

**SENATE . . . . . No. 2183**

---

**The Commonwealth of Massachusetts**

\_\_\_\_\_  
**In the Year Two Thousand Nine**  
\_\_\_\_\_

An Act to combat economic crime..

*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. The General Laws, as appearing in the 2008 Official Edition, are hereby  
2 amended by adding after Chapter 267 the following new chapter: — Chapter 267A Money  
3 Laundering.

4 Section 1. Definitions.

5 As used in this chapter, the following words shall, unless the context clearly requires  
6 otherwise, have the following meanings:—

7 “Conducts”, initiates, concludes or participates in initiating or concluding in a  
8 transaction.

9 “Criminal activity”, a criminal offense punishable under the laws of the commonwealth  
10 by imprisonment in a state prison or a criminal offense committed in another jurisdiction  
11 punishable under the laws of that jurisdiction as a felony.

12 “Transaction”, a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition,  
13 and with respect to a financial institution includes a deposit, withdrawal, bailment, transfer

14 between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock,  
15 bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other  
16 payment, transfer, or delivery by, through, or to a financial institution, by whatever means  
17 effected.

18 “Financial institution”, (a) any bank as defined in section one of chapter 167 ; (b) any  
19 national banking association, bank, savings and loan, savings bank, cooperative bank, building  
20 and loan, or credit union organized under the laws of the United States; (c) any banking  
21 association, bank, savings and loan, savings bank, cooperative bank, building and loan or credit  
22 union organized under the laws of any state; (d) any agency, agent, or branch of a foreign bank;  
23 (e) any currency dealer or exchange; (f) any person or business engaged primarily in the cashing  
24 of checks; (g) any person or business regularly engaged in the issuing, selling, or redeeming of  
25 traveler's checks, money orders or similar instruments; (h) any broker or dealer in securities or  
26 commodities; (i) any licensed transmitter of funds or other person or business regularly engaged  
27 in the transmission of funds to a foreign nation for others; (j) any investment banker or  
28 investment company; (k) any insurer; (l) any dealer in precious metals, stones or jewels; (m) any  
29 pawnbroker or scrap metal dealer; (n) any telegraph or other communications company; (o) any  
30 personal property or real estate broker; (p) any dealer in vehicles, including, but not limited to,  
31 automobiles, aircraft and vessels; (q) any operator of a betting or gambling facility; (r) any travel  
32 agent; (s) any thrift institution; (t) any operator of a credit card system; or (u) any loan or finance  
33 company.

34 “Monetary instrument”, the currency and coin of the United States or any foreign  
35 country; any bank check, money order, stock, investment security, or negotiable instrument in  
36 bearer form or otherwise in such form that title passes upon delivery; gold, silver or platinum

37 bullion or coins; diamonds, emeralds, rubies, or sapphires; any negotiable instrument including:  
38 bank checks, cashier's checks, traveler's checks, or monetary orders made payable to the order of  
39 a named party that have not been endorsed or which bear restrictive endorsements; poker chips,  
40 vouchers or other tokens exchangeable for cash by gaming entities; and credit cards, debit cards,  
41 gift cards, gift certificates, calling cards, or scrips.

42 Section 2. Money Laundering.

43 Whoever knowingly:

44 (a) engages in a transaction involving a monetary instrument or other property known to  
45 be derived from criminal activity with the intent to promote, carry on or facilitate criminal  
46 activity, or knowing that the transaction is designed in whole or in part either to conceal or  
47 disguise the nature, location, source, ownership or control of the property derived from criminal  
48 activity or to avoid a transaction reporting requirement of this chapter, of the United States, or of  
49 any other state;

50 (b) transports or possesses a monetary instrument or other property that was derived from  
51 criminal activity; or

52 (c) directs, organizes, finances, plans, manages, supervises, or controls the transportation  
53 of or transactions in monetary instruments or other property known to be derived from criminal  
54 activity or which a reasonable person would believe to be derived from criminal activity; is  
55 guilty of the crime of money laundering and shall be punished by imprisonment in the state  
56 prison for not more than 6 years or by a fine of not more than \$250,000 or twice the value of the  
57 property transacted, whichever is greater, or by both such imprisonment and fine; and for any  
58 subsequent offense shall be punished by imprisonment in the state prison for not less than 2

59 years, but not more than 8 years or by a fine of not more than \$500,000 or three times the value  
60 of the property transacted, whichever is greater, or by both such imprisonment and fine.

