**South Carolina General Assembly**

123rd Session, 2019-2020

**H. 4817**

**STATUS INFORMATION**

General Bill

Sponsors: Reps. G.R. Smith, Clemmons, Rutherford, Magnuson, Jones and Clyburn

Document Path: l:\council\bills\jn\3124cz20.docx

Introduced in the House on January 14, 2020

Currently residing in the House Committee on **Judiciary**

Summary: SC Data Privacy Act

**HISTORY OF LEGISLATIVE ACTIONS**

Date Body Action Description with journal page number

12/11/2019 House Prefiled

12/11/2019 House Referred to Committee on **Judiciary**

1/14/2020 House Introduced and read first time ([House Journal‑page 116](file:///h:\hj\20200114.docx))

1/14/2020 House Referred to Committee on **Judiciary** ([House Journal‑page 116](file:///h:\hj\20200114.docx))

View the latest [legislative information](http://www.scstatehouse.gov/billsearch.php?billnumbers=4817&session=123&summary=B) at the website

**VERSIONS OF THIS BILL**

[12/11/2019](file:///p:\pprever\2019-20\4817_20191211.docx)

**A** **BILL**

TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, TO ENACT THE “SOUTH CAROLINA DATA PRIVACY ACT” BY ADDING ARTICLE 3 TO CHAPTER 13, TITLE 17 SO AS TO PROVIDE FOR A CITATION, TO DEFINE NECESSARY TERMS, TO PROVIDE THAT A SEARCH WARRANT MUST BE ISSUED BEFORE CERTAIN ELECTRONIC DATA MAY BE SEIZED BY A LAW ENFORCEMENT AGENCY, TO REQUIRE THE LAW ENFORCEMENT AGENCY TO NOTIFY THE OWNER OF THE ELECTRONIC DEVICE, DATA, OR INFORMATION SPECIFIED IN THE SEARCH WARRANT, TO PROHIBIT A LAW ENFORCEMENT AGENCY FROM COLLECTING CERTAIN INFORMATION FROM A THIRD‑PARTY WITHOUT A SEARCH WARRANT, TO PROHIBIT THE USE OF INFORMATION OBTAINED IN VIOLATION OF THE PROVISIONS OF ARTICLE 3, AND TO PROVIDE FOR CERTAIN EXCEPTIONS; AND TO DESIGNATE SECTIONS 17‑13‑10 THROUGH 17‑13‑170 OF CHAPTER 13, TITLE 17 AS ARTICLE 1, ENTITLED “GENERAL PROVISIONS”.

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

SECTION 1. Chapter 13, Title 17 of the 1976 Code is amended by adding:

“Article 3

South Carolina Data Privacy Act

Section 17‑13‑200. This article may be cited as the “South Carolina Data Privacy Act”.

Section 17‑13‑210. As used in this article:

(1) ‘Electronic communication’ means a transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, photooptical system, or any other device that affects intrastate, interstate, or foreign commerce, but does not include:

(a) any wire or oral communication;

(b) any communication made through a tone‑only paging device; or

(c) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

(2) ‘Electronic communication service’ means a service that provides to users of the service the ability to send or receive wire or electronic communications.

(3) ‘Electronic device’ means a device that enables access to or use of an electronic communication service, remote computing service, or location information service.

(4) ‘Electronic information’ or ‘data’ means information or data including a sign, signal, writing, image, sound, data, or intelligence of any nature transmitted or stored in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system. This includes location information, stored data, or transmitted data or an electronic device but does not include:

(a) any wire or oral communication;

(b) any communication made through a tone‑only paging device; or

(c) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

(5) ‘Law enforcement agency’ means a lawfully established federal, state, or local public agency that is responsible for the prevention and detection of crime, and its agents and officers are empowered by law to conduct criminal investigations and to make arrests.

(6) ‘Locational information’ means information obtained by means of a tracking device concerning the location of an electronic device that, in whole or in part, is generated or derived from or obtained by the operation of the electronic device.

(7) ‘Location information service’ means the provision of a global positioning service or other mapping, location, or directional information service.

