MISSISSIPPI LEGISLATURE REGULAR SESSION 2018

By: Representative Bomgar

To: Judiciary B

HOUSE BILL NO. 1092

AN ACT TO PROHIBIT LAW ENFORCEMENT OFFICIALS FROM USING CELL SITE SIMULATOR DEVICES TO INTERCEPT DATA FROM COMMUNICATIONS DEVICES WITHOUT A PROBABLE CAUSE WARRANT; TO DEFINE CERTAIN TERMS; TO PRESCRIBE THE REQUIREMENTS FOR AN APPLICATION FOR A WARRANT TO USE A CELL SITE SIMULATOR DEVICE AND THE CONDITIONS UNDER WHICH A COURT MAY ISSUE A WARRANT AUTHORIZING USE OF THE DEVICE; TO AUTHORIZE THE WARRANTLESS USE OF A CELL SITE SIMULATOR DEVICE IN EMERGENCY SITUATIONS; TO REQUIRE A LAW ENFORCEMENT AGENCY USING A CELL SITE SIMULATOR DEVICE TO TAKE STEPS TO LIMIT OBTAINING UNAUTHORIZED DATA; TO REQUIRE NOTICE TO BE GIVEN TO THE OWNER OF A TARGETED COMMUNICATIONS DEVICE; TO PROVIDE THAT DATA OBTAINED IN VIOLATION OF THIS ACT IS INADMISSIBLE; TO REQUIRE THE ATTORNEY GENERAL TO DEVELOP TRAINING PROTOCOLS ON THE USE OF CELL SITE SIMULATOR DEVICES AND TO REPORT TO THE LEGISLATURE ON THEIR USAGE; TO REQUIRE COURTS TO ANNUALLY SUBMIT DATA RELATING TO THE USE OF CELL SITE SIMULATOR DEVICES TO THE ATTORNEY GENERAL; TO AUTHORIZE CIVIL PENALTIES FOR PERSONS WHO ARE THE VICTIMS OF THE UNLAWFUL USE BY LAW ENFORCEMENT OF A CELL SITE SIMULATOR DEVICE; TO PROHIBIT PUBLIC AGENCIES AND EMPLOYEES FROM USING LICENSE PLATE SCANNERS ON PUBLIC HIGHWAYS; TO CREATE EXCEPTIONS FOR CERTAIN PUBLIC AGENCIES ENGAGED IN PLANNING AND ENFORCEMENT OF HIGHWAY WEIGHT RESTRICTIONS; TO PROHIBIT PUBLIC EMPLOYEES FROM ADMINISTERING ORAL FLUID TESTS FOR THE PURPOSE OF DETERMINING IF AN INDIVIDUAL IS UNDER THE INFLUENCE OF CONTROLLED SUBSTANCES; AND FOR RELATED PURPOSES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MISSISSIPPI:

SECTION 1. As used in Sections 1 through 12 of this act, the following words and phrases have the meanings ascribed in this section unless the context clearly indicates otherwise:

(a) "Authorized possessor" means 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" means:

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

(ii) Flight from prosecution;

(iii) Destruction of or tampering with evidence;

(iv) Intimidation of potential witnesses; or

(v) Otherwise seriously jeopardizing an investigation.

(c) "Cell site simulator device" means 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. "Cell site simulator device" 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. "Cell site simulator device" does not include any device used or installed by an electric utility solely to the extent the device is used by that utility to measure electrical usage, to provide services to customers or to operate the electric grid.

(d) "Communications device" means 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" means 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" means 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" means 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" means 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" means the specific communications device as to which judicial authorization was sought and received, pursuant to Sections 1 through 12 of this act, to use a cell site simulator device to obtain data.

(j) "Targeted party" means a person or entity as to which judicial authorization was sought and received, pursuant to Sections 1 through 12 of this act, to obtain data using a cell site simulator device.

SECTION 2. (1) Subject to the requirements of Sections 1 through 12 of this act and all applicable provisions of the United States Constitution and the constitution and laws of the State of Mississippi, no state, county, municipal or other local governing agency, department, authority or other entity, including agents and employees, may 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 Sections 1 through 12 of this act.

(2) No employee or agent of the state or any county, municipal or other local governing authority, other than a law enforcement official who is trained and authorized specifically to do so pursuant to Sections 1 through 12 of this act, may operate a cell site simulator device.

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

(a) Authorization to do so is sought and received pursuant to Sections 3 and 4 of this act;

(b) All requirements and limitations that apply to cell site simulator devices under Sections 1 through 12 of this act are applied to the installed monitoring software or application, including, but not limited to, restrictions on duration; and

(c) 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, Article 7, Chapter 29, Title 41, Mississippi Code of 1972.

(4) Any use of a cell site simulator device by a law enforcement official or other employee or agent of a state, county, municipal or other local governing authority not authorized by a warrant pursuant to Section 4 of this act or subject to the provisions of Section 5 of this act constitutes a violation of Sections 1 through 12 of this act.

(5) This act may not be construed to authorize or allow any surveillance act or operation that otherwise is prohibited by law.

SECTION 3. (1) An application for a warrant authorizing the use of a cell site simulator device must be made under oath.

(2) An application under this section must comply with all applicable laws regarding search warrants in this state and must certify that:

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

(i) 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

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

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

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

(3) An application under this section must 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 or officials who will operate it.

(4) An application under this section must specify sufficient facts:

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

(b) For a court to make the findings necessary under Section 4 of this act.

(5) An application under this section must include:

(a) 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;

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

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

(d) The qualifications, training and agency affiliation of the persons who will operate the cell site simulator device; and

(e) All information required to be included in the warrant under subsection (4) of Section 4 of this act.

SECTION 4. (1) 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.

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

(3) A warrant under this section must comply with all applicable laws regarding search warrants in this state and may only be issued if the court finds that:

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

(i) 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

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

(b) Alternative methods of investigation and surveillance with less incidental impact on nontargeted parties and devices are inadequate to achieve the same purposes.

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

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

(b) The identities, if known, of:

(i) The person who owns the targeted communications device;

(ii) The person who possesses the targeted communications device; and

(iii) The person who is the subject of the criminal investigation;

(c) 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;

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

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

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

(g) All specific types of data which 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;

(h) Whether or not the cell site simulator device incidentally will obtain data from any nontargeted 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;

(i) 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 nontargeted parties or communications devices, and a reasonable estimate of the number of communications devices that may experience such disruption; and

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

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

(6) A warrant issued under this section may not authorize the use of a cell site simulator device for a period exceeding fourteen (14) days, and the warrant will terminate immediately when the data authorized in the warrant is obtained.

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

(8) A court may not authorize the access, use, transmission, copying, disclosure or retention of any data obtained by a cell site simulator device which was neither specifically authorized to be obtained by a warrant under this section at the time the data was obtained nor validly obtained pursuant to Section 5 and specifically authorized by a timely warrant pursuant to subsection (2) of Section 5.

(9) This act may not 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.

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

(11) A warrant issued pursuant to this section may be sealed upon a showing of need, but for not more than one hundred eighty (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. (1) Notwithstanding any other provision of Sections 1 through 12 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:

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

(b) 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;

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

(d) Alternative methods of investigation and surveillance with less incidental impact on nontargeted parties and devices are inadequate to achieve the same purposes; and

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

(2) 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 forty-eight (48) hours of beginning

to use the 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 subsection (1) and were reasonable at the time.

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

(a) The data sought is obtained;

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

(c) Forty-eight (48) hours have elapsed since the commencement of the cell site simulator device's use.

(4) The knowing use of a cell site simulator device pursuant to this section without submitting an application for an authorizing warrant within forty-eight (48) hours of the commencement of the device's use constitutes a violation of this act.

(5) A cell site simulator device may 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. (1) With respect to nontargeted parties and devices, a law enforcement agency or department using a cell site simulator device must take all reasonable steps to minimize:

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

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

(c) The data obtained.

(2) 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.

(3) (a) 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 deleted permanently as soon as reasonably possible and in no event, later than the end of the day on which it was obtained.

(b) Notwithstanding the requirements of paragraph (a), if the cell site simulator device is used to identify an unknown communications device, the data necessary to the identification process but relating to nontarget communications devices must be deleted permanently no later than: the earlier of the end of the day on which the unknown communications device is identified; or seven (7) days after the commencement of the cell site simulator device's use.

(c) Any data obtained pursuant to Section 5 which is not specifically authorized by a timely issued warrant pursuant to subsection (2) of this section must be deleted permanently as soon as reasonably possible and in no event, later than the day on

which use of a cell site simulator device is required to terminate under subsection (3) of Section 5.

