



House of Representatives

File No. 732

General Assembly

February Session, 2016

(Reprint of File No. 614)

Substitute House Bill No. 5640
As Amended by House Amendment
Schedule "A"

Approved by the Legislative Commissioner
April 25, 2016

**AN ACT CONCERNING COMPELLED DISCLOSURE OF CELLULAR
TELEPHONE AND INTERNET RECORDS AND FRAUD COMMITTED
THROUGH TELEPHONE SOLICITATION.**

Be it enacted by the Senate and House of Representatives in General
Assembly convened:

1 Section 1. Section 54-47aa of the general statutes is repealed and the
2 following is substituted in lieu thereof (*Effective October 1, 2016*):

3 (a) For the purposes of this section:

4 (1) "Basic subscriber information" means: (A) Name, (B) address, (C)
5 local and long distance telephone connection records or records of
6 session times and durations, (D) length of service, including start date,
7 and types of services utilized, (E) telephone or instrument number or
8 other subscriber number or identity, including any assigned Internet
9 protocol address, and (F) means and source of payment for such
10 service, including any credit card or bank account number;

11 (2) "Call-identifying information" means dialing or signaling
12 information that identifies the origin, direction, destination or

13 termination of each communication generated or received by a
14 subscriber or customer, excluding geo-location data, by means of any
15 equipment, facility or service of a telecommunications carrier;

16 (3) "Electronic communication service" means "electronic
17 communication service" as defined in 18 USC 2510, as amended from
18 time to time;

19 (4) "Exigent circumstance" means an emergency involving danger of
20 serious physical injury to or death of a person;

21 (5) "Geo-location data" means information concerning the location
22 of an electronic device, including the real-time and historical location
23 of the device, that, in whole or in part, is generated by, derived from or
24 obtained by the operation of an electronic device, including, but not
25 limited to, a cellular telephone surveillance device;

26 [(4)] (6) "Law enforcement official" means the Chief State's Attorney,
27 a state's attorney, an inspector with the Division of Criminal Justice, a
28 sworn member of the Division of State Police within the Department of
29 Emergency Services and Public Protection or a sworn member of an
30 organized local police department;

31 [(5)] (7) "Remote computing service" means "remote computing
32 service" as defined in section 18 USC 2711, as amended from time to
33 time; and

34 [(6)] (8) "Telecommunications carrier" means "telecommunications
35 carrier" as defined in 47 USC 1001, as amended from time to time.

36 (b) A law enforcement official may [request] apply for an ex parte
37 order from a judge of the Superior Court to compel (1) a
38 telecommunications carrier to disclose call-identifying information
39 pertaining to a subscriber or customer, [or] (2) a provider of electronic
40 communication service or remote computing service to disclose basic
41 subscriber information pertaining to a subscriber or customer, or (3) a
42 telecommunications carrier or a provider of electronic communication

43 service or remote computing service to disclose the content of a
44 subscriber's or customer's communications or geo-location data
45 associated with a subscriber's or customer's call-identifying
46 information. The judge shall grant such order if the law enforcement
47 official [states] swears under oath to a statement of (A) a reasonable
48 and articulable suspicion that a crime has been or is being committed
49 [or that exigent circumstances exist] and such call-identifying or basic
50 subscriber information is relevant and material to an ongoing criminal
51 investigation, [. The order] in which case such order shall not authorize
52 disclosure of the content of any communication or geo-location data,
53 or (B) probable cause to believe that a crime has been or is being
54 committed and the content of such subscriber's or customer's
55 communications or the geo-location data associated with such
56 subscriber's or customer's call-identifying information is relevant and
57 material to an ongoing criminal investigation, in which case such order
58 shall authorize the disclosure of such information, content or geo-
59 location data. Any such order entered pursuant to this subsection shall
60 state upon its face the case number assigned to such investigation, the
61 date and time of issuance and the name of the judge authorizing the
62 order. The law enforcement official shall have any ex parte order
63 issued pursuant to this subsection signed by the authorizing judge
64 within forty-eight hours or not later than the next business day,
65 whichever is earlier. No order pursuant to this subsection shall
66 authorize the disclosure of any such information, content or data for a
67 period in excess of fourteen days.

