2023 -- S 0396

========
LC000948
========

S T A T E O F R H O D E I S L A N D

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2023

_____

A N A C T

RELATING TO CRIMINAL PROCEDURE -- ELECTRONIC INFORMATION AND DATA PRIVACY ACT

Introduced By: Senators de la Cruz, Rogers, F. Lombardi, Ciccone, Felag, E Morgan, Bell, Raptakis, DeLuca, and Burke
Date Introduced: February 16, 2023

Referred To: Senate Judiciary

It is enacted by the General Assembly as follows:

SECTION 1. Title 12 of the General Laws entitled "CRIMINAL PROCEDURE" is hereby amended by adding thereto the following chapter:

CHAPTER 34

ELECTRONIC INFORMATION AND DATA PRIVACY ACT

12-34-1. Short title.

This chapter shall be known and may be cited as the "Electronic Information and Data Privacy Act".

12-34-2. Definitions.

As used in this chapter:

(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) "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, photo-electronic, or photo-optical system:

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

(ii) "Electronic information or data" does not include:

(A) A wire or oral communication;

(B) A 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 money.

(4) "Law enforcement agency" means an entity of the state or a political subdivision of the state including any municipality within the state, or any agency acting on their behalf, that exists primarily to 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 from 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) "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.

(8) "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communication system.

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

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

(ii) An electronic device to a nearby antenna.

(10) "Wire communications" 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 the connection in a switching station) furnished or operated by any person engaged in providing or operating the facilities for the transmission of communications. The term includes any electronic storage of the communication.

12-34-3. Electronic information or data privacy-Warrant required for disclosure.

(a) Except as provided in subsection (e) of this section, for a criminal investigation or prosecution, a law enforcement agency may not obtain, without a search warrant issued by a court upon a finding of probable cause:

(1) The location information, stored data, or transmitted data of an electronic device; or

(2) 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 (d) of this section, 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:

(1) Is not the subject of the warrant; and

(2) 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 described in subsection (a) of this section.

(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 (b) of this section shall be destroyed in an unrecoverable manner by the law enforcement agency as soon as reasonably possible after the electronic information is collected.

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

(1) If the device is reported stolen by the owner;

(2) With the informed, affirmative consent of the owner or user of the electronic device;

(3) In accordance with a judicially recognized exception to the warrant requirement;

(4) If the owner has voluntarily and publicly disclosed the location information; or

(5) From the remote computing service provider if the remote computing service provider voluntarily discloses the 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, sexual abuse, or dishonesty.

(f) 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:

(1) With the informed consent of the owner of the electronic device or electronic information or data;

(2) In accordance with a judicially recognized exception to the warrant requirement;

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

(4) From the remote computing service provider if the remote computing service provider voluntarily discloses the 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, sexual abuse, or dishonesty.

(g) A prosecutor, may obtain a judicial order based on a finding of probable cause, consistent with 18 U.S.C. § 2703 and 18 U.S.C. § 2702, to the electronic communications system or service or remote computing service provider that owns or controls the Internet protocol address, websites, email address, or service to a specific telephone number, requiring the production of the following information, if available, upon providing in the court order the Internet protocol address, email address, telephone number, or other identifier, and the dates and times the address, telephone number, or other identifier suspected of being used in the commission of the offense;

(1) Names of subscribers, service customers, and users;

(2) Addresses of subscribers, service customers, and users;

(3) Records of session times and durations;

(4) Length of service, including the start date and types of service utilized; and

(5) Telephone or other instrument subscriber numbers or other subscriber identifiers, including any temporarily assigned network address.

(h) An electronic communication service provider or remote computing service provider, their officers, agents, employees or other specified individuals acting pursuant to and in accordance with the provisions of this chapter, may not be held liable for providing information, facilities, or assistance in good faith reliance on the terms of the warrant or without a warrant in accordance with subsections (e) and (f) of this section.

(i) Nothing in this chapter affects the provisions of chapter 2 of title 38, (access to public records act,) or limits or affects the rights of an employer to voluntarily provide location

information, stored or transmitted data from an electronic device, or electronic information or data transmitted by an employee utilizing an electronic device owned by the employer.

12-34-4. Notification required - Delayed notification.

(a) Except as provided in subsection (b) of this section, a law enforcement agency that executes a warrant pursuant to this chapter, shall, within fourteen (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 includes the following information:

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

(2) The kind 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 or magistrate who issued the warrant.

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

(c) A law enforcement agency seeking a warrant pursuant to this chapter may submit a request, and the court may grant permission, to delay notification required by subsection (a) of this section for a period not to exceed thirty (30) days, if the court determines that there is reasonable cause to believe that the notification may:

(1) Endanger the life or physical safety of an individual;

(2) Cause a person to flee from prosecution;

(3) Lead to the destruction of evidence;

(4) Intimidate a potential witness; or

(5) Otherwise seriously jeopardize an investigation or unduly delay a trial.

(d) When a delay of notification is granted under subsection (c) of this section and upon application by the law enforcement agency, the court may grant additional extensions of up to thirty (30) days each.

(e) Notwithstanding subsection (d) of this section, when a delay of notification is granted under subsection (c) of this section, and upon application by a law enforcement agency, the court may grant an additional extension of up to sixty (60) days if the court determines that a delayed notification is justified because the investigation involving the warrant:

(1) Is interstate in nature and sufficiently complex; or

(2) Is likely to extend up to or beyond an additional sixty (60) days.

(f) Upon expiration of the period of delayed notification granted under subsections (c) or (d) of this section, 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:

(1) States with reasonable specificity the nature of the law enforcement inquiry including:

(i) The information described in subsection (a) of this section;

(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.

(g) 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.

12-34-5. Third-party electronic information or data.

(a) As used in this section, "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:

(1) Name;

(2) Address;

(3) Local and long distance telephone connection record, or record of session time and duration;

(4) Length of service, including the start date;

(5) Type of service used;

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

(7) Means and source of payment for the service, including credit card or bank account numbers.

(b) Except for purposes of grand jury testimony or use at trial after indictment, a law enforcement agency may not obtain, use, copy or disclose a subscriber record.

(c) 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.

(d) Notwithstanding subsections (b) and (c) of this section, 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:

(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 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;

(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; or

(iii) Subject to subsection (d) of this section, as otherwise permitted under 18 U.S.C. § 2702.

(e) A provider of an electronic communication service or remote computing service, or the provider's officers, 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 (d) of this section.

12-34-6. Exclusion of records.

All electronic information or data and records of a provider of an electronic communication 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 Article 1, Section 6 of the Rhode Island Constitution.

SECTION 2. This act shall take effect upon passage.

========
LC000948
========

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO CRIMINAL PROCEDURE -- ELECTRONIC INFORMATION AND DATA PRIVACY ACT

***

This act would require law enforcement agencies to obtain search warrants for electronic information, data, location information and other identifying information of subscribers and customers, except in specified circumstances.

This act would take effect upon passage.

========
LC000948
========