

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;
- ▶ provides for the exclusion of electronic information or data obtained without a warrant; and
- ▶ makes technical and conforming amendments.

Money Appropriated in this Bill:

None

Other Special Clauses:



26 None

27 **Utah Code Sections Affected:**

28 AMENDS:

29 **77-23c-102**, as last amended by Laws of Utah 2016, Chapter 161

30 **77-23c-103**, as enacted by Laws of Utah 2014, Chapter 223

31 ENACTS:

32 **77-23c-101.1**, Utah Code Annotated 1953

33 **77-23c-104**, Utah Code Annotated 1953

34 **77-23c-105**, Utah Code Annotated 1953

35 RENUMBERS AND AMENDS:

36 **77-23c-101.2**, (Renumbered from 77-23c-101, as enacted by Laws of Utah 2014,
37 Chapter 223)



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

40 Section 1. Section **77-23c-101.1** is enacted to read:

41 **CHAPTER 23c. ELECTRONIC INFORMATION OR DATA PRIVACY ACT**

42 **77-23c-101.1. Title.**

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

44 Section 2. Section **77-23c-101.2**, which is renumbered from Section 77-23c-101 is
45 renumbered and amended to read:

46 ~~**77-23c-101.**~~ **77-23c-101.2. Definitions.**

47 As used in this chapter:

48 (1) "Electronic communication service" means a service that provides to users of the
49 service the ability to send or receive wire or electronic communications.

50 (2) "Electronic device" means a device that enables access to or use of an electronic
51 communication service, remote computing service, or location information service.

52 (3) "Government entity" means the state, a county, a municipality, a higher education
53 institution, a local district, a special service district, or any other political subdivision of the
54 state or an administrative subunit of any political subdivision, including a law enforcement
55 entity or any other investigative entity, agency, department, division, bureau, board, or
56 commission, or an individual acting or purporting to act for or on behalf of a state or local

57 agency.

58 (4) (a) "Electronic information or data" means information or data including a sign,
59 signal, writing, image, sound, or intelligence of any nature transmitted or stored in whole or in
60 part by a wire, radio, electromagnetic, photoelectronic, or photooptical system.

61 (b) "Electronic information or data" includes the location information, stored data, or
62 transmitted data of an electronic device.

63 (c) "Electronic information or data" does not include:

64 (i) a wire or oral communication;

65 (ii) a communication made through a tone-only paging device; or

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

68 (5) "Law enforcement agency" means an entity of the state or a political subdivision of
69 the state that exists to primarily prevent, detect, or prosecute crime and enforce criminal
70 statutes or ordinances.

71 ~~[(4)]~~ (6) "Location information" means information concerning the location of an
72 electronic device that, in whole or in part, is generated or derived from or obtained by the
73 operation of an electronic device.

74 ~~[(5)]~~ (7) "Location information service" means the provision of a global positioning
75 service or other mapping, location, or directional information service.

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

77 ~~[(6)]~~ (9) "Remote computing service" means the provision to the public of computer
78 storage or processing services by means of an electronic communications system.

79 (10) "Wire communication" means the same as that term is defined in Section
80 [77-23a-3](#).

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

82 **77-23c-102. Electronic information or data privacy -- Warrant required for**
83 **disclosure.**

84 (1) (a) Except as provided in Subsection (2) ~~[, a government entity]~~, for a criminal
85 investigation or prosecution, a law enforcement agency may not obtain, without a search
86 warrant issued by a court upon probable cause:

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

88 ~~[without a search warrant issued by a court upon probable cause.]; or~~

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

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

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

98 (ii) is ~~H~~→ **[incidentally]** ←~~H~~ collected as part of an effort to obtain the location
98a information,
99 stored data, transmitted data of an electronic device, or electronic information or data provided
100 by a remote computing service provider that is the subject of the warrant in Subsection (1)(a).

101 (c) A ~~[government entity]~~ law enforcement agency may use, copy, or disclose the
102 transmitted data of an electronic device used to communicate with the electronic device that is
103 the subject of the warrant if the ~~[government entity]~~ law enforcement agency reasonably
104 believes that the transmitted data is necessary to achieve the objective of the warrant.

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

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

110 (i) in accordance with Section [53-10-104.5](#);

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

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

114 (iv) in accordance with a judicially recognized ~~[exceptions]~~ exception to warrant
115 requirements; ~~[or]~~

116 (v) if the owner has voluntarily and publicly disclosed the location information~~[-]; or~~

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

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

122 (B) that is inadvertently discovered by the remote computing service provider and
123 appears to pertain to the commission of a felony, or of a misdemeanor involving physical or
124 sexual violence, or deception.

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

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

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

131 ~~[(b)]~~ (c) A prosecutor may obtain a judicial order as ~~[defined]~~ described in Section
132 77-22-2.5 for the purposes enumerated in Section 77-22-2.5.

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

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

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

145 (5) Nothing in this chapter limits or affects the disclosure of public records under Title
146 63G, Chapter 2, Government Records Access and Management Act.

