Amendments to the Electronic Data Privacy Protection Act

Summary: The proliferation of Internet-connected and geolocation-enabled devices presents new challenges for state laws protecting personal information from unauthorized search. This model act aims to provide some clarity for the courts, law enforcement, and consumers by stating that a warrant or exception is required prior to search of mobile devices incident to arrest, and obtaining geolocation information. Also, the act requires courts to issue a report on the number of warrants requested and exceptions granted.

Digital Information Electronic Data Privacy Protection Act

Purpose: The proliferation of Internet-connected and geolocation-enabled devices presents new challenges for state laws protecting personal information from unauthorized search. This model act aims to provide some clarity for the courts, law enforcement, and consumers by stating that a warrant or exception is required prior to obtain, access, and use a person's digital information, whether stored on their own device or with a third party, to search of mobile devices incident to arrest, and obtaining geolocation information. Also, the act requires courts to issue a report on the number of warrants requested and exceptions granted.

SECTION 1. (Title) This Act may be cited as the Digital Information Electronic Data Privacy Protection Act.

SECTION 2. (Purpose) The purpose of this Act is to clarify requirements to obtain, access, and use a person's digital information, whether stored on their own device or held by a third party, for searches of electronic messages, mobile devices incident to arrest, and obtaining geolocation information.

SECTION 3. (Definitions)

(A) As used in this subchapter, unless otherwise indicated, the following terms have the following meanings.

1. **Adverse Result.** “Adverse Result” means:
   a. Immediate danger of death or serious physical injury;
   b. Flight from prosecution;
   c. Destruction of or tampering with evidence;
   d. Intimidation of a potential witness; or
   e. Substantially jeopardizes an investigation.
2. **Biometric Information System.** “Biometric Information System” means any tool, program, service, or system used to uniquely identify, verify identity of, and track individuals using retina and iris scans, fingerprints, voiceprints, hand and face geometry, gait patterns, or other automated systems identifying individuals through analysis of human features.

3. **Electronic Communication Service.** “Electronic Communication Service” means a service that provides Users the ability to send or receive wire or electronic communications as defined in 18 U.S.C. § 2510(15).

3. **Electronic Device.** “Electronic Device” means a device that contains data; or enables access to, or use of, a Third Party’s Electronic Communication Service, or Remote Computing Service or Geolocation Information Service; or a radio-frequency identification chip or other transponder.

4. a. Digital Information means:
   i. Information that a person creates that exists in digital form, either online or on an electronic storage device. It includes information necessary to access the digital information; and
   ii. Information that a person shares with a third party in connection to the provision of goods or services to that person and is recorded in digital form. This includes all digital records containing such information; and
   iii. Information concerning the location of an Electronic Device that is generated by or derived from the operation or tracking of the device and could be used to determine or infer information regarding the location of the person, but does not include Internet Protocol addresses

   b. This definition does not include information a person voluntarily shares with the public or a third party with the understanding that the third party will share that information with the public.

5. **Domestic Entity.** “Domestic Entity” has the meaning assigned by the state business organizations code.

6. **Government Entity.** “Government Entity” means a state or local department or agency

7. **Geolocation Information.** “Geolocation Information” means any information that is not the content of an electronic communication as defined in 18 U.S.C. § 2510, concerning the location of an Electronic Device that, in whole or in part, is generated by or derived from the operation or tracking of that device and that could be used to determine or infer information regarding the location of the person, but does not include Internet Protocol addresses.

8. **Geolocation Information Service.** “Geolocation Information Service” means the provision of a global positioning service or other mapping, locational, or directional information service to the public, or to such class of users as to be effectively available to the public, by or through the operation of any wireless communication device, including any Electronic Device, global positioning system receiving device, or other similar or successor device.

9. a. **User.** “User” means any person or entity who—
Section 4. (Warrant required prior to search of Electronic Device obtained incident to arrest; warrant needed for acquisition of a person’s digital information or Geolocation Information)

(A) Except as provided in this subchapter or another provision of law, a Government Entity may not search or seize digital information of any person, whether stored on their electronic device or held by a third party, conduct a search of an Electronic Device without a valid search or seizure warrant issued upon probable cause by a duly authorized judge or justice using state warrant procedures.

(B) Except as provided in this subchapter or another provision of law, digital information contained or stored in an Electronic Device is not subject to a search or seizure by a Government Entity incident to a lawful custodial arrest without a valid search or seizure warrant issued upon probable cause by a duly authorized judge or justice using state warrant procedures.

(C) Except as provided in this subchapter or another provision of law, a Government Entity may not compel a User or Geolocation Information Service to provide a passkey, password, key code, to any Geolocation Information or Electronic Device without a valid search warrant issued by a duly authorized judge or justice using state warrant procedures.

