Cell Site Simulator Privacy Model Bill

SECTION 1. Definitions. As used in this Act:

(A) "Authorized possessor" shall mean the person in possession of a communications device when that person is the owner of the device or has been authorized to possess the device by the owner of the device.

(B) "Adverse result" shall mean:

(1) Endangering the life or physical safety of an individual;

(2) Flight from prosecution;

(3) Destruction of or tampering with evidence;

(4) Intimidation of potential witnesses; or

(5) Otherwise seriously jeopardizing an investigation.

(C) "Cell site simulator device":

(1) Shall mean a 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;

(2) Includes an international mobile subscriber identity (IMSI) catcher or other cell phone or telephone surveillance or eavesdropping device that mimics a cellular base station and transmits radio waves that cause cell phones or other communications devices in the area to transmit or receive radio waves, electronic data, location data, information used to calculate location, identifying information, communications content, or metadata, or otherwise obtains this information through passive means, such as through the use of a digital analyzer or other passive interception device;

(3) Does not include any device used or installed by an electric utility solely to the extent such device is used by that utility to measure electrical usage, to provide services to customers, or to operate the electric grid.

(D) "Communications device" shall mean any electronic device that transmits signs, signals, writings, images, sounds, or data in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

(E) "Data transmitted or received by a communications device" shall mean all dialing, routing, addressing, or signaling information, including but not limited to the device's unique numeric identifier, channel and cell site codes identifying the device's location, as well as the content of any communications.

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

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

(H) "Law enforcement official" shall mean an employee or agent of a state, county or local law enforcement agency or department, including but not limited to prosecutors.

(I) "Targeted communications device" shall mean the specific communications device as to which judicial authorization was sought and received, pursuant to this Act, to use a cell site simulator device to obtain data.

(J) "Targeted party" shall mean a person or entity as to which judicial authorization was sought and received, pursuant to this Act, to obtain data using a cell site simulator device.

SECTION 2. Warrant Required for Use of Cell Site Simulator Device.

(A) Subject to the requirements of this Act and all applicable provisions of the United States Constitution and the constitution and laws of this state, no state, county, or local agency, department, authority, or other entity, including any agents and employees thereof, shall use a cell site simulator device to obtain any data transmitted or received by a communications device or stored on a communications device without a warrant based on probable cause and issued pursuant to this Act.

(B) No employee or agent of the state or any county or local government, other than a law enforcement official who is specifically trained and authorized to do so pursuant this Act, may operate a cell site simulator device.

(C) A cell site simulator device may not be used to install monitoring software or applications on a communications device, unless:

(1) Authorization to do so is sought and received pursuant to Sections 3 and 4;

(2) All requirements and limitations that apply to cell site simulator devices under to this Act are applied to the installed monitoring software or application, including but not limited to restrictions on duration; and

(3) The installation and use of the monitoring software or applications conforms with all applicable provisions of the United States Constitution and the constitution and laws of this state, including but not limited to [insert citation to your state law governing the issuance of wiretaps].

(D) Any use of a cell site simulator device by a law enforcement official or other employee or agent of a state, county, or local government entity not authorized by a warrant pursuant

to Section 4, or subject to the provisions of Section 5, shall constitute a violation of this Act.

(E) Nothing in this Act shall be construed to authorize or allow any surveillance act or operation that is otherwise prohibited by law.

SECTION 3. Applications for the Use of Cell Site Simulator Devices.

(A) An application for a warrant authorizing the use of a cell site simulator device shall be made under oath.

(B) An application under this Section shall comply with all applicable laws regarding search warrants in this state, and shall certify that:

(1) There is probable cause to believe that the use of a cell site simulator device will lead to:

(a) Obtaining evidence of a crime, contraband, fruits of crime, things criminally possessed, weapons, or other things by means of which a crime has been committed, is being committed, or is about to be committed; or

(b) The location of a person whom there is probable cause to believe has committed, is committing, or is about to commit a crime;

(2) The law enforcement applicant will comply with the requirements of Section 6; and

(3) All relevant law enforcement agencies are in compliance with Sections 6 and 9 of this Act.

