**A** **BILL**

TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, TO ENACT THE “ELECTRONIC DATA PRIVACY PROTECTION ACT” BY ADDING CHAPTER 53 TO TITLE 23, SO AS TO PROVIDE THAT AN ENTITY MAY NOT SEARCH AN ELECTRONIC DEVICE WITHOUT A SEARCH WARRANT, TO PROVIDE EXCEPTIONS, AND TO PROVIDE CERTAIN NOTICE REQUIREMENTS.

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. Title 23 of the 1976 Code is amended by adding:

“CHAPTER 53

Electronic Data Privacy Protection Act

Section 23‑53‑10. This chapter may be cited as the ‘Electronic Data Privacy Protection Act’.

Section 23‑53‑20. The purpose of this chapter is to clarify requirements for searches of electronic messages, mobile devices incident to arrest, and obtaining geolocation information.

Section 23‑53‑30. As used this chapter, unless the context clearly indicates otherwise:

(1) ‘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’ 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.

(3) ‘Electronic communication service’ means a service that provides to users the ability to send or receive wire or electronic communications as defined in 18 U.S.C. Section 2510(15).

(4) ‘Electronic device’ means a device that contains electronic user data; or enables access to, or use of, an electronic communication service, remote computing service, or geolocation information service; or a radio‑frequency identification chip or other transponder.

(5) ‘Electronic storage’ means any storage of electronic user data on a computer, computer network, or computer system, regardless of whether the data is subject to recall, further manipulation, deletion, or transmission, and includes any storage or electronic communication by an electronic communications service or a remote computing service, as well as temporary intermediate storage of electronic data or information incidental to the electronic transmission of electronic user data or communication.

(6) ‘Electronic user data’ means data or records that are in the possession, care, custody, or control of a provider of an electronic communications service, a remote computing service, or geolocation information service, that contains:

(a) information revealing the identity of users of the applicable service, device, or program;

(b) information about a user’s use of the applicable service, device, or program;

(c) information that identifies the recipient or destination of a wire communication or electronic communication sent to or by the user;

(d) the content of a wire communication or electronic communication sent to or by the user; or

(e) any data, documents, files, or communications stored by or on behalf of the user with the applicable service provider or on the user’s electronic device.

(7) ‘Geolocation information’ means any information that is not the content of a communication 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’ 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) ‘Governmental entity’ means the State or any of its political subdivisions, including school districts.

(10) ‘Remote computing service’ means, as defined in 18 U.S.C. Section 2711(2), the provision to the public of computer storage or processing services by means of an electronic communications system, as defined in 18 U.S.C. Section 2510(14).

(11) ‘User’ means any person or entity who:

(a) uses an electronic communication service, remote computing service, geolocation information service, or an electronic device; and

(b) may or may not be the person or entity having legal title, claim, or right to the electronic device or electronic user data.

Section 23‑53‑40. (A) Except as provided in this chapter or another provision of law:

(1) A governmental entity may not conduct a search of an electronic device or compel an electronic communication service or remote computing service to disclose the content of a user’s communications without a valid search warrant issued by a duly authorized judge or justice using state warrant procedures.

(2) Information contained or stored in an electronic device is not subject to a search by a governmental entity incident to a lawful custodial arrest without a valid search warrant issued by a duly authorized judge or justice using state warrant procedures.

(3) A governmental entity may not compel a user, electronic communication service, remote computing service, or geolocation information service to provide a passkey, password, or key code to any electronic communications, geolocation information, or remote computing service, electronic device, electronic storage, or any other form of stored electronic user data, without a valid search warrant issued by a duly authorized judge or justice using state warrant procedures.

(B) A governmental 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, provided that the geolocation information will be used only for the purpose for which the consent was granted and will remain only with the governmental entity that obtained the consent;

(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, provided that the geolocation information will be used only for the purpose for which the consent was granted and will remain only with the governmental entity that obtained the consent;

(4) when such geolocation information is accessed through a system that is configured so that such information is readily accessible to the general public;

(5) in an emergency, if the geolocation information is used to 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

(6) to locate a stolen electronic device with the consent of the owner or operator of such device.

(C) Except as provided in this chapter or another provision of law, a governmental 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 that is maintained by an electronic communications, remote computing, or geolocation information service, without a valid search warrant issued by a duly authorized judge or justice using state warrant procedures.

(D)(1) A judge may issue a search warrant pursuant to this chapter for electronic user data held in electronic storage, including the contents of and records and other information related to a wire communication or electronic communication held in electronic storage, by a provider of an electronic communications service or a provider of a remote computing service regardless of whether the user data is held at a location in this State or at a location in another state.

