SECOND REGULAR SESSION

SENATE BILL NO. 811

98TH GENERAL ASSEMBLY

INTRODUCED BY SENATOR KRAUS.

Pre-filed December 14, 2015, and ordered printed.

4749S.01I

ADRIANE D. CROUSE, Secretary.

AN ACT

To repeal sections 542.400, 542.406, 542.410, 542.412, 542.414, 542.416, 542.418, 542.420, RSMo, section 542.402 as enacted by senate bill no. 491, ninety-seventh general assembly, second regular session, and section 542.402 as enacted by senate bill no. 712, ninety-first general assembly, second regular session, and to enact in lieu thereof ten new sections relating to the authority to engage in certain investigative practices, with penalty provisions.

Be it enacted by the General Assembly of the State of Missouri, as follows:

Section A. Section 542.400, 542.406, 542.410, 542.412, 542.414, 542.416,

- 2 542.418, 542.420, RSMo, section 542.402 as enacted by senate bill no. 491, ninety-
- 3 seventh general assembly, second regular session, and section 542.402 as enacted
- 4 by senate bill no. 712, ninety-first general assembly, second regular session, are
- 5 repealed and ten new sections enacted in lieu thereof, to be known as sections
- $6\quad 542.400,\ 542.402,\ 542.405,\ 542.406,\ 542.410,\ 542.412,\ 542.414,\ 542.416,\ 542.418,$
- 7 542.420, to read as follows:

542.400. As used in sections 542.400 to 542.422, the following words and

- 2 phrases mean:
- 3 (1) "Aggrieved person", a person who was a party to any intercepted wire
- 4 communication or a person against whom the interception was directed;
- 5 (2) "Cell site simulator device", an international mobile
- 6 subscriber identity catcher or other device that mimics a cell phone
- tower and sends out signals to cause communications devices in the
- B area to transmit their locations, identifying information of the
- 9 subscriber or customer of a communication common carrier, or the
- 10 contents of any communication, data, or metadata sent or received by

14

15

16

26

2728

29

30

31 32

33

- 11 or stored on a communications device;
- 12 **(3)** "Communication common carrier", an individual or corporation 13 undertaking to transport messages for compensation;
 - (4) "Communications device", any device that transmits or receives radio waves, and is capable of sending or receiving communications, including cell phones, aircards, tablets, and laptops;
- [(3)] (5) "Contents", when used with respect to any wire communication, includes any information concerning the identity of the parties, the substance, purport, or meaning of that communication;
- [(4)] (6) "Court of competent jurisdiction", any circuit court having general criminal jurisdiction within the territorial jurisdiction where the communication is to be intercepted including any circuit judge specially assigned by the supreme court of Missouri pursuant to section 542.404;
- [(5)] (7) "Electronic, mechanical, or other device", any device or apparatus which can be used to intercept a wire communication other than:
 - (a) Any telephone or telegraph instrument, equipment or facility, or any component thereof, owned by the user or furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or being used by a communications common carrier in the ordinary course of its business or by an investigative office or law enforcement officer in the ordinary course of his duties; or
 - (b) A hearing aid or similar device being used to correct subnormal hearing to not better than normal;
- [(6)] (8) "Intercept", the aural acquisition of the contents of any wire communication through the use of any electronic or mechanical device, including but not limited to interception by one spouse of another spouse;
- [(7)] (9) "Investigative officer" or "law enforcement officer or agency", any officer or agency of this state or a political subdivision of this state, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in sections 542.400 to 542.422, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;
- [(8)] (10) "Oral communication", any communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;
- 46 [(9)] (11) "Person", any employee, or agent of this state or political

subdivision of this state, and any individual, partnership, association, joint stockcompany, trust, or corporation;