68 (c) A law enforcement official may apply directly to a
69 telecommunications carrier or provider of electronic communication
70 service or remote computing service for production of geo-location
71 data for a period not in excess of forty-eight hours, including real-time
72 or historical geo-location data, or any combination of such data,
73 pertaining to an identified subscriber or customer. The
74 telecommunications carrier or provider of electronic
75 telecommunication service or remote computing service may provide
76 the requested geo-location data upon the applicant stating under oath:

77 (1) That facts exist upon which to base a belief that the data sought is
78 relevant and material to an ongoing criminal investigation; (2) a belief
79 that exigent circumstances exist; and (3) the facts supporting the belief
80 that exigent circumstances exist. Any subsequent application for
81 information from the same telecommunication carrier or provider of
82 electronic communication service or remote computing service for
83 production of geo-location data in connection with the same
84 investigation shall be made pursuant to subsection (b) of this section.

85 [(c)] (d) A telecommunications carrier shall disclose call-identifying
86 information and a provider of electronic communication service or
87 remote computing service shall disclose basic subscriber information
88 to a law enforcement official when an order is issued pursuant to
89 subsection (b) of this section.

90 [(d)] (e) Not later than forty-eight hours after the issuance of an
91 order pursuant to subsection (b) of this section, the law enforcement
92 official shall mail notice of the issuance of such order to the subscriber
93 or customer whose call-identifying information or basic subscriber
94 information is the subject of such order, except that such notification
95 may be delayed for a period of up to ninety days upon the execution of
96 a written certification of such official to the judge who authorized the
97 order that there is reason to believe that notification of the existence of
98 the order may result in (1) endangering the life or physical safety of an
99 individual, (2) flight from prosecution, (3) destruction of or tampering
100 with evidence, (4) intimidation of potential witnesses, or (5) otherwise
101 seriously jeopardizing the investigation. The law enforcement official
102 shall maintain a true copy of such certification. During such ninety-day
103 period, the law enforcement official may request the court to extend
104 such period of delayed notification. Such period may be extended
105 beyond ninety days only upon approval of the court. The applicant
106 shall file a copy of the notice with the clerk of the court that issued
107 such order. If information is provided in response to the order, the
108 applicant shall, not later than ten days after receiving such
109 information, file with the clerk a return containing an inventory of the
110 information received. If a judge finds there is a significant likelihood

111 that such notification would seriously jeopardize the investigation and
112 issues an order authorizing delayed notification under this subsection,
113 the telecommunications carrier or provider of electronic
114 communication service or remote computing service from whom the
115 call-identifying information or basic subscriber information is sought
116 shall not notify any person, other than legal counsel for the
117 telecommunications carrier or provider of electronic communication
118 service or remote computing service and the law enforcement official
119 that requested the ex parte order, of the existence of the ex parte order.
120 Any information provided in response to the court order shall be
121 disclosed to the defense counsel.

122 [(e)] (f) A telecommunications carrier or provider of electronic
123 communication service or remote computing service that provides
124 information pursuant to an order issued pursuant to subsection (b) of
125 this section or pursuant to an application made pursuant to subsection
126 (c) of this section shall be compensated for the reasonable expenses
127 incurred in providing such information.

128 [(f)] (g) Any telecommunications carrier or provider of electronic
129 communication service or remote computing service that provides
130 information [in good faith] pursuant to an order issued pursuant to
131 subsection (b) of this section or an application made pursuant to
132 subsection (c) of this section shall be afforded the legal protections
133 provided under 18 USC 3124, as amended from time to time, with
134 regard to such actions.

135 (h) No information obtained pursuant to subsection (b) or (c) of this
136 section shall be retained for a period in excess of fourteen days, unless
137 such information relates to an ongoing criminal investigation. Any
138 information provided pursuant to said subsection (b) or (c) shall be
139 disclosed to the defense counsel.

