

HOUSE No. 1653

The Commonwealth of Massachusetts

PRESENTED BY:

Jay D. Livingstone

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act to protect private electronic communication, browsing and other activity.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
<i>Jay D. Livingstone</i>	<i>8th Suffolk</i>	<i>1/19/2023</i>
<i>Jason M. Lewis</i>	<i>Fifth Middlesex</i>	<i>2/21/2023</i>

HOUSE No. 1653

By Representative Livingstone of Boston, a petition (accompanied by bill, House, No. 1653) of Jay D. Livingstone and Jason M. Lewis relative to claims against certain corporations, its officers, or other persons for providing electronic records, information, facilities, or assistance in accordance with the terms of search warrants. The Judiciary.

The Commonwealth of Massachusetts

**In the One Hundred and Ninety-Third General Court
(2023-2024)**

An Act to protect private electronic communication, browsing and other activity.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

1 SECTION 1. Chapter 276 of the General Laws, as appearing in the 2020 official edition,
2 is hereby amended by striking Section 1B and inserting in its place the following new sections:-

3 Section 1B. (a) As used in this section, the following words shall have the following
4 meanings:

5 "Adverse result", the following situations:

6 (i) danger to the life or physical safety of an individual;

7 (ii) a flight from prosecution;

8 (iii) the destruction of or tampering with evidence;

9 (iv) the intimidation of a potential witness or witnesses; or

10 (vi) serious jeopardy to an investigation or undue delay of a trial.

11 “Electronic communication,” the transfer of signs, signals, writings, images, sounds, or
12 data of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-
13 optical system. This term does not include wire and oral communications as defined in section 99
14 or chapter 272.

15 “Electronic communication information”, any information pertaining to an electronic
16 communication or the use of an electronic communication service, including, but not limited to
17 the content of electronic communications, metadata, sender, recipients, format, or location of the
18 sender or recipients at any point during the communication, the time or date the communication
19 was created, sent, or received, or any information pertaining to any individual or device
20 participating in the communication. Electronic communication information does not include
21 subscriber information as defined in this section.

22 “Electronic communication services,” a service that provides to its subscribers or users
23 the ability to send or receive electronic communications, including any service that acts as an
24 intermediary in the transmission of electronic communications, or stores electronic
25 communication information. This definition shall not apply to corporations that do not provide
26 electronic communication services to the general public.

27 “Electronic device” or “device”, any device that stores, generates, or transmits
28 information in electronic form and that enables access to, or use of, an electronic communication
29 service, remote computing service, or location information service.

30 “Electronic device information”, electronic communication information and location
31 information stored in a device.

32 “Electronic information”, electronic communication information and location information
33 stored by a service provider on behalf of a subscriber or user of an electronic communication
34 service, location information service, or remote computing service.

35 "Foreign corporation", any corporation or other entity that makes a contract or engages in
36 a terms of service agreement with a resident of the commonwealth to be performed in whole or
37 in part by either party in the commonwealth. The making of the contract or terms of service
38 agreement shall be considered to be the agreement of the foreign corporation that a search
39 warrant which has been properly served on it has the same legal force and effect as if served
40 personally within the commonwealth.

41 “Location information”, information derived from a device or from interactions between
42 devices, with or without the knowledge of the user and regardless of the technological method
43 used, that pertains to or directly or indirectly reveals the present or past geographical location of
44 an individual or device within the Commonwealth of Massachusetts

45 “Location information service”, a service that generates location information or is
46 otherwise used to provide location information to the user or subscribed or the service. This term
47 includes global positioning system services and other mapping, locational, or directional
48 information services.

49 "Massachusetts corporation", any corporation or other entity that is subject to chapter 155
50 or chapter 156B.

51 “Metadata”, information, other than communications content, which is necessary to or
52 associated with the provision of electronic communication services, remote computing services,
53 or location information services, including but not limited to information about the source or

54 destination of electronic communications, date and time of electronic communications, delivery
55 instructions, account information, internet protocol address, quantum of data, data or file type, or
56 data tags.

57 "Properly served", delivery of a search warrant by hand, by United States mail, by
58 commercial delivery service, by facsimile or by any other manner to any officer of a corporation
59 or its general manager in the commonwealth, to any natural person designated by it as agent for
60 the service of process, or if such corporation has designated a corporate agent, to any person
61 named in the latest certificate filed pursuant to section 15.03 of chapter 156D.