61 Section 3. Record Keeping.

62 (a) A financial institution shall file with the attorney general a copy of any and all reports  
63 required by the Currency and Foreign Transactions Act, set forth in 31 U.S.C., sections 5311  
64 through 5315, 31 C.F.R. 103. (b) A financial institution, or any officer, employee, or agent  
65 thereof that keeps and files a record in reliance of this section shall not be liable to its customer,  
66 to a state or local agency, or to any person for any loss or damage caused in whole or in part by  
67 the making, filing, or governmental use of the report, or any information contained therein.  
68 Nothing in this chapter shall be construed to give rise to a private cause of action for relief or  
69 damages. This paragraph does not preclude a financial institution, in its discretion, from  
70 instituting contact with, and thereafter communicating with and disclosing customer financial  
71 records to appropriate federal, state, or local law enforcement agencies when the financial  
72 institution has reason to suspect that the records or information demonstrate that the customer  
73 has violated any provisions of this chapter. (c) Any report, record, or information obtained by the  
74 attorney general pursuant to this section is not a public record and is not subject to disclosure,  
75 except to other state and federal law enforcement agencies. (d) Any violation of this section,  
76 which is not a violation of section 2, shall be punished by a fine of \$100 for each report not filed.

77 Section 4. Forfeiture.

78 All monetary instruments or other property, real or personal, obtained directly as a result  
79 of a violation of section 2 of this chapter, shall be subject to forfeiture to the commonwealth.

80 SECTION 2. The General Laws, as appearing in the 2008 Official Edition, are hereby  
81 amended by adding after Chapter 271 the following new chapter: — Chapter 271A Enterprise  
82 Crime.

83 Section 1. Definitions.

84 As used in this chapter, the following words shall, unless the context clearly requires  
85 otherwise, have the following meanings:—

86 “Enterprise”, any individual, sole proprietorship, partnership, corporation, trust or other  
87 legal entity, or any unchartered union, association or group of persons associated in fact although  
88 not a legally recognized entity, and includes unlawful as well as lawful enterprises and  
89 governmental as well as other entities.

90 “Pattern of criminal enterprise activity”, engaging in at least two incidents of criminal  
91 enterprise activity that have the same or similar pattern, intents, results, accomplices, victims or  
92 methods of commission, or are otherwise interrelated by distinguishing characteristics and are  
93 not isolated incidents, provided at least one of the acts occurred after the effective date of this  
94 act, and the last of the incidents occurred within five years after a prior commission of criminal  
95 enterprise activity.

96 “Criminal enterprise activity”, to commit, to attempt to commit, to conspire to commit, or  
97 to solicit, coerce, aid, abet, or intimidate another to commit any of the following criminal activity  
98 under the laws of the commonwealth or equivalent crimes under the laws of any other  
99 jurisdiction: murder; rape; manslaughter; assault; assault and battery; mayhem; robbery;  
100 extortion; stalking; criminal harassment; kidnapping; arson; burglary; malicious destruction of  
101 property; commission of a felony for hire; breaking and entering; child exploitation; poison;

102 human trafficking; violation of constitutional rights; usury; uttering; misuse or fraudulent use of  
103 credit cards; identity fraud; misappropriation of funds; gross fraud; insurance fraud; prize  
104 fighting; boxing matches; counterfeiting; perjury; subornation of perjury; obstruction of justice;  
105 money laundering; witness intimidation; bribery; electronic eavesdropping; prostitution;  
106 receiving stolen property; larceny over \$250.00; larceny by false pretenses/embezzlement;  
107 forgery; prohibited financial interest; procurement fraud; false claims; tax evasion; filing false  
108 tax return; crimes involving violations of: gambling and lottery laws; gift laws; liquor laws;  
109 tobacco laws; firearms laws; securities laws; lobbying laws; ethics laws; conflict of interest laws;  
110 child and elder abuse laws; or any conduct defined as a racketeering activity under Title 18,  
111 U.S.C. s. 1961(1)(A)(B) and (D).

112 “Unlawful debt”, a debt incurred or contracted in an illegal gambling activity or business  
113 or which is unenforceable under state or federal law in whole or part as to principal or interest  
114 because of the law relating to usury.

