

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: Todd Weiler

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 changes.

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 (3) (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 (4) "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)]~~ (5) "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)]~~ (6) "Location information service" means the provision of a global positioning
 75 service or other mapping, location, or directional information service.

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

77 ~~[(6)]~~ (8) "Remote computing service" means the provision to the public of computer
 78 storage or processing services by means of an electronic communications system.

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

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

81 **77-23c-102. Electronic information or data privacy -- Warrant required for**
 82 **disclosure.**

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

86 (i) the location information, stored data, or transmitted data of an electronic device
 87 ~~[without a search warrant issued by a court upon probable cause.];~~ or

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

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

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

97 (ii) is collected as part of an effort to obtain the location information, stored data,
98 transmitted data of an electronic device, or electronic information or data provided by a remote
99 computing service provider that is the subject of the warrant in Subsection (1)(a).

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

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

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

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

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

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

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

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

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

118 (A) under a belief that an emergency exists involving an imminent risk to an individual

119 of death, serious physical injury, sexual abuse, live-streamed sexual exploitation, kidnapping,
120 or human trafficking; or

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

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

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

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

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

132 ~~[(b)]~~ (c) A prosecutor may obtain a judicial order as [defined] described in Section
133 77-22-2.5 for the purposes enumerated in Section 77-22-2.5.

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

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

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

145 (4) 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 (5) Nothing in this chapter affects the rights of an employer under Subsection
148 34-48-202(1)(e) or an administrative rule adopted under Section 63F-1-206.

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

150 **77-23c-103. Notification required -- Delayed notification.**

151 (1) (a) Except as provided in Subsection (2), a ~~[government entity]~~ law enforcement
152 agency that executes a warrant pursuant to Subsection 77-23c-102(1)(a) or 77-23c-104(3) shall,
153 within 14 days after the day on which the ~~[operation concludes]~~ electronic information or data
154 that is the subject of the warrant is obtained by the law enforcement agency, issue a notification
155 to the owner of the electronic device or electronic information or data specified in the warrant
156 that states:

157 ~~[(a)]~~ (i) that a warrant was applied for and granted;

158 ~~[(b)]~~ (ii) the kind of warrant issued;

159 ~~[(c)]~~ (iii) the period of time during which the collection of the electronic information or
160 data ~~[from the electronic device]~~ was authorized;

161 ~~[(d)]~~ (iv) the offense specified in the application for the warrant;

162 ~~[(e)]~~ (v) the identity of the ~~[government entity]~~ law enforcement agency that filed the
163 application; and

164 ~~[(f)]~~ (vi) the identity of the judge who issued the warrant.

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

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

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

174 (b) cause a person to flee from prosecution;

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

176 (d) intimidate a potential witness; or

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

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

181 (b) Notwithstanding Subsection (3)(a), when a delay of notification is granted under
182 Subsection (2), and upon application by a law enforcement agency, the court may grant an
183 additional extension of up to 60 days if the court determines that a delayed notification is
184 justified because the investigation involving the warrant:

185 (i) is interstate in nature and sufficiently complex; or

186 (ii) is likely to extend up to or beyond an additional 60 days.

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

191 (a) states with reasonable specificity the nature of the law enforcement inquiry; and

192 (b) contains:

193 (i) the information described in Subsections (1)(a)(i) through [~~(v)~~] (vi);

194 (ii) a statement that notification of the search was delayed;

195 (iii) the name of the court that authorized the delay of notification; and

196 (iv) a reference to the provision of this chapter that allowed the delay of notification.

197 (5) A [~~government entity~~] law enforcement agency is not required to notify the owner
198 of the electronic device or electronic information or data if the owner is located outside of the
199 United States.

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

201 **77-23c-104. Third party electronic information or data.**

202 (1) As used in this section, "subscriber record" means a record or information of a
203 provider of an electronic communication service or remote computing service that reveals the
204 subscriber's or customer's:

205 (a) name;

206 (b) address;

207 (c) local and long distance telephone connection record, or record of session time and
208 duration;

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

210 (e) type of service used;

211 (f) telephone number, instrument number, or other subscriber or customer number or

212 identification, including a temporarily assigned network address; and

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

215 (2) Except as provided in Chapter 22, Subpoena Powers for Aid of Criminal
216 Investigation and Grants of Immunity, a law enforcement agency may not obtain, use, copy, or
217 disclose a subscriber record.

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

222 (4) Notwithstanding Subsections (2) and (3), a law enforcement agency may obtain,
223 use, copy, or disclose a subscriber record, or other record or information related to a subscriber
224 or customer, without a warrant:

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

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

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

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

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

233 (A) death;

234 (B) serious physical injury;

235 (C) sexual abuse;

236 (D) live-streamed sexual exploitation;

237 (E) kidnapping; or

238 (F) human trafficking; or

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

241 (A) a felony; or

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

243 (5) A provider of an electronic communication service or remote computing service, or
244 the provider's officers, employees, agents, or other specified persons may not be held liable for
245 providing information, facilities, or assistance in good faith reliance on the terms of a warrant
246 issued under this section, or without a warrant in accordance with Subsection (3).

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

248 **77-23c-105. Exclusion of records.**

249 All electronic information or data and records of a provider of an electronic
250 communications service or remote computing service pertaining to a subscriber or customer
251 that are obtained in violation of the provisions of this chapter shall be subject to the rules
252 governing exclusion as if the records were obtained in violation of the Fourth Amendment to
253 the United States Constitution and Utah Constitution, Article I, Section 14.