The Digital Privacy Protection Act

Purpose:

This proposal restricts the ability of law enforcement to obtain, access, and use a person's digital information, whether stored on their own device or in the cloud. It contains exemptions for when a warrant is not needed to access a person's information.

Text:

Section 1. Definitions

(1) "Electronic communication service" means a service that provides to users of the service the ability to send or receive wire or electronic communications.
(2) "Electronic device" means a device that enables access to or use of an electronic communication service, remote computing service, or location information service.
(3)
  (a) "Electronic information or data" means information or data including a sign, signal, writing, image, sound, or intelligence of any nature transmitted or stored in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system.
  (b) "Electronic information or data" includes the location information, stored data, or transmitted data of an electronic device.
  (c) "Electronic information or data" does not include:
    (i) a wire or oral communication;
    (ii) a communication made through a tone-only paging device; or
    (iii) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of money.
(4) "Law enforcement agency" means an entity of the state or a political subdivision of the state that exists to primarily prevent, detect, or prosecute crime and enforce criminal statutes or ordinances.
(5) "Location 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 an electronic device.
(6) "Location information service" means the provision of a global positioning service or other mapping, location, or directional information service.
(7) "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.
(8) "Subscriber record" means a record or information of a provider of an electronic communication service or remote computing service that reveals the subscriber's or customer's:
  (a) name;
  (b) address;
  (c) local and long distance telephone connection record, or record of session time and duration;
  (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.

(9) "Transmitted data" means electronic information or data that is transmitted wirelessly:

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

(b) from an electronic device to a nearby antenna.

(10) "Wire communication" means the same as that term is defined in Section 77-23a-3.

Section 2. Electronic information or data privacy

(1)

(a) Except as provided in Subsection (2), for a criminal investigation or prosecution, a law enforcement agency may not obtain, without a search warrant issued by a court upon probable cause:

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

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

(b) Except as provided in Subsection (1)(c), a law enforcement agency 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:

(i) is not the subject of the warrant; and

(ii) is 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 that is the subject of the warrant in Subsection (1)(a).

(c) A law enforcement agency 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 warrant if the law enforcement agency reasonably believes that the transmitted data is necessary to achieve the objective of the warrant.

(d) The electronic information or data described in Subsection (1)(b) shall be destroyed in an unrecoverable manner by the law enforcement agency as soon as reasonably possible after the electronic information or data is collected.

(2)

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

(i) in an emergency situation that involves the imminent risk of death or serious bodily injury to the owner of the electronic device, to be able to locate and help the person in need;

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

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

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

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

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

A) 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

B) 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, sexual abuse, or dishonesty.

(b) 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 warrant:

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

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

(iii) in connection with a report forwarded by the National Center for Missing and Exploited Children under 18 U.S.C. Sec. 2258A; or

(iv) subject to Subsection 77-23c-102(2)(a)(vi)(B), from a remote computing service provider if the remote computing service provider voluntarily discloses the stored or transmitted data as otherwise permitted under 18 U.S.C. Sec. 2702.

(3) An electronic communication service provider or 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 the warrant issued under this section or without a warrant in accordance with Subsection (2).

(4) Nothing in this chapter limits or affects the disclosure of public records under state open record laws.

Section 3. Notification

(1)

(a) Except as provided in Subsection (2), a law enforcement agency that executes a warrant pursuant to this chapter shall, within 14 days after the day on which the electronic information or data that is the subject of the warrant is obtained by the law enforcement agency, issue a notification to the owner of the electronic device or electronic information or data specified in the warrant that states:

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

(ii) the kind of warrant issued;

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

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

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

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

(b) The notification requirement under Subsection (1)(a) is not triggered until the owner of the electronic device or electronic information or data specified in the warrant is known, or could be reasonably identified, by the law enforcement agency.

(2) A law enforcement agency seeking a warrant pursuant to this chapter may submit a request, and the court may grant permission, to delay the notification required by Subsection (1) for a period not to exceed 30 days, if the court determines that there is reasonable cause to believe that 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) intimidate a potential witness; or
    (e) otherwise seriously jeopardize an investigation or unduly delay a trial.

(3)
    (a) When a delay of notification is granted under Subsection (2) and upon application by the law enforcement agency, the court may grant additional extensions of up to 30 days each.
    (b) Notwithstanding Subsection (3)(a), when a delay of notification is granted under Subsection (2), and upon application by a law enforcement agency, the court may grant an additional extension of up to 60 days if the court determines that a delayed notification is justified because the investigation involving the warrant:
        (i) is interstate in nature and sufficiently complex; or
        (ii) is likely to extend up to or beyond an additional 60 days.

(4) Upon expiration of the period of delayed notification granted under Subsection (2) or (3), 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 together with notice that:
    (a) states with reasonable specificity the nature of the law enforcement inquiry; and
    (b) contains:
        (i) the information described in Subsections (1)(a)(i) through (vi);
        (ii) a statement that notification of the search was delayed;
        (iii) the name of the court that authorized the delay of notification; and
        (iv) a reference to the provision of this chapter that allowed the delay of notification.

(5) 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 4. Third-party data

(1) A law enforcement agency may not obtain, use, copy, or disclose a subscriber record unless a subpoena or warrant has been obtained.

(2) A law enforcement agency may not obtain, use, copy, or disclose, for a criminal investigation or prosecution, any record or information, other than a subscriber record, of a provider of an electronic communication service or remote computing service related to a subscriber or customer without a warrant.

(3) Notwithstanding Subsections (1) and (2), a law enforcement agency may obtain, use, copy, or disclose a subscriber record, or other record or information related to a subscriber or customer, without a warrant:
    (a) with the informed, affirmed consent of the subscriber or customer;
    (b) in accordance with a judicially recognized exception to warrant requirements;

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

(d) if the provider of an electronic communication service or remote computing service voluntarily discloses the record:

(i) under a belief that an emergency exists involving the imminent risk to an individual of:

A) death;

B) serious physical injury;

C) sexual abuse;

D) live-streamed sexual exploitation;

E) kidnapping; or

F) human trafficking; or

(ii) that is inadvertently discovered by the provider, if the record appears to pertain to the commission of:

A) a felony; or

B) a misdemeanor involving physical violence, sexual abuse, or dishonesty.

(4) A provider of an electronic communication service or remote computing service, or 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 warrant issued under this section, or without a warrant in accordance with Subsection (2).

Section 5. Exclusion of Records

(1) All electronic information or data and records of a provider of an electronic communications service or remote computing service pertaining to a subscriber or customer that are obtained in violation of the provisions of this chapter shall be subject to the rules governing exclusion as if the records were obtained in violation of the Fourth Amendment to the United States Constitution and [*insert your state constitution's equivalent provision*].

To learn more about this model language, please contact Rees Empey at rees@libertasutah.org