62 "Remote computing service", the provision of remote computer processing services or
63 remote computer storage of digital assets. This definition shall not apply to corporations that do
64 not provide those services to the general public.

65 "Service provider", a person or entity offering electronic communication services,
66 location information services, or remote computing services.

67 "Subscriber information", the name, street address, telephone number, email address, or
68 similar contact information provided by the subscriber to a service provider to establish or
69 maintain an account or communication channel, a subscriber or account number or identifier, the
70 length of service, and the types of services used by a user of or subscriber to a service provider.

71 (b) Except pursuant to a warrant issued by a justice of the superior court or acting in
72 accordance with a legally recognized exception under subsection (k), it shall be unlawful for a
73 government office, law enforcement agency as defined in section 1 of chapter 6E, or public
74 official to

75 (i) obtain or access electronic information or subscriber information from a service
76 provider

77 (ii) access electronic device information from the electronic device, whether by physical
78 or electronic means.

79 (c) A justice of the superior court may issue a search warrant upon a sworn application by
80 the applicant showing there is probable cause to believe that:-

81 (i) particular identified records or information are in the actual or constructive custody of
82 the Massachusetts or foreign corporation acting as a service provider; and

83 (ii) such records or information constitute evidence of or the means or instrumentalities
84 of the commission of a specified criminal offense under the laws of the commonwealth.

85 (d) Search warrants issued under this section shall:-

86 (i) designate the person, corporation, or other entity, if any, in possession of the records
87 or data sought;

88 (ii) describe, with particularity, the information sought and to be provided;

89 (iii) be directed to the law enforcement officer or government making the application for
90 the warrant and authorize them to properly serve the warrant upon the corporation and to take all
91 other actions prescribed by this section; and

92 (iv) be issued in the form and manner prescribed in sections 2A½ and 2B, insofar as they
93 are applicable.

94 (e) The following provisions shall apply to any search warrant issued under this section:-

95 (i) when properly served with a search warrant, a corporation subject to this section shall
96 provide all records sought pursuant to that warrant within 14 days of receipt, including those
97 records maintained or located outside the commonwealth;

98 (ii) if the applicant makes a showing and the court finds that failure to produce records
99 within less than 14 days would cause an adverse result, a warrant may require production of
100 records within less than 14 days;

101 (iii) a court may reasonably extend the time required for production of the records upon
102 finding that the corporation has shown good cause for that extension and that an extension of
103 time would not cause an adverse result;

104 (iv) a corporation seeking to quash a warrant served on it pursuant to this section shall
105 seek relief from the court that issued the warrant within the time required for production of
106 records pursuant to this section. The court shall hear and decide such motion not later than 14
107 days after the motion is filed; and

108 (v) the corporation shall verify the authenticity of records that it produces by providing an
109 affidavit from the person in custody of those records certifying that they are true and complete.

110 (f) A Massachusetts corporation that provides electronic communication services, remote
111 computing services, or location information services, when served with a warrant or subpoena
112 issued by another state to produce records that would reveal the identity of the customers using
113 those services, data stored by, or on behalf of the customer, the customer's usage of those
114 services, the recipient or destination of communications sent to or from those customers, or the
115 content of those communications, shall produce those records as if that warrant or subpoena had
116 been issued under the law of the commonwealth.

117 (g) No claim shall lie against any foreign or Massachusetts corporation subject to this
118 section, its officers, employees, agents, or other persons for providing records, information,
119 facilities, or assistance in accordance with the terms of a search warrant issued pursuant to this
120 section.

121 (h) Not later than 7 days after information is obtained by a law enforcement officer or
122 government office pursuant to a warrant under this section, that officer or office shall serve upon,
123 or deliver by registered or first-class mail, electronic mail, or other means reasonably calculated
124 to be effective as specified by the court issuing the warrant, to the individual to whom the
125 information pertains to, a copy of the warrant, a copy of the application for the warrant and
126 notice that informs them of the following:-

127 (i) the nature of the law enforcement inquiry with reasonable specificity;

128 (ii) in the case of electronic information, that such information was requested by or
129 supplied to that government office or public official, a description of the information, and the
130 dates on which the request was made and on which the information was supplied;

131 (iv) whether notification of the customer, subscriber, or user was delayed under
132 subsection (i); and

133 (v) which court made the certification or determination under which that delay was made,
134 if applicable.