(C) An application under this Section shall identify the law enforcement official making the application, the law enforcement agency or department conducting the investigation, the law enforcement agency in possession of the cell site simulator device to be used, the law enforcement agency that owns the cell site simulator device, and the law enforcement official(s) who will operate it.

(D) An application under this Section shall specify sufficient facts:

(1) To demonstrate that alternative methods of investigation and surveillance with less incidental impact on non-targeted parties and devices are inadequate to achieve the same purposes; and

(2) For a court to make the findings necessary under Section 4.

(E) An application under this Section shall include:

(1) The technological nature and capabilities of the cell site simulator device to be used, as well as the manner of its operation, methods of deployment, and the techniques to be employed in the instant case;

(2) The likely impact on privacy and communications services of non-targeted parties of the proposed deployment, including the geographical area(s) in which the cell site simulator device will be deployed, the estimated number of non-targeted parties likely to be impacted by the proposed deployment, and whether signals will be sent into private spaces;

(3) The applying agency's or department's procedures for compliance with the requirements of Section 6;

(4) The qualifications, training, and agency affiliation of the person(s) who will operate the cell site simulator device; and

(5) All information required to be included in the warrant by Section 4(D).

SECTION 4. Warrants Authorizing the Use of Cell Site Simulator Devices.

(A) A court may authorize the use of a cell site simulator device only upon receipt of a valid application pursuant to Section 3. If the application seeks authority to use a cell site simulator device to intercept the contents of communications, authorization may be granted only in compliance with the procedural and substantive limitations on wiretaps contained in state and federal law, and consistent with constitutional limits on wiretapping.

(B) A court shall not authorize the use of a cell site simulator device for any purpose other than obtaining data.

(C) A warrant under this Section shall comply with all applicable laws regarding search warrants in this state, and shall only issue if the court finds that:

(1) There is probable cause to believe that the use of a cell site simulator device will lead to:

(a) Obtaining evidence of a crime, contraband, fruits of crime, things criminally possessed, weapons, or other things by means of which a crime has been committed, is being committed, or is about to be committed; or

(b) The location of a person whom there is probable cause to believe has committed, is committing, or is about to commit a crime; and

(2) Alternative methods of investigation and surveillance with less incidental impact on non-targeted parties and devices are inadequate to achieve the same purposes.

(D) A warrant under this Section authorizing the use of a cell site simulator device must specify:

(1) The manner in which the cell site simulator device will be used, including whether it will be deployed aerially or through another method;

(2) The identities, if known, of:

(a) The person(s) who own the targeted communications device;

(b) The person(s) who possess the targeted communications device; and

(c) The person(s) who are the subject of the criminal investigation;

(3) The telephone number, electronic serial number, or other unique identifier of the targeted communications device, except when such information is unknown and the cell site simulator device is authorized for the purpose of identifying the targeted communications device;

(4) If known, the physical location of the targeted communications device;

(5) The type of communications device being targeted, and the communications protocols being used by the targeted communications device;

(6) The geographic area(s) where the cell site simulator device will be operated, and where any signals emitted by the device will extend;

(7) All specific types of data that there is probable cause to obtain from or about the targeted communications device through use of a cell site simulator device including, but not limited to, device electronic serial numbers, communications metadata, communications content, or geolocation information;

(8) Whether or not the cell site simulator device will incidentally obtain data from any non-targeted communications devices, and if so, what types of data will be obtained and a reasonable estimate of the number of communications devices from which such data will be obtained;

(9) Whether any disruptions to access or use of an electronic communications service may be caused by use of the cell site simulator device, including to non-targeted parties or communications devices, and a reasonable estimate of the number of communications devices that may experience such disruption; and

(10) The offense to which the information likely to be obtained relates.

(E) Unless the court finds that doing so is necessary and consistent with the requirements of Section 6, a cell site simulator device shall not be deployed using aircraft.

(F) A warrant issued under this Section shall authorize the use of a cell site simulator device for a period not to exceed 14 days, and shall immediately terminate when the data authorized in the warrant is obtained.

(G) An extension of such a warrant may be granted, for a period not to exceed 14 days, only upon a new application under Section 3 and a new warrant under this Section. An application for an extension shall include a certification of good faith belief that the information sought is more likely to be to be obtained under the extension period than under any previous period of authorization, including any prior extensions.

(H) A court shall not authorize the access, use, transmission, copying, disclosure, or retention of any data obtained by a cell site simulator device that was neither specifically authorized to be obtained by a warrant under this Section at the time such data was

obtained nor validly obtained pursuant to Section 5 and specifically authorized by a timely warrant pursuant to Section 5(B).

(I) Nothing in this Act shall be construed to authorize the use of a cell site simulator device to obtain data regarding the targeted communications device from any device not targeted in the warrant pursuant to this Section.

(J) The foreseeability of incidental acquisition of data not specifically authorized to be obtained shall not be construed as authorization to obtain, access, use, transmit, copy, disclose, or retain the information.

(K) A warrant issued pursuant to this Section may be sealed upon a showing of need, but for no more than 180 days, with any further extensions to be granted upon a certification that an investigation remains active or a showing of exceptional circumstances.

SECTION 5. Emergency Exceptions.

(A) Notwithstanding any other provision of this Act, a law enforcement official specially designated by the Attorney General, or a law enforcement official specially designated by the principal prosecuting attorney of the jurisdiction, may use a cell site simulator device to obtain data if the law enforcement official and the Attorney General or principal prosecuting attorney reasonably determine that:

(1) An emergency situation requiring the use of a cell site simulator device exists;

(2) The emergency situation requires use of a cell site simulator device before a warrant authorizing such use can, with due diligence, be sought and issued;

(3) A judicially recognized exception to warrant requirements applies;

(4) Alternative methods of investigation and surveillance with less incidental impact on non-targeted parties and devices are inadequate to achieve the same purposes; and

(5) There are grounds upon which a warrant could be sought pursuant to Section 3 and issued pursuant to Section 4.

(B) The law enforcement official using a cell site simulator device under this Section must apply for and obtain a warrant under Sections 3 and 4 within 48 hours of beginning to use such device. A warrant pursuant to this Section must contain, in addition to the requirements of Section 4, findings that the requisite determinations were made by the appropriate persons under Section 5(A) and were reasonable at the time.

(C) In the absence of a warrant under Section 4, any use of a cell site simulator device under this section shall terminate immediately when:

(1) The data sought is obtained;

(2) The application under Section 3 is denied; or

(3) 48 hours have elapsed since the commencement of the cell site simulator device's use.

(D) The knowing use of a cell site simulator device pursuant to this Section without submitting an application for an authorizing warrant within 48 hours of the commencement of the device's use shall constitute a violation of this Act.

(E) A cell site simulator device shall not be used pursuant to this Section on the basis of an outstanding warrant for the search or seizure of any persons, places, or things.

SECTION 6. Restrictions on Use of Cell Site Simulator Devices and Data.

(A) With respect to non-targeted parties and devices, a law enforcement agency or department using a cell site simulator device must take all reasonable steps to minimize:

(1) The number of adversely affected parties and devices;

(2) The degree of the adverse impacts, including, but not limited to, adverse impacts on privacy, communications services, and device functionality; and

(3) The data obtained.

(B) With respect to targeted parties and devices, a law enforcement agency or department using a cell site simulator device must take all reasonable steps to minimize the unauthorized data obtained.

(C) Deletion Requirements

(1) If the cell site simulator device is used to locate, track, or obtain data from a communications device, all data obtained without authorization must be permanently deleted as soon as reasonably possible and not later than the end of the day on which it was obtained.

(2) Notwithstanding the requirements of Section 6(C)(1), if the cell site simulator device is used to identify an unknown communications device, such data necessary to the identification process but relating to non-target communications devices must be permanently deleted not later than the earlier of the end of the day on which the unknown communications device is identified or seven days after the commencement of the cell site simulator device's use.

(3) Any data obtained pursuant to Section 5 that is not specifically authorized by a timely issued warrant pursuant to Section 5(B) shall be permanently deleted as soon as reasonably possible and not later than the day on which use of a cell site simulator device is required to terminate under Section 5(C).

(4) Any data obtained by an authorized cell site simulator device shall be permanently deleted when the probable cause identified for purposes of Section 4(C)(3) no longer exists, except to the extent that retention of that data is justified or required by rules or caselaw governing disclosure of exculpatory or material evidence to the defense in a criminal case. Any data required to be retained by

such rules or caselaw shall be segregated from law enforcement investigative files and shall not be accessed for any purpose other than as required by such rules or caselaw.

(D) Data required to be deleted under this Section shall not be accessed, used, transmitted, copied, disclosed, or retained for any purpose prior to deletion, except as provided in Section 6(C)(4).

(E) Knowingly accessing, using, transmitting, copying, disclosing, or retaining unauthorized data obtained by a cell site simulator device shall constitute a violation of this Act.

SECTION 7. Notice.

(A) Unless delayed notice is ordered under Section 7(B), not later than 3 days after a law enforcement official deploys a cell site simulator device under this Act, the law enforcement official, or another law enforcement official acting as an agent thereof, shall serve upon or deliver by registered or first-class mail, electronic mail, or other reasonable means approved by the court issuing the warrant to the authorized possessor of the targeted communications device:

(1) A copy of the application and warrant; and

(2) Notice that informs the authorized possessor of the targeted communications device:

(a) Of the nature of the law enforcement inquiry with reasonable specificity;

(b) That content or data stored or transmitted by the device and/or location information was obtained by the law enforcement official, the date on which it was obtained, and whether it has been deleted, including the date of such deletion;

(c) Whether notification of the authorized possessor was delayed pursuant to Section 7(B); and

(d) If applicable, what court approved the Section 7(B) application for delayed notification and the reason delayed notification was approved.

(B) A law enforcement official applying for use of a cell site simulator device under Section 3 may include in the application a request to delay the notification required under Section 7(A) for a period not to exceed 90 days. The court shall grant such a delay if it determines that notification of the existence of the warrant is likely to have an adverse result.

(C) Upon expiration of the period of delay granted under Section 7(B), the law enforcement official shall provide the authorized possessor of the targeted communications device with a copy of the Section 7(B) application and warrant, together with notice required pursuant to Section 7(A).

(D) The court may, upon application, grant one or more extensions of delayed notification granted under Section 7(B) for an additional 90 days each.

SECTION 8. Suppression.

(A) Except as proof of a violation of this Act, no data obtained, accessed, used, transmitted, copied, disclosed, or retained in violation of this Act, nor any evidence derived therefrom, shall be admissible in any criminal, civil, administrative, or other proceeding.

(B) Any data obtained pursuant to this Act or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the warrant, and accompanying application, under which the information was obtained. This ten-day period may be waived by the court if the court finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

SECTION 9. Training.

(A) The Attorney General shall develop training protocols for law enforcement officials involved in the authorization, deployment, and technical operation of cell site simulator devices, which must include training on privacy and civil liberties.

(B) Law enforcement agencies or departments using cell site simulator devices shall conduct appropriate trainings based on these protocols for all law enforcement officials involved in the authorization, deployment, and technical operation of cell site simulator devices.

(C) Cell site simulator devices may only be operated by law enforcement officials who have been authorized by their agency or department to operate the technology and who have received the training required pursuant to this Section.

SECTION 10. Reporting Requirements.

(A) By March 15 of each calendar year, any court issuing or denying a warrant under Sections 4 or 5 of the Act during the preceding calendar year shall report to the Attorney General:

(1) The number of warrants applied for.

(2) Separately, the number of applications that were:

(a) Denied;

(b) Modified; and

(c) Granted.

(3) The number of warrants granted whose total duration, including extensions, was:

(a) 0-14 days;

(b) 15-28 days;

(c) 29-42 days; and

(d) 43 days or greater.

(B) By March 15 of each calendar year, any agency or department using a cell site simulator device during the preceding calendar year shall report to the Attorney General:

(1) The number of warrants applied for.

(2) Separately, the number of warrant applications that were:

(a) Denied;

(b) Modified; and

(c) Granted.

(3) With respect to each cell site simulator device warrant application or deployment:

(a) Whether the application was granted, modified or denied;

(b) The offense(s) specified in the warrant application;

(c) The purpose(s) for which for the cell site simulator device was used or, if the application was denied, the proposed purpose(s);

(d) Whether the initial use of the cell site simulator device was (1) pursuant to Section 4; (2) pursuant to Section 5; (3) unauthorized by this Act; or (4) the device was never used;

(e) The geographic area(s) where the cell site simulator device was used or, if the application was denied, the proposed location(s);

(f) Whether monitoring software or applications were installed on any communications device(s) during the cell site simulator devices' use and, if so, whether none, some or all of the device(s) on which they were installed were targeted communications devices;

(g) The duration of the warrant, including any extensions granted, under which the cell site simulator device was used or, if the application was denied, the proposed duration; and

(h) The number of communications devices from which data was obtained.

(C) Information provided to the Attorney General pursuant to Section 10(A) and (B) shall be subject to [insert citation to your state's open records law].

(D) On or before June 30th of each year, beginning in the year after this bill is enacted, the Attorney General shall transmit to the legislature a full and complete report concerning the number of applications pursuant to Section 3 of this Act, the number of times access

to content, data or location information was obtained pursuant to Section 5 of this Act, and the number of warrants granted or denied pursuant to Section 4 of this Act during the preceding calendar year.

(1) Such report shall include a summary and analysis of the data required to be filed with the Attorney General by Section 10(A) and (B).

(2) A copy of such the report required by Section 10(D) shall be made publicly available on the website for the Attorney General.

(3) The Attorney General is authorized to issue binding regulations regarding the content and form of the reports required to be filed pursuant to Section 10(A) and (B).

SECTION 11. Enforcement.

(A) Any person whose data is obtained, accessed, used, transmitted, copied, disclosed, or retained by any knowing violation of this Act, or on whose communications device software or applications are installed in violation of Section 2(C), may, in a civil action, recover from the person or entity that engaged in the violation such relief as may be appropriate.

(1) In a civil action under this Section, appropriate relief may include:

(a) Such preliminary and other equitable or declaratory relief as is appropriate;

(b) Damages under Section 11(A)(2); and

(c) Reasonable attorney's fees and other litigation costs.

(2) The court may assess as damages in a civil action under this Section the sum of the actual damages suffered by the plaintiff, but in no case shall a person whose data is obtained, accessed, used, transmitted, copied, disclosed, or retained by any knowing violation of this Act, or on whose communications device software or applications are installed in violation of Section 2(C), receive less than minimum statutory damages of $1,000. If the violation is intentional, the court may assess punitive damages.

(B) If a court or the Attorney General determines that a state, county, or local agency, department, authority, or other entity, including any agent, employee, or law enforcement official thereof (1) has violated any provision of this Act, and (2) that 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, shall be included in the next report issued pursuant to Section 10(C).

SECTION 12. Severability.

The provisions in this Act are severable. If any part or provision of this Act, or the application of this Act to any person, entity, or circumstance, is held invalid, the remainder of this Act, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.

SECTION 13. Effective Date.

This Act shall take effect upon passage.