- 49 [(10)] (12) "Prosecuting attorney", the elected prosecuting attorney of the 50 county or the circuit attorney of any city not contained within a county;
- 51 [(11)] (13) "State", the state of Missouri and political subdivisions of the 52 state;
- [(12)] (14) "Wire communication", any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception including the use of such connection in a switching station furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of local, state or interstate communications.
 - 542.402. 1. Except as otherwise specifically provided in sections 542.400 to 542.422, a person is guilty of a class E felony and upon conviction shall be punished as provided by law, if such person:
- 4 (1) Knowingly intercepts, endeavors to intercept, or procures any other 5 person to intercept or endeavor to intercept, any wire communication;
- 6 (2) Knowingly uses, endeavors to use, or procures any other person to use 7 or endeavor to use any electronic, mechanical, or other device to intercept any 8 oral communication when such device transmits communications by radio or 9 interferes with the transmission of such communication; provided, however, that 10 nothing in sections 542.400 to 542.422 shall be construed to prohibit the use by 11 law enforcement officers of body microphones and transmitters in undercover 12 investigations for the acquisition of evidence and the protection of law 13 enforcement officers and others working under their direction in such 14 investigations;
- 15 (3) Knowingly discloses, or endeavors to disclose, to any other person the 16 contents of any wire communication, when he knows or has reason to know that 17 the information was obtained through the interception of a wire communication 18 in violation of this subsection; [or]
- 19 (4) Knowingly uses, or endeavors to use, the contents of any wire 20 communication, when he knows or has reason to know that the information was 21 obtained through the interception of a wire communication in violation of this 22 subsection; or

23

(5) Knowingly installs or uses a cell site simulator device in

30

31

32

33

3435

36

37

38 39

40

41

3

violation of sections 542.400 to 542.422 to obtain information from a communications device, including the location of the communications device, identifying information of the subscriber or customer of a communication common carrier, or the contents of any communication, data, or metadata sent or received by or stored on the communications device.

- 2. It is not unlawful under the provisions of sections 542.400 to 542.422:
- (1) For an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication, however, communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks;
- (2) For a person acting under law to intercept a wire or oral communication, where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception;
- 42 (3) For a person not acting under law to intercept a wire communication 43 where such person is a party to the communication or where one of the parties 44 to the communication has given prior consent to such interception unless such 45 communication is intercepted for the purpose of committing any criminal or 46 tortious act.
 - 542.402. 1. Except as otherwise specifically provided in sections 542.400 to 542.422, a person is guilty of a class D felony and upon conviction shall be punished as provided by law, if such person:
- 4 (1) Knowingly intercepts, endeavors to intercept, or procures any other 5 person to intercept or endeavor to intercept, any wire communication;
- 6 (2) Knowingly uses, endeavors to use, or procures any other person to use 7 or endeavor to use any electronic, mechanical, or other device to intercept any 8 oral communication when such device transmits communications by radio or 9 interferes with the transmission of such communication; provided, however, that 10 nothing in sections 542.400 to 542.422 shall be construed to prohibit the use by 11 law enforcement officers of body microphones and transmitters in undercover 12 investigations for the acquisition of evidence and the protection of law 13 enforcement officers and others working under their direction in such

14 investigations;

23

24

26

27

28

29

30

31

32

33 34

35

36

3738

39

40

- 15 (3) Knowingly discloses, or endeavors to disclose, to any other person the 16 contents of any wire communication, when he knows or has reason to know that 17 the information was obtained through the interception of a wire communication 18 in violation of this subsection; [or]
- 19 (4) Knowingly uses, or endeavors to use, the contents of any wire 20 communication, when he knows or has reason to know that the information was 21 obtained through the interception of a wire communication in violation of this 22 subsection; or
 - (5) Knowingly installs or uses a cell site simulator device in violation of sections 542.400 to 542.422 to obtain information from a communications device, including the location of the communications device, identifying information of the subscriber or customer of a communication common carrier, or the contents of any communication, data, or metadata sent or received by or stored on the communications device.
 - 2. It is not unlawful under the provisions of sections 542.400 to 542.422:
 - (1) For an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication, however, communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks;
 - (2) For a person acting under law to intercept a wire or oral communication, where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception;
- 42 (3) For a person not acting under law to intercept a wire communication 43 where such person is a party to the communication or where one of the parties 44 to the communication has given prior consent to such interception unless such 45 communication is intercepted for the purpose of committing any criminal or 46 tortious act.
 - 542.405. 1. An appellate judge or any judge of a court having original jurisdiction of criminal offenses may issue a warrant for the use of a cell site simulator device to obtain information from a

4 communications device, including the location of the device, identifying 5 information of the subscriber or customer of a communication common 6 carrier, or the contents of any communication, data, or metadata sent 7 or received by or stored on the device. A warrant under this section 8 may be issued in the same territorial jurisdiction where the

9 investigation or the communications device, or the person who owns or

10 possesses the communications device, with respect to which the

11 warrant is sought, is located.