(D) A Government Entity may not obtain Geolocation Information revealing the past, present or future location of an Electronic Device except:

1. With a valid search warrant issued by a duly authorized judge or justice using state warrant procedures;
2. With the consent of the person to whom the Geolocation Information pertains;
3. With the consent of a parent or legal guardian of a child or person adjudicated to be mentally incompetent to whom the Geolocation Information pertains;
4. In an emergency if the Geolocation Information is used respond to a request for assistance from the person to whom the information pertains, or to assist such person in circumstances when it is reasonable to believe that the life or safety of such person is threatened; or
5. To locate a stolen Electronic Device with the consent of the owner or operator of such device.

(D) Nothing in this section prevents a Government Entity from using Digital Information to locate a stolen Electronic Device with consent of the owner of the device.

(E)(F) Except as provided in another provision of law a Government Entity may not operate an Electronic Device to access data held by a Third Party stored on an Electronic Communications Service or Remote Computing Service.

(F)(F) Except as provided in this subchapter or another provision of law, a Government Entity may not track, monitor or observe an individual, or an individual's electronic communications, electronic habits or routines, or an individual's habits or routines in public, using Biometric Information Systems, or obtain any information regarding a Biometric Information System related to Users without a valid search warrant issued by a duly authorized judge or justice using state warrant procedures.

(G)(G) A warrant issued under this subchapter may be served only on a service provider that is a Domestic Entity or a company or entity otherwise doing business in this state under a contract or terms of service agreement with a resident of this state, if any part of that contract or agreement is to be performed in this state, and the service provider shall produce all information sought regardless of where the information is held and within the period allowed for under the state's criminal code provisions for compliance with the warrant.

(H)(H) A judge or justice may issue a wiretap warrant under this subchapter for the Digital Geolocation Information of an Electronic Device pursuant to this section for a period of time necessary to achieve the objective of the authorization, but in no case may an initial wiretap warrant seek present or future Geolocation Digital Information for a period longer than 10 days. A judge or justice may grant an extension of a wiretap warrant upon a finding of continuing probable cause and a finding that the extension is necessary to achieve the objective of the authorization. An extension may not exceed 10 days.

Section 5. {Notice}

(A) Notice must be given to the User whose Electronic Device was searched or whose Digital Geolocation Information was obtained by a Government Entity.

(B) Timing and content of notice. Unless delayed notice is ordered under subsection C, the Government Entity shall provide notice to the User whose Electronic Device was searched or Geolocation-Digital Information was obtained by a Government Entity within three days of obtaining the Geolocation-Digital Information or conducting the search. The notice must be made by service or delivered by registered or first-class mail, e-mail or any other means reasonably calculated to be effective as specified by the court issuing the warrant. The notice must contain the following information:

1. The nature of the law enforcement inquiry, with reasonable specificity;
2. The Geolocation Digital Information and information on the Electronic Device of the User that was supplied to or requested by the Government Entity and the date on which it was provided or requested;

3. If Geolocation Digital Information was obtained from a Third Party Provider of Geolocation Information Service or other third party, the identity of the Third Party Provider of the Geolocation Information Service or the third party from whom the information was obtained; and

4. Whether the notification was delayed pursuant to subsection C and, if so, the court that granted the delay and the reasons for granting the delay.

(C) Delay of notification. A Government Entity acting under section 4 may include in the application for a warrant a request for an order to delay the notification required under this section for a period not to exceed 90 days. The court shall issue the order if the court determines that there is reason to believe that notification may have an Adverse Result. Upon expiration of the period of delay granted under this subsection and any extension granted under subsection E, the Government Entity shall provide the User a copy of the warrant together with a notice pursuant to subsections A and B.

(D) Preclusion of notice to User. A Government Entity acting under section 4 may include in its application for a warrant a request for an order directing a provider of Geolocation Information Service Third Party to which a warrant is directed not to notify any other person of the existence of the warrant for a period of not more than 90 days. The court shall issue the order if the court determines that there is reason to believe that notification of the existence of the warrant may have an Adverse Result. Absent an order to delay notification or upon expiration of the period of delay, a Third Party Service provider of Geolocation Information Service to which a warrant is directed may provide notice to any other person.

(E) Extension. The court, upon application, may grant one or more extensions of orders granted under subsection C or D for up to an additional 90 days.

SECTION 6. (Exceptions)

(A) Nothing in this subchapter shall be interpreted to affect the rights and responsibilities of Third Party service providers of an Electronic Communication Service, Geolocation Information Service, Remote Computing Service, or a Government Entity conferred by 18 U.S.C. §§ 2702 (a)-(c), 47 U.S.C. § 222, or a lawful exception to the warrant requirement.

(B) A Third Party service provider of Geolocation Information Service, Electronic Communication Service, or Remote Computing Services may divulge Geolocation Digital Information pertaining to a user of such service to a government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of Geolocation Digital Information relating to the emergency so long as such disclosure is not in violation of 18 U.S.C. § 2702.

