

Amendment No. 1

COMMITTEE/SUBCOMMITTEE ACTION

ADOPTED	_____	(Y/N)
ADOPTED AS AMENDED	_____	(Y/N)
ADOPTED W/O OBJECTION	_____	(Y/N)
FAILED TO ADOPT	_____	(Y/N)
WITHDRAWN	_____	(Y/N)
OTHER		

1 Committee/Subcommittee hearing bill: Criminal Justice
2 Subcommittee

3 Representative Rodrigues, R. offered the following:

Amendment (with title amendment)

6 Remove everything after the enacting clause and insert:

7 Section 1. This act may be cited as the "Florida Privacy
8 Protection Act."

9 Section 2. The Legislature declares that digital data is
10 property that is constitutionally protected from unreasonable
11 search and seizure.

12 Section 3. Section 933.41, Florida Statutes, is created to
13 read:

14 933.41 Prohibition against search using wall-penetrating
15 radar device.-

16 (1) A law enforcement officer or law enforcement agency in
17 this state may not use a wall-penetrating radar device, except

Amendment No. 1

18 pursuant to a warrant signed by a judge and based on probable
19 cause or pursuant to a lawful exception to the search warrant
20 requirement, including exceptions to the search warrant
21 requirement established by the United States Supreme Court and
22 Florida Supreme Court.

23 (2) Evidence obtained in violation of this section is not
24 admissible in a criminal, civil, administrative, or other
25 proceeding except as proof of a violation of this section.

26 Section 4. Section 934.60, Florida Statutes, is created to
27 read:

28 934.60 Internet protocol address privacy.—

29 (1) A provider of electronic communications services to
30 the public shall not provide third parties with information that
31 allows an Internet protocol address to be linked to a specific
32 subscriber or customer without the express permission of the
33 subscriber or customer. The request for permission must be clear
34 and conspicuous and must require the subscriber or customer to
35 take an affirmative action to acknowledge such permission. This
36 subsection does not prohibit a provider of electronic
37 communications services from complying with a lawful subpoena,
38 court order, or warrant.

39 (2) A person may institute a civil action in a court of
40 competent jurisdiction to seek injunctive relief to enforce
41 compliance with this section or to recover damages and penalties
42 from a provider that violates this section. A person is entitled
43 to recover a \$10,000 penalty for each violation of this section.

786529 - h0571-strike.docx

Published On: 3/11/2015 6:21:39 PM

Amendment No. 1

44 (3) An action under this section must commence within 2
45 years after the date that the information is disclosed.

46 (4) Consenting to a provider's terms and conditions or a
47 provider's privacy statement describing such provider's data
48 sharing practices shall

49 Section 5. Section 934.70, Florida Statutes, is created to
50 read:

51 934.70 Portable electronic device privacy.—

52 (1) DEFINITIONS.—As used in this section, the term:

53 (a) "Department" means the Department of Law Enforcement.

54 (b) "Government entity" means a federal, state, or local
55 government agency, including, but not limited to, a law
56 enforcement agency or any other investigative entity, agency,
57 department, division, bureau, board, or commission or an
58 individual acting or purporting to act for, or on behalf of, a
59 federal, state, or local government agency. The term does not
60 include a federal agency to the extent that federal law preempts
61 this section.

62 (c) "Information" includes any information concerning the
63 substance or meaning or purported substance or meaning of a
64 communication, including, but not limited to, the name and
65 address of the sender and receiver and the time, date, location,
66 and duration of the communication.

67 (d) "Portable electronic device" means any portable device
68 that is capable of creating, receiving, accessing, or storing
69 electronic data or communications, including, but not limited

Amendment No. 1

70 to, cellular telephones.

71 (2) Information contained in a portable electronic device
72 is not subject to search by a government entity, including a
73 search incident to a lawful arrest, except pursuant to a warrant
74 signed by a judge and based on probable cause or pursuant to a
75 lawful exception to the warrant requirement, including
76 exceptions to the warrant requirement established by the United
77 States Supreme Court and Florida Supreme Court.

78 (3) Evidence obtained in violation of subsection (2) is
79 not admissible in a criminal, civil, administrative, or other
80 proceeding except as proof of a violation of this section.

81 (4) A government entity may not enter into a nondisclosure
82 agreement with a vendor who sells equipment to monitor
83 electronic devices. Any existing nondisclosure agreements are
84 declared void as being against the public policy of the state.
85 Records otherwise protected by such agreements are declared
86 subject to the public records laws, and an agency may not refuse
87 to disclose such agreements or related records upon request by
88 citing such an agreement.