115 Section 2. Enterprise Crime.

116 Whoever knowingly:

117 (a) through a pattern of criminal enterprise activity or through the collection of an  
118 unlawful debt, receives anything of value or acquires or maintains, directly or indirectly, any  
119 interest in or control of any enterprise;

120 (b) has received any proceeds derived, directly or indirectly, from a pattern of criminal  
121 enterprise activity or through the collection of an unlawful debt, to use or invest, directly or  
122 indirectly, any part of the proceeds including proceeds derived from the investment, in the  
123 acquisition of any interest in real property, or in the establishment or operation of, any enterprise;

124 (c) is employed by or associated with any enterprise to conduct or participate, directly or  
125 indirectly, in the conduct of the enterprise's affairs by engaging in a pattern of criminal enterprise  
126 activity or through the collection of an unlawful debt; or

127 (d) conspires or attempts to violate subsections (a), (b), or (c) of this section; is guilty of  
128 enterprise crime and shall be punished by imprisonment in the state prison for not less than 3  
129 years and not more than 15 years or by a fine of not more than \$25,000, or by both such  
130 imprisonment and fine.

131 A purchase of securities on the open market for purposes of investment, and without the  
132 intention of controlling or participating in the control of the issuer, or of assisting another to do  
133 so, shall not be unlawful under this subsection (1) if the securities of the issuer held by the  
134 purchaser, the members of his immediate family, and his or their accomplices in any pattern of  
135 criminal activity or the collection of an unlawful debt after such purchase do not amount in the  
136 aggregate to one percent of the outstanding securities of any one class and do not confer, either  
137 in law or in fact, the power to elect one or more directors of the issuer.

138 Section 3. Forfeiture.

139 All monetary proceeds or other property, real or personal, obtained directly as a result of  
140 a violation of this chapter, shall be subject to forfeiture to the commonwealth.

141 SECTION 3. The General Laws, as appearing in the 2008 Official Edition, are hereby  
142 amended by striking out section 99 of Chapter 272 and inserting, in place thereof, the following  
143 new section: —

144 Section 99. Wiretap and Electronic Surveillance

145 Section 1. Preamble

146 The purpose of this section is to provide a procedure for law enforcement agencies to  
147 seek court-approved wire and surveillance orders that will keep pace with modern technology  
148 and criminal techniques, while at the same time protecting individual rights and privacy.

149 Section 2. Definitions.

150 As used in this section, the following words shall, unless the context clearly requires  
151 otherwise, have the following meanings:—

152 “Aggrieved person” means a person who was a party to any intercepted wire, oral, or  
153 electronic communication or a person against whom the interception was directed.

154 “Attorney for the state” means the attorney general, any assistant attorney general  
155 specially designated by the attorney general, any district attorney, or any assistant district  
156 attorney specially designated by the district attorney authorized to commence and prosecute an  
157 action under this section.

158 “Aural transfer” means a transfer containing the human voice at any point between and  
159 including the point of origin and the point of reception.

160 “Communication common carrier” means any person engaged as a common carrier in  
161 providing or operating wire or electronic communication facilities.

162 “Contents” when used with respect to any wire, oral, or electronic communication,  
163 includes any information concerning the substance, purport, or meaning of that communication.



164           “Corporate and institutional trading partners” means financial institutions and general  
165 business entities and corporations which engage in the business of cash and asset management,  
166 asset management directed to custody operations, securities trading, and wholesale capital  
167 markets including foreign exchange, securities lending, and the purchase, sale or exchange of  
168 securities, options, futures, swaps, derivatives, repurchase agreements and other similar financial  
169 instruments with such financial institution.

170           “Court of competent jurisdiction” means a superior court of the commonwealth.

171           “Electronic communication” means any transfer of signs, signals, writing, images,  
172 sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,  
173 electromagnetic, photo-electronic or photo-optical system, excluding:

174           (1) any wire or oral communication;

175           (2) any communication made through a tone-only paging device;

176           (3) any communication from a tracking device, defined as an electronic or mechanical  
177 device which permits the tracking of the movement of a person or object; or

178           (4) electronic funds transfer information stored by a financial institution in a  
179 communications system used for the electronic storage and transfer of funds.

180           “Electronic communication service” means any service which provides to its users the  
181 ability to send or receive wire or electronic communications.

182           “Electronic communications system” means any wire, radio, electromagnetic, photo-  
183 optical or photo-electronic facilities for the transmission of wire or electronic communications,

184 and any computer facilities or related electronic equipment for the electronic storage of such  
185 communications.