(C) No later than 48 hours after seeking disclosure of information pursuant to this subsection, the Government Entity seeking to conduct the search or obtain the Digital Geolocation Information shall file
with the appropriate court a written statement setting forth the facts giving rise to the emergency and
the facts as to why the information sought is believed to be important in addressing the emergency.

SECTION 7 (Reporting requirements)

(A) Report by judge or justice. No later than January 31st each year, the clerk of the court who issues or
denies a warrant under Section 4 during the preceding calendar year must report on each warrant to the
state’s administrative office of the courts. The report must include, but is not limited to:

1. The fact that the warrant was applied for;
2. The identity of the Government Entity that made the application;
3. The offense specified in the warrant or warrant application;
4. The nature of the facilities from which, the place where or the technique by which Digital
   Geolocation Information was to be obtained;
5. The number of Electronic Devices searched and about which Digital Geolocation Information was
to be obtained;
6. Whether the warrant was granted as applied for or was modified or denied; and
7. The period of disclosures authorized by the warrant, and the number and duration of any
   extensions of the warrant

(B) Report by administrative office of the courts to Legislature. In June of each year, beginning in 2014,
the administrative office of the courts of the state shall submit to the Legislature a full and complete
report concerning the number of applications for warrants authorizing or requiring searches or the
disclosure of Geolocation Digital Information pursuant to this subchapter, the number of times access to
Geolocation Digital Information was obtained pursuant to Section 6 during the preceding calendar year,
the given reason for each exception under Section 6, and the identity of the Government Entity that
requested the exception. The full and complete report must include a summary and analysis of the data
required under this subsection, as well as a searchable, itemized, and accessible database populated
with the complete data required under this subsection.

(C) Report publicly accessible. In June of each year, beginning in 2014, the report summary and
database required under subsection B must be made publicly available on the judicial branch’s publicly
accessible website. The Administrative Office of the Courts may prescribe the form of the reports and
databases under this section and shall make concentrated efforts to provide and maintain reports and
databases available online to the general public in optimally usable forms or formats at no cost.

SECTION 8. (Conditions of use of information)
(A) Use of data GeolocationDigital Information obtained in violation of this subchapter not admissible. Except as proof of a violation of this subchapter, information obtained in violation of this subchapter is not admissible as evidence in a criminal, civil, administrative or other proceeding.

(B) Conditions of use of data GeolocationDigital Information in proceeding. Data or GeolocationDigital Information obtained pursuant to this subchapter or evidence derived from that information may be received in evidence or otherwise disclosed in a trial, hearing or other proceeding only if each party, before the trial, hearing or proceeding, has been furnished with a copy of the warrant and accompanying application under which the information was obtained pursuant to the state code of criminal procedure.

(C) Exception. The requirement under subsection B may be waived if a judge makes a finding that it was not possible to provide a party with the warrant and accompanying application prior to a trial, hearing or proceeding and that the party will not be prejudiced by the delay in receiving the information.

Section 9. (Action against a corporation)

(A) No cause of action shall lie in any court of this state against any Third Party service provider of an Electronic Communications Service, Remote Computing Service, or Geolocation Information Service, or its officers, employees, agents or other specified persons for providing information, facilities or assistance in accordance with the terms of a warrant or exception under this subchapter or with a good faith reliance on

1. A court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity); or
2. A good faith determination that such disclosure is permitted under this Act.

Section 10. (Evidentiary Admissibility)

(A) An original or certified copy of any data produced pursuant to a warrant or exception in accordance with this subsection shall be self-authenticating and admissible into evidence as provided in Fed. R. Evid. 902(11) and 803(6).
Section 11. (Reimbursement)

(A) Payment — Except as otherwise provided by law, a Government Entity obtaining data under this section shall pay to the person or entity assembling or providing such information a fee for reimbursement for costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(B) Amount — The amount of the fee provided by subsection (a) shall be as mutually agreed by the Government Entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

Section 12. (Limitations)

(A) The repeal or amendment by this act of any law, whether temporary or permanent or civil or criminal, does not affect pending actions, rights, duties, or liabilities founded thereon, or alter, discharge, release or extinguish any penalty, forfeiture, or liability incurred under the repealed or amended law, unless the repealed or amended provision shall so expressly provide. After the effective date of this act, all laws repealed or amended by this act must be taken and treated as remaining in full force and effect for the purpose of sustaining any pending or vested right, civil action, special proceeding, criminal prosecution, or appeal existing as of the effective date of this act, and for the enforcement of rights, duties, penalties, forfeitures, and liabilities as they stood under the repealed or amended laws.

Section 13. (Effective Date)

(A) This act takes effect upon approval by the Governor.

Section 14. (Severability Clause)

(A) Should any part of this Act be rendered or declared unconstitutional by a court of competent jurisdiction of the State, such invalidation of such part or portion of this Act should not invalidate the remaining portions thereof, and they shall remain in full force and effect.

Section 15. (Repealer Clause)

(A) The following laws are hereby repealed: