

## HB0057S03 compared with HB0057S01

~~{deleted text}~~ shows text that was in HB0057S01 but was deleted in HB0057S03.

Inserted text shows text that was not in HB0057S01 but was inserted into HB0057S03.

**DISCLAIMER:** This document is provided to assist you in your comparison of the two bills. Sometimes this automated comparison will NOT be completely accurate. Therefore, you need to read the actual bills. This automatically generated document could contain inaccuracies caused by: limitations of the compare program; bad input data; or other causes.

Representative Craig Hall proposes the following substitute bill:

### ELECTRONIC INFORMATION OR DATA PRIVACY

2019 GENERAL SESSION

STATE OF UTAH

**Chief Sponsor: Craig Hall**

Senate Sponsor: \_\_\_\_\_

---

#### LONG TITLE

##### General Description:

This bill modifies provisions related to privacy of electronic information or data.

##### Highlighted Provisions:

This bill:

- ▶ defines terms;
- ▶ requires issuance of a search warrant to obtain certain electronic information or data;
- ▶ addresses notification that electronic information or data was obtained;
- ▶ provides for transmission of electronic information or data to a remote computing service, including restrictions on government entities;
- ▶ provides that the individual who transmits electronic information or data is the presumed owner of the electronic information or data;

## HB0057S03 compared with HB0057S01

- ▶ provides ~~{that}~~ for the exclusion of electronic information or data obtained without a ~~{search}~~ warrant ~~{is inadmissible in any criminal proceeding}~~; and
- ▶ makes technical and conforming amendments.

### Money Appropriated in this Bill:

None

### Other Special Clauses:

None

### Utah Code Sections Affected:

AMENDS:

~~{~~ ~~77-23b-4~~, as last amended by Laws of Utah 2012, Chapter 115

~~}~~ 77-23c-102, as last amended by Laws of Utah 2016, Chapter 161

77-23c-103, as enacted by Laws of Utah 2014, Chapter 223

ENACTS:

77-23c-101.1, Utah Code Annotated 1953

77-23c-104, Utah Code Annotated 1953

77-23c-105, Utah Code Annotated 1953

RENUMBERS AND AMENDS:

77-23c-101.2, (Renumbered from 77-23c-101, as enacted by Laws of Utah 2014, Chapter 223)

---

*Be it enacted by the Legislature of the state of Utah:*

Section 1. Section ~~{77-23b-4}~~ 77-23c-101.1 is ~~{amended to read:~~

~~77-23b-4. Disclosure by a provider -- Grounds for requiring disclosure -- Court order:~~

~~(1) A government entity may only require the disclosure by a provider of electronic communication services of the contents of an electronic communication that is in electronic storage in an electronic communication system pursuant to a warrant issued under the Utah Rules of Criminal Procedure or an equivalent federal warrant.~~

~~(2) Subsection (1) applies to any electronic communication that is held or maintained on that service:~~

~~(a) on behalf of and received by means of electronic transmission from or created by~~

## HB0057S03 compared with HB0057S01

~~means of computer processing of communications received by means of electronic transmission from a subscriber or customer of the remote computing service; and~~

~~—— (b) solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any communication for purposes of providing any services other than storage or computer processing:~~

~~—— (3) (a) (i) Except under Subsection (3)(a)(ii), a provider of electronic communication services or remote computing services may disclose a record or other information pertaining to a subscriber to or customer of the service, not including the contents of communication covered by Subsection (1), to any person other than a governmental agency.~~

~~—— (ii) A provider of electronic communication services or remote computing services shall disclose a record or other information pertaining to a subscriber to or customer of the service, not including the contents of communication covered by Subsection (1), to a governmental entity only when the entity:~~

~~—— [(A) uses an administrative subpoena authorized by a state or federal statute or a state or federal grand jury subpoena;]~~

~~—— [(B)] (A) obtains a warrant issued under the Utah Rules of Criminal Procedure or an equivalent federal warrant;~~

~~—— [(C)] (B) obtains a court order for the disclosure under Subsection (4); or~~

~~—— [(D)] (C) has the consent of the subscriber or customer to the disclosure.~~

~~—— (b) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.~~

~~—— (4) (a) A court order for disclosure under this section may be issued only if the governmental entity shows there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry.~~

~~—— (b) A court issuing an order under this section, on a motion made promptly by the service provider, may quash or modify the order, if the information or records requested are unusually voluminous in nature or compliance with the order otherwise would cause an undue burden on the provider.~~

~~—— (5) A cause of action may not be brought in any court against any provider of wire or~~

## HB0057S03 compared with HB0057S01

~~electronic communications services, [its] or the provider's officers, employees, agents, or other specified persons, for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.~~

~~Section 2. Section 77-23c-101.1 is enacted to read:~~

~~enacted to read:~~

### CHAPTER 23c. ELECTRONIC INFORMATION OR DATA PRIVACY ACT

#### 77-23c-101.1. Title.

This chapter is known as the "Electronic Information or Data Privacy Act."

Section ~~{3}~~2. Section **77-23c-101.2**, which is renumbered from Section 77-23c-101 is renumbered and amended to read:

#### ~~[77-23c-101].~~ **77-23c-101.2. 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) "Government entity" means the state, a county, a municipality, a higher education institution, a local district, a special service district, or any other political subdivision of the state or an administrative subunit of any political subdivision, including a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission, or an individual acting or purporting to act for or on behalf of a state or local agency.

~~(3)4~~ (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 ~~an~~:

(i) a wire or oral communication ~~or~~;

(ii) a communication made through a tone-only paging device ~~f~~.

~~(3)4~~ (4) "Government entity" means the state, a county, a municipality, a higher

## HB0057S03 compared with HB0057S01

~~education institution, a local district, a special service district, or any other}; or~~

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

(5) "Law enforcement agency" means an entity of the state or a political subdivision of the state ~~for an administrative subunit of any political subdivision, including a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission, or an individual acting or purporting to act for or on behalf of a state or local agency.~~

~~— [(4)] (5) that exists to primarily prevent, detect, or prosecute crime and enforce criminal statutes or ordinances.~~

[(4)] (6) "Location information" means information 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.

[(5)] (6;7) "Location information service" means the provision of a global positioning service or other mapping, location, or directional information service.

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

[(6)] (7;9) "Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

~~(8) "Service provider" means a provider of:~~

~~— (a) an electronic communication service; or~~

~~— (b) a remote computing service.~~

~~— Section 4}10) "Wire communication" means the same as that term is defined in Section 77-23a-3.~~

Section 3. Section 77-23c-102 is amended to read:

**77-23c-102. Electronic information or data privacy -- Warrant required for disclosure.**

(1) (a) Except as provided in Subsection (2) ~~[, a government entity],~~ 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 ~~[without a search warrant issued by a court upon probable cause.]; or~~

## HB0057S03 compared with HB0057S01

(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 [government entity] law enforcement agency may not use, copy, or disclose, for any purpose, the location information, stored data, ~~[or]~~ transmitted data of an electronic device, or electronic information or data provided by a remote computing service provider, that ~~[is not the subject of the warrant that is collected as part of an effort to obtain the { } location { } electronic information { }, stored data, { } or { } transmitted { } data { } of the electronic device { } that is the subject of the warrant in Subsection (1)(a).~~

~~(c) A } ]:~~

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

(ii) is incidentally 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 [government entity] law enforcement agency may use, copy, or disclose the transmitted ~~{ electronic information or }~~ data of an electronic device used to communicate with the electronic device that is the subject of the warrant if the [government entity] law enforcement agency reasonably believes that the transmitted ~~{ electronic information or }~~ 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 [government entity] law enforcement agency as soon as reasonably possible after the electronic information or data is collected.

(2) (a) A [government entity] law enforcement agency may obtain location information without a warrant for an electronic device:

(i) in accordance with Section 53-10-104.5;

(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 [exceptions] exception to warrant requirements; ~~[or]~~

(v) if the owner has voluntarily and publicly disclosed the location information ~~.~~

## HB0057S03 compared with HB0057S01

~~(b)~~ ~~(c)~~; 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 or sexual violence, or deception.

(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; or

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

~~(b)~~ (c) A prosecutor may obtain a judicial order as ~~defined~~ described in Section 77-22-2.5 for the purposes enumerated in Section 77-22-2.5.

(3) ~~ff~~ An electronic communication service provider ~~[, its]~~ or remote computing service provider, ~~ffits~~ the ~~service~~ provider's officers, employees, agents, or other specified persons may not be held liable for providing information, facilities, or assistance in ~~[accordance with]~~ good faith reliance on the terms of the warrant issued under this section or without a warrant ~~[pursuant to]~~ in accordance with Subsection (2).

(4) (a) Notwithstanding Subsections (1) ~~[through (3)]~~ and (2), a government entity may receive and ~~[utilize]~~ use electronic information or data containing the location information of an electronic device from a non-government entity ~~[as long as]~~ if the electronic information or data contains no information that includes, or may reveal, the identity of an individual.

(b) Electronic information or data collected in accordance with this ~~[subsection]~~ Subsection (4) may not be used for investigative or prosecutorial purposes by a law enforcement agency.

(5) Nothing in this chapter limits or affects the disclosure of public records under Title 63G, Chapter 2, Government Records Access and Management Act.

## HB0057S03 compared with HB0057S01

Section ~~{5}~~4. Section 77-23c-103 is amended to read:

### 77-23c-103. Notification required -- Delayed notification.

(1) Except as provided in Subsection (2), a ~~[government entity]~~ law enforcement agency that executes a warrant pursuant to Subsection 77-23c-102(1)(a) or 77-23c-104(~~{4}~~)(a)~~{3}~~ shall, within 14 days after the day on which the ~~[operation concludes]~~ 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:

- (a) that a warrant was applied for and granted;
- (b) the kind of warrant issued;
- (c) the period of time during which the collection of the electronic information or data ~~[from the electronic device]~~ was authorized;
- (d) the offense specified in the application for the warrant;
- (e) the identity of the ~~[government entity]~~ law enforcement agency that filed the application; and
- (f) the identity of the judge who issued the warrant.

(2) A ~~[government entity]~~ law enforcement agency seeking a warrant pursuant to Subsection 77-23c-102(1)(a) or 77-23c-104(~~{4}~~)(a)~~{3}~~ 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 probable 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) When a delay of notification is granted under Subsection (2) and upon application by the ~~[government entity]~~ law enforcement agency, the court may grant additional extensions of up to 30 days each.

(4) Upon expiration of the period of delayed notification granted under Subsection (2) or (3), the ~~[government entity]~~ 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



## HB0057S03 compared with HB0057S01

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) through (f);

(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 ~~[government entity]~~ 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 ~~{6}~~5. Section **77-23c-104** is enacted to read:

### **77-23c-104. Third party electronic information or data.**

(1) As used in this section, "~~{collected data} means electronic information or data:~~

~~— (a) received or stored by a service provider; or~~

~~— (b) (i) that reveals a person's interaction with or use}~~ 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

~~(iii)g) {is generated by a service provider in the course of a person's use of a server owned or operated by the service provider.~~

~~— (2) An individual who transmits electronic information or data to a service provider is presumed to be the owner of the electronic information or data.~~

~~— (3) Except as provided}~~ means and source of payment for the service, including a credit card or bank account number.

## HB0057S03 compared with HB0057S01

(2) Except as described in Chapter 22, Subpoena Powers for Aid of Criminal Investigation and Grants of Immunity, including the requirements described in {Subsection 34-48-202(1)(c), the individual in Subsection (2) maintains a reasonable expectation of privacy in collected data.

~~—— (4) (a) Pursuant to Subsection 77-23c-102(1), a government entity} Subsections 77-22-2(a) and (b), a law enforcement agency may not obtain, use, copy, or disclose a {person's collected data without first obtaining} subscriber record.~~

(3) 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.

~~({b}4) Notwithstanding {Subsection} Subsections ({4}2) and ({a}3), a {government entity} law enforcement agency may obtain, use, copy, or disclose a {person's collected data} subscriber record without a warrant:~~

~~({i}a) with the informed, {affirmative} affirmed consent of the {owner of the collected data} subscriber or customer}; {or}~~

~~({ii}b) in accordance with a judicially recognized {exceptions} exception to warrant requirements {.~~

~~—— (5) Electronic};~~

(c) if the subscriber or customer voluntarily discloses the subscriber 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 subscriber 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

## HB0057S03 compared with HB0057S01

(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 or sexual violence, or deception.

(5) 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 (3).

(6) Nothing in this chapter affects the rights of an employer under Subsection 34-48-202(1)(e) or an administrative rule adopted under Section 63F-1-206.

Section 6. Section 77-23c-105 is enacted to read:

### 77-23c-105. Exclusion of records.

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 ~~Subsection (4) is inadmissible in any criminal proceeding.~~ the provisions of this chapter shall be excluded as if the records were obtained in violation of the Fourth Amendment to the United States Constitution and Utah Constitution, Article I, Section 14.