89 (5) A person injured by a government entity as a result of
90 a violation of subsection (4) may file civil suit against the
91 government entity.

92 (6) (a) By January 15 of each year, a communication common
93 carrier or electronic communications service doing business in
94 this state shall report to the department the following
95 information for the preceding calendar year, disaggregated by

786529 - h0571-strike.docx

Published On: 3/11/2015 6:21:39 PM

Amendment No. 1

96 each law enforcement agency in this state making the applicable
97 requests:

98 1. The number of requests made for pen register or trap
99 and trace information.

100 2. The number of requests made for electronic serial
101 number reader information.

102 3. The number of requests made for location information.

103 4. The number of individuals whose location information
104 was disclosed.

105 5. The amount that each law enforcement agency was billed
106 by the communication common carrier or electronic communications
107 service for each request made under subsections (1)-(3).

108 (b) By the 30th day after expiration of a warrant or order
109 issued under subsection (2) or an order extending the period of
110 a warrant or order issued under subsection (2), or by the 30th
111 day after the court denies an application for a warrant or order
112 under subsection (2), the court shall submit to the department
113 the following information, as applicable:

114 1. The receipt of an application for a warrant or order
115 under this article.

116 2. The type of warrant or order for which the application
117 was made.

118 3. Whether any application for an order of extension was
119 granted, granted as modified by the court, or denied.

120 4. The period of monitoring authorized by the warrant or
121 order and the number and duration of any extensions of the

Amendment No. 1

122 warrant.

123 5. The offense under investigation, as specified in the
124 application for the warrant or order or an extension of the
125 warrant or order.

126 6. The name of the law enforcement agency or prosecutor
127 that submitted an application for the warrant or order or an
128 extension of the warrant or order.

129 (c) By January 15 of each year, each prosecutor that
130 submits an application for a warrant or order or an extension of
131 a warrant or order under this section shall submit to the
132 department the following information for the preceding calendar
133 year:

134 1. The information required to be submitted by a court
135 under paragraph (b) with respect to each application submitted
136 by the prosecutor for the warrant or order or an extension of
137 the warrant or order.

138 2. A general description of information collected under
139 each warrant or order that was issued by the court, including
140 the approximate number of individuals for whom location
141 information was intercepted and the approximate duration of the
142 monitoring of the location information of those individuals.

143 3. The number of arrests made as a result of information
144 obtained under a warrant or order issued pursuant to subsection
145 (2).

146 4. The number of criminal trials commenced as a result of
147 information obtained under a warrant or order issued pursuant to

Amendment No. 1

148 subsection (2).

149 5. The number of convictions obtained as a result of
150 information obtained under a warrant or order issued pursuant to
151 subsection (2).

152 (d) Reports submitted to the department under this section
153 are expressly declared subject to disclosure under the public
154 records laws and are not confidential or exempt.

155 (e) By March 1 of each year, the department shall submit a
156 report to the Governor, the President of the Senate, the Speaker
157 of the House of Representatives, and the chairs of the standing
158 committees of the Senate and the House of Representatives with
159 primary jurisdiction over criminal justice. The report shall
160 contain the following information for the preceding calendar
161 year:

162 1. An assessment of the extent of tracking or monitoring
163 by law enforcement agencies of pen registers, trap and trace
164 devices, electronic serial number readers, and location
165 information.

166 2. A comparison of the ratio of the number of applications
167 for warrants or orders made pursuant to subsection (2) to the
168 number of arrests and convictions resulting from information
169 obtained under a warrant or order issued pursuant to subsection
170 (2).

171 3. Identification of the types of offenses investigated
172 under a warrant or order issued pursuant to subsection (2).

173 4. With respect to both state and local jurisdictions, an

Amendment No. 1

174 estimate of the total cost of conducting investigations under a
175 warrant or order issued pursuant to subsection (2).

176 Section 6. Section 1002.227, Florida Statutes, is created
177 to read:

178 1002.227 Contract requirements relating to student data.-

179 (1) All contracts between school districts and companies
180 that process or receive student data shall explicitly prohibit
181 the companies from selling, distributing, or accessing any
182 student data, except as instructed by the school district in
183 order to comply with local, state, or federal reporting
184 requirements.

185 (2) Any data collected from students through online
186 learning is the property of the school district, not the
187 company.

188 (3) (a) Data collected on a student who is younger than 18
189 years of age may not be provided to the Federal Government or to
190 commercial companies without the written consent of the parent
191 or the guardian of the student.