140 [(g)] (i) Not later than January fifteenth of each year, each law
141 enforcement official shall report to the Chief State's Attorney the
142 information required by this subsection with respect to each order

143 issued pursuant to subsection (b) of this section and each application
144 made pursuant to subsection (c) of this section in the preceding
145 calendar year. The Chief State's Attorney shall, based upon the reports
146 filed by each law enforcement official and not later than January thirty-
147 first of each year, submit a report, in accordance with the provisions of
148 section 11-4a, to the joint standing committee of the General Assembly
149 having cognizance of matters relating to criminal law and procedure
150 concerning orders issued pursuant to subsection (b) of this section and
151 applications made pursuant to subsection (c) of this section in the
152 preceding calendar year. The report shall include the following
153 information: (1) The number of orders issued pursuant to subsection
154 (b) of this subsection and the number of applications submitted to
155 telecommunications carriers or providers of electronic communication
156 service or remote computing service pursuant to subsection (c) of this
157 section, (2) whether the order was directed to a telecommunications
158 carrier, provider of electronic communication service or provider of
159 remote computing service, (3) whether the information sought was
160 call-identifying information or basic subscriber information, (4) the
161 statutory offense or offenses that were the subject of the investigation,
162 (5) the number of notifications that were delayed pursuant to
163 subsection [(d)] (e) of this section, and the reason for such delayed
164 notification, (6) the number of motions to vacate an order that were
165 filed, and the number of motions granted or denied, (7) the number of
166 investigations concluded and the final result of such investigations,
167 and (8) the status of any criminal prosecution resulting from the
168 investigation.

169 Sec. 2. (NEW) (*Effective October 1, 2016*) (a) A person is guilty of
170 telephone fraud in the first degree when such person (1) knowingly or
171 intentionally devises or participates in a scheme to defraud another
172 person of money or property, (2) (A) employs false pretenses or false
173 promises, as described in section 53a-119 of the general statutes, to
174 obtain such money or property and the amount of such money or the
175 value of such property exceeds twenty thousand dollars, or (B)
176 regardless of its value, obtains such money or property by extortion,

177 and (3) uses a telephonic call, including, but not limited to, a call made
178 by an individual, an automated telephone call and a recorded message,
179 to obtain such money or property from such other person.

180 (b) Telephone fraud in the first degree is a class B felony.

181 Sec. 3. (NEW) (*Effective October 1, 2016*) (a) A person is guilty of
182 telephone fraud in the second degree when such person (1) knowingly
183 or intentionally devises or participates in a scheme to defraud another
184 person of money or property, (2) employs false pretenses or false
185 promises, as described in section 53a-119 of the general statutes, to
186 obtain such money or property and the amount of such money or the
187 value of such property exceeds ten thousand dollars, and (3) uses a
188 telephonic call, including, but not limited to, a call made by an
189 individual, an automated telephone call and a recorded message, to
190 obtain such money or property from such other person.

191 (b) Telephone fraud in the second degree is a class C felony.

192 Sec. 4. (NEW) (*Effective October 1, 2016*) (a) A person is guilty of
193 telephone fraud in the third degree when such person (1) knowingly or
194 intentionally devises or participates in a scheme to defraud another
195 person of money or property, (2) employs false pretenses or false
196 promises, as described in section 53a-119 of the general statutes, to
197 obtain such money or property and the amount of such money or the
198 value of such property exceeds two thousand dollars, and (3) uses a
199 telephonic call, including, but not limited to, a call made by an
200 individual, an automated telephone call and a recorded message, to
201 obtain such money or property from such other person.

202 (b) Telephone fraud in the third degree is a class D felony.

203 Sec. 5. (NEW) (*Effective October 1, 2016*) (a) A person is guilty of
204 telephone fraud in the fourth degree when such person (1) knowingly
205 or intentionally devises or participates in a scheme to defraud another
206 person of money or property, (2) employs false pretenses or false
207 promises, as described in section 53a-119 of the general statutes, to

208 obtain such money or property and the amount of such money or the
209 value of such property exceeds one thousand dollars, and (3) uses a
210 telephonic call, including, but not limited to, a call made by an
211 individual, an automated telephone call and a recorded message, to
212 obtain such money or property from such other person.