12

1617

18

19

20

2122

23

24

25

26

27

28

29

30

31 32

33

34

35

36 37

38

39

- 2. The order may authorize the acquisition of information obtained from a communications device that, at the time the information is acquired, is located outside the court's jurisdiction but within the state if the applicant for the warrant reasonably believes the device to be located within the jurisdiction at the time the warrant is issued.
- 3. The judge may issue the warrant only on the application of an authorized law enforcement officer. An application must be written and signed and sworn to or affirmed before the judge. The affidavit shall specify:
- (1) The identity of the person, if known, who possesses the communications device to be targeted by the cell site simulator device;
- (2) The telephone number or other unique subscriber account number identifying the wire or electronic communications service account used by the communications device to be targeted by the cell site simulator device and the identity of the person, if known, who is subscribed to that account;
- (3) The type of communications device, and the communications protocols being used by the device, to which the cell site simulator device is to be attached or used;
- (4) The geographic area that will be covered by the cell site simulator device;
- (5) All categories of metadata, data, communications, or other information to be collected by the cell site simulator device from the communications device to be targeted including, call records and geolocation information;
- (6) Whether the cell site simulator device will incidentally collect metadata, data, communications, or other information from any parties or communications devices not specified in the warrant, and if so, what

SB 811 7

45 46

47 48

49

50

51 52

53

54

56 57

58

59

66

68

69 70

- 41 categories of information, data, or metadata will be collected;
- (7) Any disruptions to access or use of a communications or 42internet access network that may be created by use of the cell site simulator device; 44
 - (8) The name, department, agency, and address of the applicant;
 - (9) The type of information sought from the communications device and how it relates to the criminal offense being investigated;
 - (10) The judicial circuit in which the communications device is reasonably expected to be located;
 - (11) The facts and circumstances that provide the applicant with probable cause to believe that:
 - (a) Criminal activity has been, is, or will be committed; and
 - (b) Acquisition of data, metadata, communications, or other information from the communications device is likely to produce evidence in a criminal investigation of the criminal activity described in paragraph (a) of this subdivision.
- 4. No order issued under this section may authorize or approve the use of a cell site simulator device for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty calendar days. The communications device may not be monitored with the cell site simulator device after the 62 expiration date without an extension of the warrant. The period of 63 extension shall be no longer than the court deems necessary to achieve 64 the purposes for which it was granted and in no event longer than thirty calendar days. Every warrant and extension thereof shall contain a provision that the authorization to use the cell site simulator device shall be executed as soon as practicable and shall terminate upon attainment of the authorized objective, or in any event in thirty calendar days.
 - 5. An order authorizing the use of a cell site simulator device shall include a provision directing that the law enforcement agency:
- 72 (1) Take all steps necessary to limit the collection of any data, metadata, communications, or other information to the target specified 7374in the warrant;
- 75 (2) Take all steps necessary to delete any data, metadata, communications, or other information collected from any party not 76 specified in the applicable warrant immediately following such

SB 811 8

80

81

82 83

84 85

86

87

88 89

90

91

95

96 97

98

99

100

101

102

103

104

105106

107

108 109

110 111

112

113

114

78 collection and shall not transmit, use, or retain such information, communications, data, or metadata for any purpose whatsoever; and 79

- (3) Delete any data, metadata, communications, or other information collected from the target specified in the warrant within thirty calendar days if there is no longer probable cause to support the belief that such data, metadata, communications, or information is evidence of a crime.
- 6. Notwithstanding any provision of this section to the contrary, a law enforcement officer may obtain data, metadata, communications, or other information from a communications device by operation of a cell site simulator device without a warrant if:
- (1) The communications device is reported stolen by the owner or possessor; or
- (2) There exists a hostage, barricade, or other emergency 92 situation in which a person unlawfully and directly threatens another 93 with death or exposes another to a substantial risk of serious physical injury and which: 94
 - (a) Is in the territorial jurisdiction of the law enforcement agency that employs the officer operating the cell site simulator device or assisting in the operation of the device; and
 - (b) To prevent death or serious physical injury, necessitates the use of the cell site simulator device before a warrant may be obtained under this section.
 - 7. An authorized law enforcement officer shall apply as soon as practicable for a warrant to obtain data, metadata, communications, or other information from a communications device under a circumstance described by subsection 6 of this section. If the judge finds that an emergency situation did not occur and declines to issue the warrant, any evidence obtained from the communications device via the unauthorized use of a cell site simulator device is not admissible in a criminal action.
 - 8. No later than the seventh calendar day after the date of the expiration of a warrant under this section, the law enforcement officer who requested the warrant shall deliver a copy of the warrant to the owner or possessor of the communications device that was subject to the order.
 - 9. Unless subsection 6 of this section or another exception to the