192 (b) Data collected on a student who is 18 years of age or
193 older may not be provided to the Federal Government or to
194 commercial companies without the written consent of the adult
195 student.

196 (c) This subsection does not prohibit any party from
197 complying with a lawful subpoena or warrant.

198 (4) Education technical companies that contract with
199 public schools shall be prohibited from mining student data for

Amendment No. 1

200 commercial purposes.

201 (5) Except as otherwise required by law, or where such
202 information is the subject of an ongoing disciplinary,
203 administrative, or judicial action or proceeding, upon a
204 student's graduation, withdrawal, or expulsion from an
205 educational institution, all personally identifiable student
206 data related to that student:

207 (a) Stored in a student information system shall be
208 deleted.

209 (b) In the possession or under the control of a school
210 employee or third party shall be deleted or destroyed.

211 (6) (a) A violation of this section shall result in a civil
212 fine of up to \$10,000 against the elected school board members
213 under whose jurisdiction the violation occurred.

214 (b) Except as required by applicable law, public funds may
215 not be used to defend or reimburse the unlawful conduct of any
216 person found to knowingly and willfully violate this section.

217 Section 7. The Department of Highway Safety and Motor
218 Vehicles shall not incorporate any radio frequency
219 identification device, or "RFID," or any similar electronic
220 tracking device upon or within any driver license or
221 identification card issued by the department. The department may
222 not obtain fingerprints or biometric DNA material from a United
223 States citizen for purposes of any issuance, renewal,
224 reinstatement, or modification of a driver license or
225 identification card issued by the department.

786529 - h0571-strike.docx

Published On: 3/11/2015 6:21:39 PM

Amendment No. 1

226 Section 8. If any provision of this act or its application
227 to any person or circumstance is held invalid, the invalidity
228 does not affect other provisions or applications of this act
229 which can be given effect without the invalid provision or
230 application, and to this end the provisions of this act are
231 severable.

232 Section 9. This act shall take effect July 1, 2015.
233

234 -----

235 **T I T L E A M E N D M E N T**

236 Remove everything before the enacting clause and insert:
237 An act relating to personal privacy; providing a short title;
238 providing that digital data is protected from unreasonable
239 search and seizure; creating s. 933.41, F.S.; prohibiting use of
240 certain radar technology by law enforcement agencies except for
241 specified purposes; providing that evidence unlawfully collected
242 is not admissible in criminal, civil, or administrative actions;
243 creating s. 934.60, F.S.; prohibiting certain Internet protocol
244 addresses from being disclosed unless certain conditions are
245 met; providing a private right of action; providing limitations;
246 providing what constitutes express permission; creating s.
247 934.70, F.S.; providing definitions; providing restrictions on
248 government searches of portable electronic devices; requiring a
249 warrant for all searches of such devices with exceptions;
250 providing that evidence unlawfully collected is not admissible
251 in criminal, civil, or administrative actions; prohibiting

Amendment No. 1

252 government entities from entering into nondisclosure agreements
253 with vendors of certain equipment used to monitor portable
254 electronic devices; declaring existing nondisclosure agreements
255 void; providing that such agreement is subject to public records
256 laws; authorizing a private right of action against governmental
257 entities for violations; requiring common carriers, electronic
258 communications services, courts, and prosecutors to prepare
259 certain reports to be delivered to the Florida Department of Law
260 Enforcement; providing requirements for such reports; requiring
261 the department to prepare reports to be delivered to certain
262 legislative and executive entities; providing requirements for
263 such reports; creating s. 1002.227, F.S.; requiring school
264 district contracts involving student data contain a provision
265 barring contractors from selling, distributing, or accessing
266 such data; providing exceptions; declaring student data to be
267 the property of the school district; providing that student data
268 shall not be provided to the Federal Government or commercial
269 interests without written permission of a parent or guardian or
270 the student; prohibiting companies from mining student data for
271 commercial purposes; requiring a school or third party to delete
272 or destroy certain student data under specified circumstances;
273 providing penalties; restricting the use of public funds in
274 defense of or for the reimbursement of a person who knowingly or
275 willfully violates this act; prohibiting the Department of
276 Highway Safety and Motor Vehicles from incorporating an
277 electronic tracking device upon or within a driver license or

786529 - h0571-strike.docx

Published On: 3/11/2015 6:21:39 PM

COMMITTEE/SUBCOMMITTEE AMENDMENT

Bill No. HB 571 (2015)

Amendment No. 1

278 identification card; prohibiting the Department of Highway
279 Safety and Motor Vehicles from obtaining fingerprints or
280 biometric DNA material of citizens; providing severability;
281 providing an effective date.