135 (i) A government office, law enforcement agency, or public official may include in its
136 application for a warrant a request for an order delaying the notification required under
137 subsection (h) for a period not to exceed 90 days, and the court may issue the order if it

138 determines there is reason to believe that notification of the existence of the warrant may have an
139 adverse result. Upon expiration of any period of delay granted under this subsection, the
140 government office, law enforcement agency as defined in section 1 of chapter 6E, or public
141 official shall provide the customer or subscriber a copy of the warrant together with notice
142 required under, and by the means described in, subsection (h).

143 (j) A government office, law enforcement agency as defined in section 1 of chapter 6E, or
144 public official may include in its application for a warrant a request for an order directing a
145 corporation or other entity to which a warrant is directed not to notify any other person of the
146 existence of the warrant for a period of not more than 90 days, and the court may issue the order
147 if the court determines that there is reason to believe that notification of the existence of the
148 warrant will have an adverse result.

149 The court may, upon application, grant one or more extensions of orders delaying
150 notification for an additional 90 days if the court determines that there is reason to believe that
151 notification of the existence of the warrant will have an adverse result.

152 (k) Notwithstanding any general or special law to the contrary, a government office, law
153 enforcement agency as defined in section 1 of chapter 6E, or public official may obtain or access
154 the categories of information mentioned in subsection (b):-

155 (i) with the specific contemporaneous written consent of the individual to whom the
156 information pertains as the owner or authorized user of the device or as user or subscriber of the
157 remote computing services, electronic communications services, or location information
158 services;

159 (ii) with the specific contemporaneous written consent of the recipient of an electronic
160 communication.

161 (iii) in order to respond to a call for emergency services; or

162 (iii) in response to an emergency involving immediate danger of death or serious physical
163 injury to any person requires obtaining without delay information relating to the emergency;
164 provided, however, that the request is narrowly tailored to address the emergency and subject to
165 the following limitations:-

166 (a) the request shall document the factual basis for believing that an emergency involving
167 immediate danger of death or serious physical injury to a person requires obtaining without delay
168 of the information relating to the emergency; and

169 (b) not later than 48 hours after the government office obtains access to records, it shall
170 file with the appropriate court a signed, sworn statement of a supervisory official of a rank
171 designated by the head of the office setting forth the grounds for the emergency access.

172 (iv) in case of electronic device information, if the government office, law enforcement
173 agency, or public official, in good faith, believes the device to be lost, stolen, or abandoned;
174 provided, however, that the entity shall only access electronic device information in order to
175 attempt to identify, verify, or contact the owner or authorized possessor of the device.

176 (l) Within five business days after issuing or denying a warrant, the court shall report to
177 the office of court management within the trial court the following information:-

178 (i) the name of the agency making the application;

179 (ii) the offense specified in the warrant or application therefore;

- 180 (iii) the nature of the information sought;
- 181 (iv) if the warrant application sought authorization to obtain or access information from a
182 corporation or other entity, the name of that entity;
- 183 (v) whether the warrant was granted as applied for, was modified, or was denied;
- 184 (vi) the period of disclosures or access authorized by the warrant;
- 185 (vii) the number and duration of any extensions of the warrant; and
- 186 (viii) any order directing delayed notification of the warrant's existence.

187 In June of each year, the court administrator in the office of court management within the
188 trial court shall transmit to the legislature a full and complete report concerning the number of
189 applications for warrants authorizing or requiring the disclosure of or access to information
190 under this section. The reports shall include a summary and analysis of the data required to be
191 filed with that office. The reports shall be filed with the offices of the clerk of the house and the
192 senate and shall be public records. The court administrator in the office of court management
193 within the trial court shall issue guidance regarding the form of the reports.

194 (m) The requirements of this section shall apply to all state and local law enforcement
195 officers operating in the commonwealth, whether said officers are assigned to state and local law
196 enforcement operations exclusively, or to a joint task force or other collaborative operations with
197 federal law enforcement agencies.

198

199 Section 1C. (a) As used in this section, the following words shall have the following
200 meanings:

201 “Reverse-keyword court order”, any court order, including a search warrant or subpoena,
202 compelling the disclosure of records or information identifying any unnamed persons, by name
203 or other unique identifiers, who electronically searched for particular words, phrases, or
204 websites, or who visited a particular website through a link generated by such a search,
205 regardless of whether the order is limited to a specific geographic area or time frame.

206 “Reverse-keyword request”, any request, in the absence of a court order, by any
207 government entity for the voluntary provision of records or information identifying any unnamed
208 persons, by name or other unique identifiers, who electronically searched for particular words,
209 phrases, or websites, or who visited a particular website through a link generated by such a
210 search, regardless of whether or not the request is limited to a specific geographic area or time
211 frame. Such requests shall include offers to purchase such records or information.

212 “Reverse-location court order”, any court order, including a search warrant or subpoena,
213 compelling the disclosure of records or information pertaining to the location of previously
214 unidentified electronic devices or their unnamed users or owners and whose scope extends to an
215 unknown number of electronic devices present in a specified geographic area at a specified time,
216 irrespective of whether such location is identified via global positioning system coordinates, cell
217 tower connectivity, wi-fi positioning, or any other form of location detection.

218 “Reverse-location request”, any request, in the absence of a court order, by any
219 government entity for the voluntary provision of records or information pertaining to the location
220 of unidentified electronic devices or their unnamed users or owners and whose scope extends to

221 an unknown number of electronic devices present in a specified geographic area at a specified
222 time, irrespective of whether such location is identified via global positioning system
223 coordinates, cell tower connectivity, wi-fi positioning, or any other form of location detection.
224 Such requests shall include offers to purchase such records or information.

225 "Subpoena", a grand jury or trial subpoena issued in the course of a criminal proceeding
226 or an administrative subpoena issued pursuant to section 17B of chapter 271.

227 (b) It shall be unlawful for a government office, law enforcement agency as defined in
228 section 1 of chapter 6E, or public official to:-

229 (i) seek, from any court, a reverse-location court order or a reverse-keyword court order.

230 (ii) seek, secure, obtain, borrow, purchase, or review any information or data obtained
231 through a reverse-location court order or a reverse-keyword court order.

232 (c) No court subject to the laws of the commonwealth shall issue a reverse-location court
233 order or a reverse-keyword court order.

234 (d) No person or entity in the commonwealth, as a result of any law, regulation, or
235 agreement adopted by the commonwealth or any political subdivision thereof, shall be obligated
236 to comply with a reverse-location court order or a reverse-keyword court order issued by the
237 commonwealth or a political subdivision thereof.

238 (e) It shall be unlawful for a government office, law enforcement agency, or public
239 official to:-

240 (i) make a reverse-location request or a reverse-keyword request;

241 (ii) seek, secure, obtain, borrow, purchase, or review any information or data obtained
242 through a reverse-location request or a reverse-keyword request.

243 (iii) seek the assistance of any agency of the federal government or any agency of the
244 government of another state or subdivision thereof in obtaining information or data from a
245 reverse-location court order, reverse-keyword court order, reverse-location request, or reverse-
246 keyword request if the government entity would be barred from directly seeking such
247 information under this section.

248 (f) For the purposes of this section, a record, information, or evidence is “derived from” a
249 reverse-location court order, reverse-keyword court order, reverse-location request, or reverse-
250 keyword request where the government entity would not have originally possessed the
251 information or evidence but for the violative court order or request, and regardless of any claim
252 that the record, information, or evidence is attenuated from the unlawful order or request, would
253 inevitably have been discovered, or was subsequently reobtained through other means.

254

255 Section 1D. (a) As used in this section, the following words shall have the following
256 meanings:

257 "Cell site simulator device", any device that functions as or simulates a base station for
258 commercial mobile services or private mobile services in order to identify, locate, or intercept
259 transmissions from cellular devices for purposes other than providing ordinary commercial
260 mobile services or private mobile services.

261 (b) It shall be unlawful for a government office, law enforcement agency, or public
262 official to use a cell site simulator device for any purpose other than to locate or track the
263 location of a specific electronic device, pursuant to a warrant consistent with subsection (d), or if
264 exigent circumstances exist requiring swift action to prevent imminent danger to the safety of an
265 individual or the public.