213 (b) Telephone fraud in the fourth degree is a class A misdemeanor.

214 Sec. 6. (NEW) (*Effective October 1, 2016*) (a) A person is guilty of
215 telephone fraud in the fifth degree when such person (1) knowingly or
216 intentionally devises or participates in a scheme to defraud another
217 person of money or property, (2) employs false pretenses or false
218 promises, as described in section 53a-119 of the general statutes, to
219 obtain such money or property and the amount of such money or the
220 value of such property exceeds five hundred dollars, and (3) uses a
221 telephonic call, including, but not limited to, a call made by an
222 individual, an automated telephone call and a recorded message, to
223 obtain such money or property from such other person.

224 (b) Telephone fraud in the fifth degree is a class B misdemeanor.

225 Sec. 7. (NEW) (*Effective October 1, 2016*) (a) A person is guilty of
226 telephone fraud in the sixth degree when such person (1) knowingly or
227 intentionally devises or participates in a scheme to defraud another
228 person of money or property, (2) employs false pretenses or false
229 promises, as described in section 53a-119 of the general statutes, to
230 obtain such money or property and the amount of such money or the
231 value of such property is five hundred dollars or less, and (3) uses a
232 telephonic call, including, but not limited to, a call made by an
233 individual, an automated telephone call and a recorded message, to
234 obtain such money or property from such other person.

235 (b) Telephone fraud in the sixth degree is a class C misdemeanor.

This act shall take effect as follows and shall amend the following sections:

Section 1	<i>October 1, 2016</i>	54-47aa
Sec. 2	<i>October 1, 2016</i>	New section
Sec. 3	<i>October 1, 2016</i>	New section
Sec. 4	<i>October 1, 2016</i>	New section
Sec. 5	<i>October 1, 2016</i>	New section
Sec. 6	<i>October 1, 2016</i>	New section
Sec. 7	<i>October 1, 2016</i>	New section

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact:

Agency Affected	Fund-Effect	FY 17 \$	FY 18 \$
Correction, Dept.; Judicial Dept. (Probation)	GF - Potential Cost	See Below	See Below
Resources of the General Fund	GF - Potential Revenue Gain	See Below	See Below

Note: GF=General Fund

Municipal Impact: None

Explanation

The bill creates a new offense of telephone fraud in the first to sixth degree, which carries with it various fines and potential imprisonment. To the extent that offenders are prosecuted for new or expanded offenses under this bill, potential costs for incarceration or probation supervision in the community, or judicial revenue would result. On average, it costs the state \$7,260 (including benefits) to supervise an inmate in the community as opposed to \$61,320 (including benefits) to incarcerate an offender.

The bill makes various other changes to disclosure of cellphone and internet records that do not result in a fiscal impact.

House "A" creates the new offense of telephone fraud, which results in the fiscal impact described above. The amendment makes various other changes that do not result in a fiscal impact.

The Out Years

The annualized ongoing fiscal impact identified above would continue into the future subject to the number of violations.

OLR Bill Analysis**sHB 5640 (as amended by House "A")******AN ACT CONCERNING COMPELLED DISCLOSURE OF CELLULAR TELEPHONE AND INTERNET RECORDS.*****SUMMARY:**

Under current law, telecommunications carriers must disclose call-identifying information, and electronic communication or remote computing service providers must disclose basic subscriber information, to law enforcement officials based on ex parte court orders (i.e., orders issued without a hearing or prior notice to the customer), under specified conditions.

This bill allows law enforcement officials to also seek ex parte court orders to compel these carriers or service providers to disclose a communication's contents or geo-location data associated with call-identifying information. It sets a higher standard for the issuance of these orders (probable cause) than the existing standard for orders to compel disclosure of call-identifying or basic subscriber information (reasonable and articulable suspicion).

In addition, the bill allows a carrier or service provider to disclose up to 48 hours of geo-location data upon the request of law enforcement, without a court order, if there are exigent circumstances (i.e., an emergency involving danger of serious physical injury or death to someone).

Among other things, the bill also (1) limits such orders from authorizing disclosure of information covering more than 14 days, (2) requires law enforcement to disclose the information to defense counsel, and (3) adds to existing reporting requirements.