SB 811

120

without:

warrant requirement provided under state or federal law applies, a law enforcement officer may not obtain or use information from a cell site simulator device to assist with, participate in, provide material support or resources for, or enable or facilitate an investigation conducted by a law enforcement agency of the federal government or of another state

- 121 (1) The consent of the owner or possessor of the communications
 122 device: or
- 123 (2) A warrant obtained under this section.
 - 542.406. 1. Any investigative officer or law enforcement officer who, by 2 any means authorized by sections 542.400 to 542.422, has lawfully obtained 3 knowledge of:
 - 4 (1) The contents of any wire communication, or evidence derived 5 therefrom[,]; or
 - 6 (2) The contents of any data, metadata, communication, or other 7 information obtained from a communications device by a cell site 8 simulator device;
 - 9 may disclose such contents to another investigative officer or law enforcement 10 officer to the extent that such disclosure is necessary to the proper performance 11 of the official duties of the officer making or receiving the disclosure for 12 investigative purposes only.
 - 2. Any investigative officer or law enforcement officer who, by any means authorized by sections 542.400 to 542.422, has lawfully obtained knowledge of:
 - 15 (1) The contents of any wire or oral communication, or evidence derived therefrom[,]; or
 - 17 **(2)** The contents of any data, metadata, communication, or other 18 information from a communications device obtained by a cell site 19 simulator device, or evidence derived therefrom;
- 20 may use such contents to the extent such use is necessary to the proper 21 performance of his **or her** official duties.
- 3. Any person who has received, by any means authorized by sections 542.400 to 542.422, any information obtained with the use of a cell site simulator device or information concerning a wire communication [, or evidence derived therefrom,] intercepted in accordance with the provisions of sections 542.400 to 542.422, or evidence derived therefrom, shall disclose the contents of that communication, information obtained, or such derivative evidence

28 while giving testimony under oath or affirmation in any criminal proceeding,

- 29 including deposition in any court or in any grand jury proceeding, subject to the
- 30 rules of evidence.

17

18

19

20

- 4. No otherwise privileged wire communication intercepted **or** information obtained in accordance with, or in violation of, the provisions of sections 542.400 to 542.422 shall lose its privileged character and shall be suppressed upon motion.
- 542.410. 1. The contents of any wire communication intercepted by any means authorized by sections 542.400 to 542.422 shall be recorded on tape or wire 2 or other comparable device. The recording of the contents of any wire or oral 3 communication as required by this section shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the court issuing such order and shall be sealed under its directions. Custody of the recordings shall be wherever the court orders. The recordings shall not be destroyed except upon an order of the issuing court and in any event shall be kept for ten years. Duplicate recordings shall be made for use for disclosure pursuant to the provisions of subsections 1 and 2 of section 11 12 542.406 for investigations and discovery in accordance with applicable supreme court rules. The presence of the seal provided for by subsection 2 of this section, 13 14 or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire communication or evidence 15 16 derived therefrom under the provisions of subsection 3 of section 542.406.
 - 2. Applications made and orders granted under sections 542.400 to 542.422 shall be sealed by the court. Custody of the applications and orders shall be wherever the court directs. Such applications and orders shall be disclosed only upon a showing of good cause before a court of competent jurisdiction and shall not be destroyed except on order of the issuing or denying court, and in any event shall be kept for ten years.
- 23 3. Any violation of the provisions of this section shall be punishable as a 24 class A misdemeanor.
- 4. Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under the provisions of sections 542.400 to 542.422 or the termination of the period of an order or extensions thereof, whichever is later, the issuing or denying court shall cause to be served, on the persons named in the order or the application, and such other parties to