266 (c) Any warrant application seeking to intercept the substance of a wire or oral
267 communication from an electronic device may only be granted pursuant to section 99 of chapter
268 272.(d) An application for a warrant to use a cell site simulator device must include:

269 (i) a statement of facts establishing probable cause to believe that the use of a cell site
270 simulator will aid in the apprehension of a person who the applicant has probable cause to
271 believe has committed, is committing, or is about to commit a felony; and

272 (ii) sufficient facts demonstrating that less invasive methods of investigation or
273 surveillance to the privacy of non-targeted parties have been tried and failed or reasonably
274 unlikely to succeed if tried; and

275 (iii) a description of the nature and capabilities of the cell site simulator device that will
276 be used and the manner and method of its deployment, including whether the cell site simulator
277 device will obtain data from non-target communications devices; and

278 (iv) a description of the procedures that will be followed to protect the privacy of non-
279 targets during the investigation, including the deletion of data obtained from non-target
280 communication devices.

281 (v) the name of the government agency that owns the cell site simulator device.

282 (e) All non-target data must be deleted immediately upon collection, but no later than
283 once every 24 hours.

284 (f) All target data must be deleted within thirty days if there is no longer probable cause
285 to support the belief that such information or metadata is evidence of a crime.

286 (g) The warrant shall permit the use of a cell site simulator for a period not to exceed
287 fifteen days. Any time prior to the expiration of a warrant, the applicant may apply to the issuing
288 judge for a renewal thereof with respect to the same electronic device, person, and location of
289 surveillance. An application for renewal must incorporate the warrant sought to be renewed
290 together with the application and any accompanying papers upon which it was issued. The
291 application for renewal must set forth the results of the investigation thus far conducted, as well
292 as present grounds for extension in conformity with subsection (d). Upon such application, the
293 judge may issue an order renewing the warrant and extending the authorization for a period not
294 exceeding fifteen days.

295 (h) For the purposes of this section, a record, information, or evidence is “derived from”
296 unauthorized use of a cell site simulator where the government entity would not have originally
297 possessed the information or evidence but for the violative court order or request, and regardless
298 of any claim that the record, information, or evidence is attenuated from the unlawful order or
299 request, would inevitably have been discovered, or was subsequently re-obtained through other
300 means.

301

302 Section 1E. (a) Any individual whose information was obtained by a government entity
303 in violation of sections 1B, 1C, and 1D shall be notified of the violation, in writing, by the

304 government office, law enforcement agency, or public official who committed the violation and
305 of the legal recourse available to that person pursuant to this section.

306 (b) Except in a judicial, administrative or legislative trial, hearing, or other proceeding
307 alleging a violation of sections 1B, 1C, and 1D, no information acquired in violation of said
308 sections, and no evidence derived therefrom, may be received in evidence in any trial, hearing, or
309 other proceeding in or before any court, grand jury, department, officer, agency, regulatory body,
310 legislative committee, or other authority of the commonwealth, or a political subdivision thereof.

311 (c) Any individual alleging harm caused by a violation of sections 1B, 1C, and 1D may
312 bring a civil action against the government office, law enforcement agency, or public official
313 who violated those sections in the Superior Court or any court of competent jurisdiction. Venue
314 in the Superior Court shall be proper in the county in which the plaintiff resides or was located at
315 the time of the violation.

316 (d) An individual protected by this section shall not be required, as a condition of service
317 or otherwise, to file an administrative complaint with the attorney general or to accept mandatory
318 arbitration of a claim arising under this chapter. Chapter 258 shall not apply to a claim brought
319 under this section.

320 (e) In a civil action in which the plaintiff prevails, the court may award actual damages,
321 including damages for emotional distress, of one thousand dollars per violation or actual
322 damages, whichever is greater, (punitive damages; and any other relief, including but not limited
323 to injunctive or declaratory relief, that the court deems to be appropriate. In addition to any relief
324 awarded, the court shall award reasonable attorney's fees and costs to any prevailing plaintiff.

325 (i) In assessing the amount of punitive damages, the court shall consider:-

326 (a) The number of people whose information was disclosed;

327 (b) Whether the violation directly or indirectly targeted persons engaged in the exercise
328 of activities protected by the Constitution of the United States of America or the Massachusetts
329 Declaration of Rights, and

330 (c) The persistence of violations by the government office, law enforcement agency, or
331 public official.