In addition, the bill creates a specific crime of telephone fraud. The bill classifies this crime into six degrees, generally based on the amount of money or value of the property the violator obtained illegally.

*House Amendment "A" adds the provisions on telephone fraud. It also makes various changes to the disclosure provisions, such as (1) allowing, rather than requiring, carriers and service providers to disclose up to 48 hours of geo-location data without a court order in exigent circumstances; (2) defining "exigent circumstances"; (3) eliminating exigent circumstances as a basis for compelled disclosure of geo-location data or a communication's contents; and (4) making clarifying and conforming changes.

EFFECTIVE DATE: October 1, 2016

§ 1 — DISCLOSURE OF CUSTOMER OR SUBSCRIBER INFORMATION

Definitions

The bill defines "geo-location data" as information on an electronic device's location (both real-time and historical) that, in whole or part, is generated by, derived from, or obtained by the operation of such a device, including a cell phone surveillance device.

Current law defines "call-identifying information" as dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber or customer by means of any equipment, facility, or service of a telecommunications carrier. The bill excludes geo-location data from this definition.

Standard to Grant Ex Parte Court Order

Under current law, if a law enforcement official (e.g., a prosecutor or police officer) requests an ex parte order to compel disclosure of an individual's call-identifying information or basic subscriber information, the judge must grant the order if the official states (1) a reasonable and articulable suspicion that a crime has been, or is being,

committed or that exigent circumstances exist and (2) that the customer information is relevant and material to an ongoing criminal investigation.

The bill requires the law enforcement official to swear under oath that the standard is met. It also reframes the standard. It continues to allow disclosure of this information based on a reasonable and articulable suspicion of a crime and the information's relevance and materiality to an investigation, but it does not allow such disclosure on the basis of exigent circumstances absent a crime. It specifies that an order under this standard cannot authorize disclosure of a communication's contents or geo-location data.

For an order to compel disclosure of a communication's contents or geo-location data associated with call-identifying information, the bill requires the official to swear under oath that (1) there is probable cause to believe that a crime has been or is being committed and (2) the content of the communications or the geo-location data is relevant and material to an ongoing criminal investigation.

In either case, the bill prohibits the order from authorizing the disclosure of more than 14 days of data.

Direct Application to Company

As an alternative to a court order, the bill allows law enforcement officials to apply directly to a telecommunications carrier or electronic communication or remote computing service provider to request production of up to 48 hours of geo-location data for a subscriber or customer. The carrier or provider may comply if the applicant states under oath:

1. that facts exist to support the belief that the requested data is relevant and material to an ongoing criminal investigation,
2. a belief that exigent circumstances exist, and
3. the facts supporting the belief of these circumstances.

The bill allows a law enforcement official to apply to a given carrier or provider only once in the same investigation. An official who seeks disclosure of additional geo-location data must apply for a court order as described above.

As is the case under existing law for data provided by court order, carriers and service providers must be paid the reasonable expenses they incur to comply with the request.

Immunity

Under current law, carriers and service providers who provide information in good faith pursuant to such a court order are subject to the same immunity as is available under specified federal law (18 U.S.C. § 3124). The bill extends this protection to carriers or service providers who provide geo-location data pursuant to a direct request from law enforcement without a court order.

The bill also removes the specific reference to good faith. Federal law (1) prohibits a cause of action against service providers for cooperating with specified courts orders or law enforcement requests in an emergency for certain electronic surveillance devices and (2) provides that a good faith reliance on such a court order or request or a legislative or statutory authorization is a complete defense against a civil or criminal action brought under any law.

Data Retention and Disclosure to Defense Counsel

Under the bill, law enforcement officials who receive this information, whether through a court order or direct application to the company, (1) may retain it for more than 14 days only if it relates to an ongoing criminal investigation and (2) must disclose it to defense counsel.

Delayed Notification After Court Order

By law, after the court issues an order described above, the law enforcement official who requested it must mail a notice within 48 hours to the person whose records were sought, unless the official

requests a 90-day delay for certain reasons (e.g., notification would endanger someone's safety or otherwise seriously jeopardize the investigation). The court may approve delays beyond 90 days.