(8) ‘Oral communication’ means any oral communication uttered by a person exhibiting an expectation that the communication is not subject to interception, under circumstances justifying that expectation, but does not include any electronic communication.

(9) ‘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).

(10) ‘Subscriber record’ means a record or information held by a electronic communication service provider or a remote computing service provider that reveals the subscriber’s or customer’s:

(a) name;

(b) address;

(c) local and long distance telephone connection record, including the time and duration of each call;

(d) length of service, including the start date;

(e) type of service used;

(f) telephone number, instrument number, or other subscriber or customer number or identification, including a temporarily assigned network address; and

(g) means and source of payment for the service, including a credit card or bank account number.

(11) ‘Transmitted data’ means electronic information or data transmitted wirelessly from an electronic device to:

(a) another electronic device without the use of an intermediate connection or relay; or

(b) a nearby antenna.

(12) ‘Wire communication’ means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the use of this connection in a switching station furnished or operated by any person engaged in providing or operating the facilities for the transmission of intrastate, interstate, or foreign communications or communications affecting intrastate, interstate, or foreign commerce. The term includes any electronic storage of the communication.

Section 17‑13‑220. (A)(1) A law enforcement agency may not obtain the following for a criminal investigation without a valid search warrant or court order issued by a duly authorized judge or justice using state warrant procedures and based upon probable cause:

(a) the location information, stored data, or transmitted data of an electronic device; or

(b) electronic information or data transmitted by the owner of the electronic information or data to a remote computing service provider.

(2) A law enforcement agency:

(a) may not use, copy, or disclose, for any purpose, the location information, stored data, transmitted data of an electronic device, or electronic information or data provided by a remote computing service provider that is not within the subject of the search warrant collected as part of an effort to obtain the location information, stored data, transmitted data of an electronic device, or electronic information or data provided by a remote computing service provider subject to a search warrant;

(b) may use, copy, or disclose the transmitted data of an electronic device used to communicate with the electronic device that is the subject of the search warrant if the agency reasonably believes that the transmitted data is necessary to achieve the objective of the search warrant; and

(c) must destroy the electronic information or data in an unrecoverable manner as soon as reasonably possible after the electronic information or data is collected.

(B)(1) A law enforcement agency may obtain location information without a search warrant for an electronic device:

(a) when the law enforcement agency has reason to believe that the electronic device user is in need of emergency response services or in an emergency situation that involves the imminent risk of death or serious bodily injury;

(b) if the device is reported stolen by the owner;

(c) with the informed affirmative consent of the owner or user of the electronic device;

(d) in accordance with a judicially recognized exception to warrant requirements;

(e) if the owner has voluntarily and publicly disclosed the location information; or

(f) from the remote computing service provider if the remote computing service provider voluntarily discloses location information:

(i) under a belief that an emergency exists involving an imminent risk to an individual of death, serious physical injury, sexual abuse, live‑streamed sexual exploitation, kidnapping, or human trafficking; or

(ii) that is inadvertently discovered by the remote computing service provider and appears to pertain to the commission of a felony or of a misdemeanor involving physical violence or sexual abuse.

(2) A law enforcement agency may obtain stored or transmitted data from an electronic device or electronic information or data transmitted by the owner of the electronic information or data to a remote computing service provider without a search warrant:

(a) with the informed consent of the owner of the electronic device or electronic information or data;

(b) in accordance with a judicially recognized exception to warrant requirements;

(c) in connection with a report forwarded by the National Center for Missing and Exploited Children; or

(d) if the data was inadvertently discovered by a remote computing service provider that appears to pertain to the commission of a felony or of a misdemeanor involving physical violence or sexual abuse.

(C) An electronic communication service provider, remote computing service provider, the provider’s officers, employees, agents, or other specified persons may not be held liable for providing information, facilities, or assistance in good faith reliance on the terms of a search warrant issued pursuant to the provisions of this article or acting without a search warrant in accordance with this section.