33

36

37

38

13

14

15 16

17

18 19

20

30 intercepted communications or whose data, metadata, communications, or

- 31 other information was collected incidentally by a cell site simulator
- 32 **device**, an inventory which shall include notice of:
 - (1) The fact of the entry of the order or the application;
- 34 (2) The date of the entry and the period of authorized, approved 35 interception or use of a cell site simulator device;
 - (3) The fact that during the period oral communications were or were not intercepted or information, data, communications, or metadata were obtained from a communications device; and
- 39 (4) The nature of said conversations, information, data, 40 communications, or metadata. The court, upon the filing of a motion, shall 41 make available to such person or his counsel for inspection and copying such 42 intercepted communications, applications and orders.
- 542.412. 1. The contents of any intercepted wire communications or data, metadata, communication, or other information obtained from a cell site simulator device, or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in federal or state court nor in any administrative proceeding unless each party, in compliance with supreme court rules relating to discovery in criminal cases, 7 hearings and proceedings, has been furnished with a copy of the court order and accompanying application under which the interception or use of the cell site simulator device was authorized or approved and a transcript of any 10 intercepted wire communication, or a copy of any data, metadata, 11 communication, or other information obtained from a cell site 12 **simulator device**, or evidence derived therefrom.
 - 2. If the defense in its request designates material or information not in the possession or control of the state, but which is, in fact, in the possession or control of other governmental personnel, the state shall use diligence and make good faith efforts to cause such materials to be made available to the defendant's counsel, and if the state's efforts are unsuccessful and such material or other governmental personnel are subject to the jurisdiction of the court, the court, upon request, shall issue suitable subpoenas or orders to cause such material or information to be made available to the state for disclosure to the defense.
 - 542.414. 1. Any aggrieved person in any trial, hearing, or proceeding in 2 or before any court, department, officer, agency, regulatory body, or other 3 authority of the United States, the state, or a political subdivision thereof, may

4 move to suppress the contents of any intercepted wire communication, or

- 5 information, data, communication, or metadata obtained from cell site
- 6 simulator device, or evidence derived therefrom, on the grounds that:
- 7 (1) The communication was unlawfully intercepted;
- 8 (2) The information, data, communication, or metadata was 9 unlawfully obtained by a cell site simulator device;
- 10 (3) The order of authorization or approval under which [it] the 11 communication was intercepted or the cell site simulator device was used 12 is insufficient on its face;
- 13 **[(3)] (4)** The interception **or use of the cell site simulator device** was 14 not made in conformity with the order of authorization or approval; or
- 15 [(4)] (5) The communication was intercepted or the cell site simulator 16 device was used in violation of the provisions of the Constitution of the United States or the state of Missouri or in violation of a state statute. Such motion 1718 shall be made before the trial, hearing, or proceeding unless there was no reasonable opportunity to make such motion or the person was not aware of the 20 existence of grounds for the motion. If the motion is granted, the contents of the intercepted wire communication, or information, data, communication, or 21metadata obtained from the cell site simulator device, or evidence derived 2223 therefrom, or the contents of any communication intercepted or information, data, communication, or metadata obtained as a result of any extension of 24the original order authorizing or approving the interception of wire 2526 communication or use of a cell site simulator device, and any evidence 27 derived therefrom, shall be treated as having been obtained in violation of 28 sections 542.400 to 542.422.
- 29 2. In addition to any other right to appeal, the state shall have the right to appeal from an order granting a motion to suppress made under subsection 1 of this section if the prosecuting attorney shall certify to the court or other official granting such motion that the appeal be taken within thirty days after the date the order was entered and shall be diligently prosecuted.
 - 542.416. 1. Within thirty days after the expiration of an order or each extension thereof entered pursuant to the provisions of **section 542.405 or** section 542.408, the issuing court shall report to the state courts administrator:
 - (1) The fact that an order or extension was applied for;
- 5 (2) The kind of order or extension applied for;