147 Section 4. Section **77-23c-103** is amended to read:

148 **77-23c-103. Notification required -- Delayed notification.**

149 (1) Except as provided in Subsection (2), a ~~[government entity]~~ law enforcement

150 agency that executes a warrant pursuant to Subsection 77-23c-102(1)(a) or 77-23c-104(3) shall,
151 within 14 days after the day on which the [~~operation concludes~~] electronic information or data
152 that is the subject of the warrant is obtained by the law enforcement agency, issue a notification
153 to the owner of the electronic device or electronic information or data specified in the warrant
154 that states:

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

163 (2) A [~~government entity~~] law enforcement agency seeking a warrant pursuant to
164 Subsection 77-23c-102(1)(a) or 77-23c-104(3) may submit a request, and the court may grant
165 permission, to delay the notification required by Subsection (1) for a period not to exceed 30
166 days, if the court determines that there is probable cause to believe that the notification may:

- 167 (a) endanger the life or physical safety of an individual;
- 168 (b) cause a person to flee from prosecution;
- 169 (c) lead to the destruction of or tampering with evidence;
- 170 (d) intimidate a potential witness; or
- 171 (e) otherwise seriously jeopardize an investigation or unduly delay a trial.

172 (3) When a delay of notification is granted under Subsection (2) and upon application
173 by the [~~government entity~~] law enforcement agency, the court may grant additional extensions
174 of up to 30 days each.

175 (4) Upon expiration of the period of delayed notification granted under Subsection (2)
176 or (3), the [~~government entity~~] law enforcement agency shall serve upon or deliver by
177 first-class mail, or by other means if delivery is impracticable, to the owner of the electronic
178 device or electronic information or data a copy of the warrant together with notice that:

- 179 (a) states with reasonable specificity the nature of the law enforcement inquiry; and
- 180 (b) contains:

- 181 (i) the information described in Subsections (1)(a) through (f);
- 182 (ii) a statement that notification of the search was delayed;
- 183 (iii) the name of the court that authorized the delay of notification;
- 184 (iv) a reference to the provision of this chapter that allowed the delay of notification.
- 185 (5) A ~~[government entity]~~ law enforcement agency is not required to notify the owner
- 186 of the electronic device or electronic information or data if the owner is located outside of the
- 187 United States.

188 Section 5. Section **77-23c-104** is enacted to read:

189 **77-23c-104. Third party electronic information or data.**

190 (1) As used in this section, "subscriber record" means a record or information of a

191 provider of an electronic communication service or remote computing service that reveals the

192 subscriber's or customer's:

- 193 (a) name;
- 194 (b) address;
- 195 (c) local and long distance telephone connection record, or record of session time and
- 196 duration;
- 197 (d) length of service, including the start date;
- 198 (e) type of service used;
- 199 (f) telephone number, instrument number, or other subscriber or customer number or
- 200 identification, including a temporarily assigned network address; and
- 201 (g) means and source of payment for the service, including a credit card or bank
- 202 account number.

203 (2) Except as described in Chapter 22, Subpoena Powers for Aid of Criminal

204 Investigation and Grants of Immunity, including the requirements described in Subsections

205 77-22-2(a) and (b), a law enforcement agency may not obtain, use, copy, or disclose a

206 subscriber record.

207 (3) A law enforcement agency may not obtain, use, copy, or disclose, for a criminal

208 investigation or prosecution, any record or information, other than a subscriber record, of a

209 provider of an electronic communication service or remote computing service related to a

210 subscriber or customer without a warrant.

211 (4) Notwithstanding Subsections (2) and (3), a law enforcement agency may obtain,

212 use, copy, or disclose a subscriber record without a warrant:

213 (a) with the informed, affirmed consent of the subscriber or customer;

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

215 (c) if the subscriber or customer voluntarily discloses the subscriber record in a manner

216 that is publicly accessible; or

217 (d) if the provider of an electronic communication service or remote computing service

218 voluntarily discloses the subscriber record:

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

220 of:

221 (A) death;

222 (B) serious physical injury;

223 (C) sexual abuse;

224 (D) live-streamed sexual exploitation;

225 (E) kidnapping; or

226 (F) human trafficking; or

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

228 the commission of:

229 (A) a felony; or

230 (B) a misdemeanor involving physical or sexual violence, or deception.

231 (5) A provider of an electronic communication service or remote computing service, or

232 the provider's officers, employees, agents, or other specified persons may not be held liable for

233 providing information, facilities, or assistance in good faith reliance on the terms of a warrant

234 issued under this section, or without a warrant in accordance with Subsection (3).

235 (6) Nothing in this chapter affects the rights of an employer under Subsection

236 [34-48-202\(1\)\(e\)](#) or an administrative rule adopted under Section [63F-1-206](#).

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

238 **77-23c-105. Exclusion of records.**

239 All electronic information or data and records of a provider of an electronic

240 communications service or remote computing service pertaining to a subscriber or customer

241 that are obtained in violation of the provisions of this chapter shall be excluded ~~it~~ **subject to the**

241a **rules governing exclusion** ~~it~~ as if the records

242 were obtained in violation of the Fourth Amendment to the United States Constitution and

243 Utah Constitution, Article I, Section 14.