Section 17‑13‑230. (A) A law enforcement agency that executes a search warrant pursuant to this article must issue a notification to the owner of the electronic device or electronic information or data specified in the search warrant within fourteen days after the day on which the electronic information or data subject to the search warrant is obtained stating:

(1) that a warrant was applied for and granted;

(2) the type of warrant issued;

(3) the period of time during which the collection of the electronic information or data was authorized;

(4) the offense specified in the application for the warrant;

(5) the identity of the law enforcement agency that filed the application; and

(6) the identity of the judge who issued the warrant.

(B)(1) A law enforcement agency seeking a warrant may submit a request to delay the notification for a period not to exceed thirty days. A court of appropriate jurisdiction may approve the delay if it determines that there is reasonable cause to believe the notification may:

(a) endanger the life or physical safety of an individual;

(b) cause a person to flee from prosecution;

(c) lead to the destruction of or tampering with evidence;

(d) lead to the intimidation of a potential witness; or

(e) otherwise seriously jeopardize an investigation or unduly delay a trial.

(2) The court may grant an additional extension of up to sixty days if it finds that an extension is appropriate and the investigation is:

(a) interstate in nature and sufficiently complex; or

(b) likely to extend up to or beyond an additional sixty days.

(C) Upon expiration of the period of delayed notification, the law enforcement agency shall serve upon or deliver by first‑class mail, or by other means if delivery is impracticable, to the owner of the electronic device or electronic information or data a copy of the warrant and a notice that states with reasonable specificity the nature of the law enforcement inquiry and contains:

(1) all information required by subsection (A);

(2) a statement indicating that notification was delayed;

(3) the court and identity of the judge who authorized the delay of notification; and

(4) a reference to the provision of law that allows for the delay of notification.

(D) A law enforcement agency is not required to notify the owner of the electronic device or electronic information or data if the owner is located outside of the United States.

Section 17‑13‑240. (A) A law enforcement agency may not obtain, use, copy, or disclose:

(1) a subscriber record without a court order or except as specifically provided for in this section; or

(2) any record of information, other than a subscriber record, of an electronic communication service provider or remote computing service provider related to a subscriber or customer without a valid search warrant.

(B) A law enforcement agency may obtain, use, copy, or disclose a subscriber record or other record of information record related to a subscriber or customer without a search warrant:

(1) with the informed affirmed consent of the subscriber or customer;

(2) in accordance with a judicially recognized exception to warrant requirements;

(3) if the subscriber or customer voluntarily discloses the record in a manner that is publicly accessible; or

(4) if the provider of an electronic communication service or remote computer service voluntary discloses the record:

(a) under a belief that an emergency exists involving the imminent risk to an individual of death, serious physical injury, sexual abuse, live‑streamed sexual exploitation, kidnapping, or human trafficking; or

(b) that was inadvertently discovered by the provider if the record appears to pertain to the commission of a felony, a misdemeanor involving physical violence, sexual abuse, or dishonesty.

(C) An electronic communication service provider or a remote computing service provider, the provider’s officers, employees, agents, or other specified persons may not be held liable for providing information, facilities, or assistance in good faith reliance on the terms of a search warrant issued pursuant to the provisions of this article or acting without a search warrant in accordance with this section.

Section 17‑13‑250. Electronic information or data and records of an electronic communications service provider or a remote computing service provider pertaining to a subscriber or customer obtained in violation of the provisions of this article are subject to rules governing exclusion as if the records were obtained in violation of the Fourth Amendment to the United States Constitution.

Section 17‑13‑260. (A) Nothing in this article may be interpreted or construed to pertain to the use of electronic monitoring devices that are pursuant to conditions of bond, home detention, probation, parole, being categorized as a sex offender, or any other court‑ordered or statutory mandate.

(B) Nothing in this article shall restrict or limit agents of the Department of Corrections, Department of Juvenile Justice, and Department of Probation, Parole and Pardon Services from the authority to conduct searches of electronic devices and receive electronic data from electronic communication services for offenders under supervision.

(C) The provisions of this article shall not apply to a governmental entity’s search of electronic devices determined to be contraband pursuant to Section 24‑3‑950.”

SECTION 2. Sections 17‑13‑10 through 17‑13‑170 of the 1976 Code are designated as Article 1, entitled “General Provisions”.

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

‑‑‑‑XX‑‑‑‑