The bill requires the official to file a copy of the order notice with the court clerk. If the official who requested the order receives information in response to it, he or she must file with the clerk a return within 10 days, including an inventory of the information received. The official also must provide any such information to defense counsel.

The bill specifies that if the judge finds that there is a significant likelihood that notification would seriously jeopardize the investigation and issues an order authorizing delayed notification, the carrier or service provider must not notify any person of the order's existence, other than the applicant and the company's legal counsel.

Reporting

Existing law requires each law enforcement official to report to the chief state's attorney by January 15 of each year on orders issued the previous year, such as the number of orders, type of information sought, and status of any resulting criminal prosecution. The chief state's attorney must compile the data in the individual reports and provide it in a report to the Judiciary Committee by January 31 of each year.

The bill requires this reporting to also include information on applications the law enforcement officials made directly to carriers or service providers for geo-location data as described above.

§ 2-7 — TELEPHONE FRAUD

The bill creates a specific crime of telephone fraud. The crime applies to someone who:

1. knowingly or intentionally devises or participates in a scheme to defraud someone of money or property;

2. obtains such money or property by false pretenses, false promises (see BACKGROUND), or extortion; and
3. uses a telephone call to obtain the money or property from the victim, including a standard call, automated call, or recorded message.

Under the bill, a person convicted of this crime may be imprisoned, fined, or both, as shown in the table below.

Under existing law, obtaining property by false pretenses, false promise, or extortion also constitutes larceny. The bill's monetary thresholds for the classification of telephone fraud, and corresponding penalties, are the same as those that generally apply under existing larceny law (CGS §§ 53a-122 to 53a-125b).

Table 1: Telephone Fraud Penalties

<i>Telephone Fraud</i>	<i>Value of Money or Property</i>	<i>Classification of Crime</i>	<i>Imprisonment</i>	<i>Fines</i>
1 st degree	above \$20,000, or any amount if the crime involved extortion	Class B felony	1 to 20 years	up to \$15,000
2 nd degree	above \$10,000	Class C felony	1 to 10 years	up to \$10,000
3 rd degree	above \$2,000	Class D felony	up to 5 years	up to \$5,000
4 th degree	above \$1,000	Class A misdemeanor	up to 1 year	up to \$2,000
5 th degree	above \$500	Class B misdemeanor	up to 6 months	up to \$1,000
6 th degree	\$500 or less	Class C misdemeanor	up to 3 months	up to \$500

BACKGROUND

Basic Subscriber Information

Under the law, "basic subscriber information" is the:

1. subscriber's name and address;
2. local and long distance telephone connection records or records of session times and durations;
3. length of service, including start date, and types of services utilized;
4. telephone or instrument number, or other subscriber number or identity, including any assigned Internet protocol address; and
5. payment source for the service, including any credit card or bank account number.

Related Federal Law

The federal Stored Communications Act sets conditions governing when electronic communication or remote computing services may or must disclose wire and electronic communications and transactional records (18 U.S.C. § 2701 *et seq.*). For example, these providers may voluntarily disclose a communication's contents in limited situations, such as disclosures to government entities if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury requires such disclosure (18 U.S.C. § 2702(b)).

Obtaining Property by False Pretenses

A person obtains property by false pretenses when, by any false token, pretense, or device, he or she obtains any property from another person, with intent to defraud anyone (CGS § 53a-119(2)).

Obtaining Property by False Promise

A person obtains property by false promise when he or she schemes to defraud someone by obtaining the person's property through express or implied representation that he or she or a third person will engage in particular conduct when he or she does not intend to do so or does not believe that the third person intends to do so (CGS § 53a-119(3)).

Related Bill

sHB 5635 (File 545) contains identical provisions on telephone fraud. It allows ex parte court orders compelling disclosure of call-identifying or basic subscriber information if it is relevant or material to the investigation, rather than requiring it to be both relevant and material.

COMMITTEE ACTION

Judiciary Committee

Joint Favorable

Yea 43 Nay 0 (03/28/2016)