332 (f) Non-waivable rights. Any provision of a contract or agreement of any kind, including
333 a private corporation terms of service or policies, that purports to waive or limit in any way an
334 individual's rights under this section, including but not limited to any right to a remedy or means
335 of enforcement, shall be deemed contrary to state law and shall be void and unenforceable.

336 (g) No private or government action brought pursuant to this chapter shall preclude any
337 other action under this chapter.

338 SECTION 2. Chapter 276 is hereby amended by inserting after section 2A the following
339 section:-

340 Section 2A½. (a) A warrant issued pursuant to section 1B for records or data from a
341 corporation providing electronic communication services, remote computing services, or location
342 information services shall be in substantially the following form:-

343 THE COMMONWEALTH OF MASSACHUSETTS.

344 (COUNTY), ss. (NAME) COURT.

345 To the Sheriffs of our several counties, or their deputies, any State Police Officer, or a
346 Police Officer of any city or town in the Commonwealth.

347 Proof by affidavit having been made this day before (name and office of person
348 authorized to issue warrant) by (names of person or persons whose affidavits have been taken)
349 that there is probable cause for believing that certain records or data are in the in the possession
350 of (identify corporation or other entity) and that those records or data constitute evidence of or
351 the means or instrumentalities of the commission of (specified criminal offense under the laws of
352 the commonwealth).

353 We therefore authorize you to present this warrant to (identify corporation or other
354 entity), which warrant shall operate as an order for immediate disclosure of the following records
355 or data:

356 (description of particular records or data),

357 and if any such records or data are disclosed to bring it before (court having jurisdiction)
358 at (name of court and location).

359 Dated at (city or town) this _____ day of _____, (insert year).

360 Justice of the Superior Court

361 (b) A warrant issued pursuant to section 1D authorizing the use of a cell site simulator
362 device shall be in substantially the following form:

363 THE COMMONWEALTH OF MASSACHUSETTS.

364 (COUNTY), ss. (NAME) COURT.

365 To the Sheriff, or their deputy, State Police Officer, or municipal Police Officer who has
366 made this complaint on oath.

367 Proof by affidavit having been made this day before (name and office of person
368 authorized to issue warrant) by (names of person or persons whose affidavits have been taken)
369 that there is probable cause for believing that the use of a cell site simulator device will lead to
370 evidence of or the means or instrumentalities of the commission of (specified criminal offense
371 under the laws of the commonwealth) or the location of a person whom there is probable cause
372 to believe has committed, is committing, or is about to commit (specified criminal offense under
373 the laws of the commonwealth).

374 We therefore authorize you to obtain or access by means of a cell site simulator device,
375 the following records or data:

376 (description of particular records or data),

377 and if any such records or data are disclosed to bring it before (court having jurisdiction)
378 at (name of court and location).

379 Dated at (city or town) this _____ day of _____, (insert year).

380 Justice of the Superior Court

381

382 SECTION 3. Section 2B of said chapter 276 is hereby amended by striking clauses 3 and
383 4 of the model affidavit and inserting in place thereof the following:-

384 3. Based upon the foregoing reliable information (and upon my personal knowledge)
385 there is probable cause to believe that the property, records or data hereinafter described (has
386 been stolen, or is being concealed, or constitutes evidence of a particular offense, etc.) and may
387 be found (in the possession of A. B. or any other person or corporation) at premises (identify).

388 4. The (property, records, or data) for which I seek issuance of a search warrant is the
389 following: (here describe the property, records, or data as particularly as possible).

390

391 SECTION 4. Section 7 of chapter 78 of the General Laws is hereby amended by striking
392 the third sentence.

393

394 SECTION 5. Said chapter 78 is hereby amended by inserting after section 7 the following
395 section:-

396 Section 7A.

397 (a) For the purposes of this section, “library user private data” shall mean that part of the
398 records of a public library which reveals the identity and intellectual pursuits of a person using
399 such library.

400 (b) Library user private data shall not be a public record as defined by clause Twenty-
401 sixth of section seven of chapter four.

402 (c) The rights contained within sections 1B, 1C and 1E of chapter 276 shall apply to a
403 library user as if that person were in possession of their library user private data.