186 “Electronic, mechanical, or other device” means any device or apparatus which can be  
187 used to intercept a wire, oral, or electronic communication other than:

188 (1) any telephone or telegraph instrument, equipment or facility, or any component  
189 thereof:

190 (A) furnished to the subscriber or user by a provider of wire or electronic communication  
191 service or commercial entity in the ordinary course of its business, and being used by the  
192 subscriber or user in the ordinary course of its business, or furnished by such subscriber or user  
193 for connection to the facilities of such service and used in the ordinary course of its business; or

194 (B) being used by a provider of wire or electronic communication service in the ordinary  
195 course of its business, or by an investigative or law enforcement officer in the ordinary course of  
196 the officer’s duties; or

197 (C) a hearing aid or similar device being used to correct subnormal hearing to not better  
198 than normal.

199 “Electronic storage” means:

200 (1) any temporary, intermediate storage of a wire or electronic communication incidental  
201 to the electronic transmission thereof; and

202 (2) any storage of such communication by an electronic communication service for  
203 purposes of backup protection of such communication.

204           “Financial institution” means a bank, as defined in section 1 of chapter 167 , and an  
205 investment bank, securities broker, securities dealer, investment adviser, mutual fund, investment  
206 company or securities custodian as defined in section 1.165-12(c)(1) of the United States  
207 Treasury Regulations.

208           “Intercept” means the secret acquisition of aural or other secret acquisition of the  
209 contents of any wire, electronic or oral communication through the use of any electronic,  
210 mechanical, or other device; provided that it shall not constitute an interception for an  
211 investigative or law enforcement officer, as defined in this section, to record or transmit a wire,  
212 electronic or oral communication if the officer is a party to such communication or has been  
213 given prior authorization to record or transmit the communication by such a party and if recorded  
214 or transmitted in the course of an investigation of any offense described in section 7, and a  
215 judicial official authorized to issue warrants pursuant to chapter 276 determines that there is  
216 probable cause that evidence of such a crime will be recorded or transmitted. Any such warrant  
217 shall be valid for no greater than 15 days from the date of issue.

218           “Investigative or law enforcement officer” means any officer of the federal government,  
219 the state or political subdivision thereof, who is empowered by law to conduct investigations of  
220 or to make arrests for offenses enumerated in this section, and any attorney authorized by law to  
221 prosecute or participate in the prosecution of such offenses.

222           “Judge of competent jurisdiction” means any judge of the superior court of the  
223 commonwealth.

224           “Oral communication” means any verbal communication uttered by a person exhibiting  
225 an expectation that such communication is not subject to interception under circumstances  
226 justifying such expectation. However, such term excludes any electronic communication.

227           “Pen register” means a device or process which records or decodes dialing, routing,  
228 addressing, or signaling information transmitted by an instrument or facility from which a wire  
229 or electronic communication is transmitted, provided, however, that such information shall not  
230 include the contents of any communication. Such term excludes any device or process used by a  
231 provider or customer of a wire or electronic communication service for billing, or recording as an  
232 incident to billing, for communications services provided by such provider of any device used by  
233 a provider, or any device or process used by a provider or customer of a wire or electronic  
234 communication service for billing, cost accounting or other like purposes in the ordinary course  
235 of its business.

236           “Person” means any employee, or agent of the United States or any state or political  
237 subdivision thereof, and any individual, partnership, association, joint stock company, trust, or  
238 corporation.

239           “Readily accessible to the general public” means, with respect to a radio communication,  
240 that such communication is not:

241           (1) scrambled or encrypted;

242           (2) transmitted using modulation techniques whose essential parameters have been  
243 withheld from the public with the intention of preserving the privacy of such communication;

244           (3) carried on a subcarrier or other signal subsidiary to a radio transmission;

245 (4) transmitted over a communication system provided by a common carrier, unless the  
246 communication is a tone only paging system communication; or

247 (5) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or  
248 part 94 of the Rules of the Federal Communications Commission, unless, in the case of a  
249 communication transmitted on a frequency allocated under part 74 that is not exclusively  
250 allocated to broadcast auxiliary services, the communication is a two-way voice communication  
251 by radio.

252 “Trap and trace device” means a device or process which captures the incoming  
253 electronic or other impulses which identify the originating number or other dialing, routing,  
254 addressing, and signaling information reasonably likely to identify the source of a wire or  
255 electronic communication, provided, however, that such information shall not include the  
256 contents of any communication. Provided, however, that any caller identification device  
257 lawfully installed shall be excluded from this definition.

258 “User” means any person or entity who:

259 (1) uses an electronic or wire communication service; and

260 (2) is duly authorized by the provider of such service to engage in such use.

