorney General may adopt regulations regarding the form and content of the reports required pursuant to this section.

Sec. 21. 1. Any person whose data is knowingly obtained, accessed, used, transmitted, copied, disclosed or retained in violation of sections 3 to 21, inclusive, of this act may commence a civil action to recover from the person or entity that engaged in the violation.

- 2. In a civil action commenced pursuant to subsection 1, the court may assess the sum of the actual damages suffered by the plaintiff. In no case shall a person whose data is knowingly obtained, accessed, used, transmitted, copied, disclosed or retained in violation of sections 3 to 21, inclusive, of this act receive damages of less than \$1,000. If the violation is intentional, the court may assess punitive damages.
- 3. In a civil action commenced pursuant to subsection 1, appropriate relief may include:
- (a) Such preliminary and other equitable or declaratory relief as is appropriate;
 - (b) Damages as described in subsection 2; and
 - (c) Reasonable attorney's fees and costs.

Sec. 22. NRS 179.410 is hereby amended to read as follows:

179.410 As used in NRS 179.410 to 179.515, inclusive, *and section 2 of this act*, except where the context otherwise requires, the words and terms defined in NRS 179.415 to 179.455, inclusive, have the meanings ascribed to them in those sections.

Sec. 23. NRS 179.530 is hereby amended to read as follows:

179.530 1. District courts of this state may issue orders authorizing the use of a pen register or trap and trace device upon the application of a district attorney, 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. §§ 3121-3127 as those provisions existed on July 1, 1989.

- 2. [As used in this section, "peace officer" means:
- (a) Sheriffs of counties and metropolitan police departments and their deputies;





- 1 (b) Personnel of the Department of Public Safety who have the 2 powers of peace officers pursuant to NRS 289.270; 3
 - (c) Police officers of cities and towns;

4

5 6

7

8

9

10

11 12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27 28

29

30 31

32 33

34 35

36

37

38 39

40 41

42

43

- (d) Agents of the Nevada Gaming Control Board who are investigating any violation of subsection 2 or 3 of NRS 463.360 or chapter 465 of NRS;
- (e) Special investigators employed by the Attorney General who have the powers of peace officers pursuant to NRS 289.170;
- (f) Investigators employed by a district attorney who have the powers of peace officers pursuant to NRS 289.170; and
- (g) The Inspector General of the Department of Corrections and the criminal investigators employed by the Department who have the powers of peace officers pursuant to NRS 289.220.
- 3.] A public utility that relies, in good faith, upon an order of a district court authorizing the use of a pen register or trap and trace device is not liable in any civil or criminal action brought against the public utility for the use of the pen register or trap and trace device in accordance with the order of the court.
- 3. A surveillance device configured as a pen register or trap and trace device, as applicable, is governed by sections 3 to 21, inclusive, of this act.
 - 4. As used in this section:
 - (a) "Peace officer" means:
- (1) Sheriffs metropolitan police of counties and departments and their deputies;
- (2) Personnel of the Department of Public Safety who have the powers of peace officers pursuant to NRS 289.270;
 - (3) Police officers of cities and towns;
- (4) Agents of the Nevada Gaming Control Board who are investigating any violation of subsection 2 or 3 of NRS 463.360 or chapter 465 of NRS;
- (5) Special investigators employed by the Attorney General who have the powers of peace officers pursuant to NRS 289.170;
- (6) Investigators employed by a district attorney who have the powers of peace officers pursuant to NRS 289.170; and
- (7) The Inspector General of the Department of Corrections and the criminal investigators employed by the Department who have the powers of peace officers pursuant to NRS 289.220.
- (b) "Surveillance device" has the meaning ascribed to it in section 7 of this act.
- **Sec. 24.** The provisions of subsection 1 of NRS 218D.380 do not apply to any provision of this act which adds or revises a requirement to submit a report to the Legislature.





1 **Sec. 25.** This act becomes effective upon passage and 2 approval.