(2) A warrant issued pursuant to this chapter 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 by law for compliance with the warrant.

(E) A judge may issue a warrant pursuant to this chapter for the 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 warrant seek present or future geolocation information for a period longer than ten days. A judge may grant an extension of a 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 ten days.

Section 23‑53‑50. (A) Notice must be given to the user whose electronic device was searched or whose geolocation information or electronic user data was obtained by a governmental entity.

(B) Unless delayed notice is ordered pursuant to subsection (C), the governmental entity shall provide notice to the user whose electronic device was searched or whose electronic user data or geolocation information was obtained by a governmental entity within three days of obtaining the geolocation information or electronic user data or conducting the search. The notice must be made by service or delivered by registered or first‑class mail, email, 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 information or electronic user data of the user that was supplied to or requested by the governmental entity and the date on which it was provided or requested;

(3) if geolocation information or electronic user data was obtained from a provider of electronic communication service or geolocation information service or other third party, the identity of the provider of electronic communication service or 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) A governmental entity acting pursuant to Section 23‑53‑40 may include in the application for a warrant a request for an order to delay the notification required pursuant to this section for a period not to exceed ninety 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 pursuant to this subsection and any extension granted pursuant to subsection (E), the governmental entity shall provide the user a copy of the warrant together with a notice pursuant to subsections (A) and (B).

(D) A governmental entity acting pursuant to Section 23‑53‑40 may include in its application for a warrant a request for an order directing a provider of electronic communication service or geolocation information service 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 ninety 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 provider of electronic communication service or geolocation information service to which a warrant is directed may provide notice to any other person.

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

Section 23‑53‑60. (A) Nothing in this chapter shall be interpreted to affect the rights and responsibilities of providers of an electronic communication service, geolocation information service, remote computing service, or a governmental entity conferred by 18 U.S.C. Section 2702 (a)‑(c), 47 U.S.C. Section 222, or a lawful exception to the warrant requirement.

(B) A provider of geolocation information service, electronic communication service, or remote computing services may divulge geolocation information pertaining to a user of such service to a governmental 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 information relating to the emergency.

(C) No later than forty‑eight hours after seeking disclosure of information pursuant to subsection (B), the governmental entity seeking to conduct the search or obtain the 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 23‑53‑70. (A) Beginning January 15, 2015, and each January thirty‑first thereafter, the clerk of the court who issues or denies a warrant pursuant to Section 23‑53‑40 during the preceding calendar year must report on each warrant to the South Carolina Court Administration. The report must include, but is not limited to:

(1) the fact that the warrant was applied for;

(2) the identity of the governmental 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 geolocation information or electronic user data was to be obtained;

(5) the number of electronic devices searched and about which 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) Beginning in June 2015, and each June thereafter, the South Carolina Court Administration shall submit to the General Assembly a full and complete report concerning the number of applications for warrants authorizing or requiring searches or the disclosure of geolocation information or electronic user data pursuant to subsection (A), the number of times access to geolocation information or electronic user data was obtained pursuant to Section 23‑53‑60 during the preceding calendar year, the given reason for each exception pursuant to Section 23‑53‑60, and the identity of the governmental entity that requested the exception. The full and complete report must include a summary and analysis of the data required pursuant to this subsection, as well as a searchable, itemized, and accessible database populated with the complete data required pursuant to this subsection.

(C) Beginning in June 2015, and each June thereafter, the report summary and database required pursuant to subsection (B) must be made publicly available on the South Carolina Court Administration’s publicly accessible website. The South Carolina Court Administration may prescribe the form of the reports and databases 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 23‑53‑80. (A) Except as proof of a violation of this chapter, information obtained in violation of this chapter is not admissible as evidence in a criminal, civil, administrative, or other proceeding.

(B) Electronic user data or geolocation information obtained pursuant to this chapter 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.

(C) The requirement pursuant to 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 23‑53‑90. No cause of action shall lie in any court of this State against any 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 pursuant to this chapter.

Section 23‑53‑100. An original or certified copy of electronic user data produced pursuant to a warrant or exception in accordance with this chapter shall be self‑authenticating and admissible into evidence as provided in Fed. R. Evid. 902(11) and 803(6).

Section 23‑53‑110. (A) Except as otherwise provided by law, a governmental entity obtaining electronic user data pursuant to this chapter 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. The 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) The amount of the fee provided by subsection (A) must be as mutually agreed by the governmental entity and the person or entity providing the information. In the absence of agreement, must be as determined by the court which issued the order for production of such information, or if no court order was issued for production of the information, the court before which a criminal prosecution relating to such information would be brought.”

SECTION 2. 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 3. This act takes effect upon approval by the Governor.

‑‑‑‑XX‑‑‑‑