(d) Any data obtained by an authorized cell site simulator device must be deleted permanently when the probable cause identified for purposes of subsection (3)(a) of Section 4 no longer exists, except to the extent that retention of that data is justified or required by rules or case law governing disclosure of exculpatory or material evidence to the defense in a criminal case. Any data required to be retained by such rules or case law must be segregated from law enforcement investigative files and may not be accessed for any purpose other than as required by the rules or case law.

(4) Data required to be deleted under this section may not be accessed, used, transmitted, copied, disclosed or retained for any purpose before its deletion, except as provided in subsection (3)(d).

(5) Knowingly accessing, using, transmitting, copying, disclosing or retaining unauthorized data obtained by a cell site simulator device constitutes a violation of Sections 1 through 12 of this act.

SECTION 7. (1) Unless delayed notice is ordered under subsection (2) of this section, not later than three (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 of the official, must

serve upon or deliver by registered or first-class mail, electronic mail or other reasonable means approved by the court issuing the warrant the following to the authorized possessor of the targeted communications device:

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

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

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

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

(iii) Whether notification of the authorized possessor was delayed pursuant to subsection (2) of this section; and

(iv) If applicable, what court approved the subsection (2) application for delayed notification and the reason delayed notification was approved.

(2) 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 subsection (1) for a period not to exceed ninety (90) days. The court must grant a delay if it determines that notification of the existence of the warrant is likely to have an adverse result.

(3) Upon expiration of the period of delay granted under subsection (2), the law enforcement official shall provide the authorized possessor of the targeted communications device with a copy of the subsection (2) application and warrant, together with notice required pursuant to subsection (1).

(4) The court, upon application, may grant one or more extensions of delayed notification granted under subsection (2) for an additional ninety (90) days each.

SECTION 8. (1) Except as proof of a violation of Sections 1 through 12 of this act, any data obtained, accessed, used, transmitted, copied, disclosed or retained in violation of this act, or any evidence derived from such data, is inadmissible in any criminal, civil, administrative or other proceeding.

(2) Any data obtained pursuant to Sections 1 through 12 of this act or evidence derived from the data may 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 (10) 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. The 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 (10) days before the trial, hearing or proceeding and that the party will not be prejudiced by the delay in receiving the information.

SECTION 9. (1) 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 protocols must include training on privacy and civil liberties.

(2) 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.

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

SECTION 10. (1) Before March 15 of each calendar year, a court issuing or denying a warrant under Sections 4 or 5 of this act during the preceding calendar year shall report to the Attorney General:

(a) The number of warrants applied for;

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

(i) Denied;

(ii) Modified; and

(iii) Granted;

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

(i) Zero (0) to fourteen (14) days;

(ii) Fifteen (15) to twenty-eight (28) days;

(iii) Twenty-nine (29) to forty-two (42) days; and

(iv) Forty-three (43) days or greater.

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

(a) The number of warrants applied for;

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

(i) Denied;

(ii) Modified; and

(iii) Granted;

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

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

(ii) The offenses specified in the warrant application;

(iii) The purposes for which the cell site simulator device was used or, if the application was denied, the proposed purposes;

(iv) Whether the initial use of the cell site simulator device was:

1. Pursuant to Section 4 of this act;

2. Pursuant to Section 5 of this act;

3. Unauthorized by this act; or

4. The device was never used;

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

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

(vii) 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

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

(3) Information provided to the Attorney General pursuant to subsections (1) and (2) is subject to the Mississippi Public Records Act of 1983.

(4) Before July 1 of each year, beginning in 2019, the Attorney General shall submit to the Legislature a full and complete report on the implementation of Sections 1 through 12 of this act. The report must include data from the preceding calendar year concerning the number of applications pursuant to Section 3, the number of times access to content, data or location information was obtained pursuant to Section 5 and the number of

warrants granted or denied pursuant to Section 4. The report also must include a summary and analysis of the data required to be filed with the Attorney General under subsections (1) and (2) of this section. A copy of the report required must be made publicly available on the website for the Attorney General. The Attorney General may issue regulations regarding the content and form of the reports required to be filed pursuant to subsections (1) and (2) of this section.

SECTION 11. (1) (a) 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 subsection (3) of Section 2, may recover, in a civil action, from the person or entity that engaged in the violation such relief as may be appropriate.