3

4

6 (3) The fact that the order or extension was granted as applied for, was

- 7 modified, or was denied;
- 8 (4) The period of interceptions or use of a cell site simulator device
- 9 authorized by the order, and the number and duration of any extensions of the
- 10 order;
- 11 (5) The offense specified in the order or application, or extension of an 12 order;
- 13 (6) The identity of the applying investigative officer or law enforcement
- 14 officer and agency making the application and the person authorizing the
- 15 application; and
- 16 (7) The nature of the facilities from which or the place where
- 17 communications were to be intercepted or the cell site simulator device was
- 18 to be used.
- 19 2. In January of each year, the principal prosecuting attorney for any
- 20 political subdivision of the state shall report to the state courts administrator:
- 21 (1) The information required by subdivisions (1) through (7) of subsection
- 22 1 of this section with respect to each application for an order or extension made
- 23 during the preceding calendar year;
- 24 (2) A general description of the interceptions made, or information
- 25 collected from a cell site simulator device, under such order or extension,
- 26 including:
- 27 (a) The approximate nature and frequency of incriminating
- 28 communications intercepted or information obtained from a cell site
- 29 simulator device;
- 30 (b) The approximate nature and frequency of other communications
- 31 intercepted or information obtained from a cell site simulator device;
- 32 (c) The approximate number of persons whose communications were
- 33 intercepted or whose information was obtained from a cell site simulator
- 34 device; and
- 35 (d) The approximate nature, amount, and cost of the manpower and other
- 36 resources used in the interceptions or use of a cell site simulator device;
- 37 (3) The number of arrests resulting from interceptions made **or the use**
- 38 of a cell site simulator device under such order or extension, and the offenses
- 39 for which arrests were made:
- 40 (4) The number of trials resulting from such interceptions or cell site
- 41 simulator device use;
- 42 (5) The number of motions to suppress made with respect to such

43 interceptions **or cell site simulator device use**, and the number granted or denied;

- 45 (6) The number of convictions resulting from such interceptions **or cell**46 **site simulator device use** and the offenses for which the convictions were
 47 obtained and a general assessment of the importance of the interceptions **or use**48 **of the device**; and
- 49 (7) The information required by subdivisions (2) through (6) of this 50 subsection with respect to orders or extensions obtained in the preceding calendar 51 year.
- 52 3. In April of each year the state courts administrator shall transmit to the Missouri general assembly a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire communications and use of cell site simulator devices and the number of 55orders and extensions granted or denied during the preceding calendar 56year. Such report shall include a summary and analysis of the data required to 57be filed with the state courts administrator by subsections 1 and 2 of this 59 section. The state courts administrator may promulgate rules and regulations dealing with the content and form of the reports required to be filed by 60 subsections 1 and 2 of this section. 61
 - 542.418. 1. The contents of any wire communication, or data, metadata, communication, or other information obtained from a cell site simulator device, or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any civil or administrative proceeding, except in civil actions brought pursuant to this section.
 - 2. Any person whose wire communication is intercepted, disclosed, or used in violation of sections 542.400 to 542.422 or whose data, metadata, communication, or other information is obtained from a cell site simulator device, disclosed, or used in violation of such sections shall:
- 10 (1) Have a civil cause of action against any person who intercepts, 11 **obtains,** discloses, or uses, or procures any other person to intercept, **obtain,** 12 disclose, or use such communications, **information, data, or metadata**; and
 - (2) Be entitled to recover from any such person:

6

9

- 14 (a) Actual damages, but not less than liquidated damages computed at the 15 rate of one hundred dollars a day for each day of violation or ten thousand dollars 16 whichever is greater;
- 17 (b) Punitive damages on a showing of a willful or intentional violation of

- 18 sections 542.400 to 542.422; and
- 19 (c) A reasonable attorney's fee and other litigation costs reasonably
- 20 incurred.
- 3. A good faith reliance on a court order or on the provisions of **section**
- 22 542.405 or section 542.408 shall constitute a prima facie defense to any civil or
- 23 criminal action brought under sections 542.400 to 542.422.
- 4. Nothing contained in this section shall limit any cause of action
- 25 available prior to August 28, 1989.
 - 542.420. Whenever any wire communication has been intercepted or cell
- 2 site simulator device has been used, no part of the contents of such
- 3 communication, or the contents of data, metadata, communications, or
- 4 information obtained from the cell site simulator device, and no evidence
- 5 derived therefrom may be received in evidence in any trial, hearing, or other
- 6 proceeding in or before any court, grand jury, department, officer, agency,
- 7 regulatory body, legislative committee, or other authority of the United States,
- 8 a state, or a political subdivision thereof if the disclosure of that information
- 9 would be in violation of sections 542.400 to 542.422.