(b) In a civil action under this subsection, appropriate relief may include:

(i) Preliminary and other equitable or declaratory relief as is appropriate;

(ii) Damages under paragraph (c) of this subsection; and

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

(c) 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 may a person whose data is obtained, accessed, used, transmitted, copied, disclosed or retained by any knowing violation of Sections 1 through 12 of this act, or on whose communications device software or applications are installed in violation of subsection (3) of Section 2, receive less than minimum statutory damages in the amount of One Thousand Dollars ($1,000.00). If the violation is intentional, the court may assess punitive damages.

(2) If a court or the Attorney General determines that a state, county, municipal or other local governing agency, department, authority or other entity, including any agent, employee or law enforcement official, has violated any provision of Sections 1 through 12 of this act and that the circumstances surrounding the violation raise serious questions about whether the violation was intentional, the Attorney General must initiate a proceeding to determine whether disciplinary action is warranted. If the Attorney General determines disciplinary action is not warranted, the reasons for the determination, including a summary of the incident and the reasons for declining disciplinary action, must be included in the next report issued pursuant to subsection (4) of Section 10.

SECTION 12. The provisions of Sections 1 through 12 of this act are severable. If any part or provision of Sections 1 through 12 of this act, or the application of those sections of this act to any person, entity or circumstance, is held invalid, the

remainder of Sections 1 through 12 of this act, including the application of such part or provision to other persons, entities or circumstances, is not affected by such that holding and continues to have force and effect.

SECTION 13. (1) Except as otherwise provided in subsection (2), an agency or employee of the state or any subdivision of the state may not use, either directly or indirectly, a license plate scanner on any public highway.

(2) (a) The Mississippi Department of Transportation or the transportation department of a county or an incorporated city or town may use a license plate scanner:

(i) To collect data for planning. If data is collected under this subparagraph (i), the Department of Transportation or the county, city or town must ensure and maintain the anonymity of the vehicle, the vehicle owner, the driver of the vehicle and any passengers in the vehicle. Data collected under this subparagraph (i) without a search warrant or outside of judicially recognized exceptions to search warrant requirements may not be used to investigate or prosecute an individual or as evidence in court; or

(ii) In a regulated parking system, but only to identify a vehicle's location and license plate number to enforce parking restrictions.

(b) The Mississippi Department of Transportation may use a device and equipment, including license plate scanners, if

necessary, to implement the provisions of Chapter 5, Title 63, Mississippi Code of 1972, if the devices or equipment are used in screening operations associated with:

(i) Virtual ports of entry;

(ii) Weigh station ramps using automated weigh station screening systems;

(iii) Virtual weigh stations using weigh-in-motion technology; or

(iv) An automatic vehicle identification system that enables participating transponder-equipped vehicles to be prescreened throughout the nation at designated weigh stations, port-of-entry facilities or agricultural interdiction facilities.

(c) Nothing in this section prohibits an agency of the state or any subdivision of the state from using its own vehicles, aircraft or equipment, including a license plate scanner, to track, monitor or otherwise maintain information about the agency's or subdivision's vehicles, aircraft or equipment.

(3) A public employee or public officer who violates this section is subject to any applicable penalties provided for by law.

(4) As used in this section, the term "license plate scanner" means a device principally designed and primarily used for determining the ownership of a motor vehicle, the mileage or route traveled by a motor vehicle, the location or identity of a motor vehicle, or the identity of a motor vehicle's occupants on

the public highways through the use of a camera or other imaging device or any other device, including, but not limited to, a transponder, cellular telephone, global positioning satellite, automated electronic toll collection system, automated license plate recognition system, or radio frequency identification device that by itself or in conjunction with other devices or information can be used to determine the ownership of a motor vehicle or the identity of a motor vehicle's occupants or the mileage, location or route traveled by the motor vehicle.

SECTION 14. The information collected and stored in any database under Section 13 of this act:

(a) Is private, not a public record and not subject to public disclosure;

(b) May be accessed by an employee of the state or a political subdivision of the state only for the purpose of providing customer service or for statistical, administrative or legal activities necessary to perform the employee's duties; and

(c) May be maintained only for the time minimally necessary, but in no event, more than eighteen (18) months.

SECTION 15. An agency or employee of the state or any subdivision of the state may not use, either directly or indirectly, oral fluid tests for the purpose of determining whether or not an individual is acting under the influence of controlled substances.

SECTION 16. This act shall take effect and be in force from and after July 1, 2018.