261 “Wire communication” means any aural transfer made in whole or in part through the use  
262 of facilities for the transmission of communications by the aid of wire, cable, or other like  
263 connection between the point of origin and the point of reception, including the use of such  
264 connection in a switching station, furnished or operated by any person engaged in providing or

265 operating such facilities for the transmission of intrastate, interstate or foreign communications  
266 or communications affecting intrastate, interstate or foreign commerce.

267 Section 3. Unlawful Interception and Disclosure of Wire, Oral, or Electronic  
268 Communications

269 (a) Except as provided in subsection (d), it is unlawful for a person to intentionally:

270 (1) intercept, endeavor to intercept, or procure any other person to intercept or endeavor  
271 to intercept, any wire, oral, or electronic communication;

272 (2) use, endeavor to use, or procure any other person to use or endeavor to use any  
273 electronic, mechanical, or other device to intercept any oral communication when:

274 (A) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or  
275 other like connection used in wire or electronic communications; or

276 (B) such device transmits communications by radio, or interferes with transmission of  
277 such communication.

278 (3) disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or  
279 electronic communication, knowing or having reason to know that the information was obtained  
280 through the interception of a wire, oral, or electronic communication in violation of this  
281 subsection; or

282 (4) use, or endeavor to use, the contents of any wire, oral, or electronic communication,  
283 knowing or having reason to know that the information was obtained through the interception of  
284 a wire, oral, or electronic communication in violation of this subsection; or

285 (5) edit, alter or tamper with any tape, transcription or recording of wire, oral, or  
286 electronic communications by any means, or attempt to edit, alter or tamper with any tape,  
287 transcription or recording of wire, oral, or electronic communications by any means with the  
288 intent to present in any judicial proceeding or proceeding under oath, or present such recording  
289 or permit such recording to be presented in any judicial proceeding or proceeding under oath,  
290 without fully indicating the nature of the changes made in the original state of the recording.

291 (b) Proof of the installation of any intercepting device by any person under circumstances  
292 evincing an intent to commit an interception, which is not authorized or permitted by this  
293 section, shall be prima facie evidence of a violation of this subsection.

294 (c) Any person who violates subsection (a) and any person who permits or on behalf of  
295 any other person commits or attempts to commit, or any person who participates in a conspiracy  
296 to commit or attempt to commit, or any accessory to a person who commits a violation of  
297 subsection (a) shall be punished as provided in subsection (f) or shall be subject to suit as  
298 provided in Section 17.

299 (d) It shall be lawful under this section for :

300 (1) an operator of a switchboard, or an officer, employee, or agent of a provider of wire  
301 or electronic communication service, whose facilities are used in the transmission of a wire or  
302 electronic communication, to intercept, disclose, or use that communication in the normal course  
303 of that person's employment while engaged in any activity which is a necessary incident to the  
304 rendition of that person's service or to the protection of the rights or property of the provider of  
305 that service, or which is necessary to prevent the use of such facilities in violation of section  
306 fourteen A of chapter two hundred and sixty-nine of the general laws; except that a provider of

307 wire or electronic communication service to the public shall not utilize service observing or  
308 random monitoring except for mechanical or service quality control checks;

309 (2) (A) providers of wire or electronic communication service, their officers, employees,  
310 and agents, landlords, custodians, or other persons, to provide information, facilities, or technical  
311 assistance to persons authorized by law to intercept wire, oral, or electronic communications or  
312 to conduct electronic surveillance, if such provider, its officers, employees, or agents, landlord,  
313 custodian, or other specified person, has been provided with:

314 (i) a court order directing such assistance signed by the authorizing judge; or

315 (ii) a certification in writing by the attorney for the state that no warrant or court order is  
316 required by law, that all statutory requirements have been met, and that the specified assistance is  
317 required. The certification shall set forth the period of time during which the provision of  
318 information, facilities, or technical assistance is authorized and specifying the information,  
319 facilities, or assistance required;

320 (B) No provider of wire or electronic communication service, officer, employee, or agent  
321 thereof, or landlord, custodian, or other specified person shall disclose the existence of any  
322 interception or surveillance or the device used to accomplish the interception or surveillance with  
323 respect to which the person has been furnished a court order or certification under this section,  
324 except as may otherwise be required by legal process and then only after prior notification to the  
325 attorney for the state as may be appropriate. Any such disclosure, shall render such person liable  
326 for the civil damages provided for in section 17.

327 (C) No cause of action shall lie in any court against any provider of wire or electronic  
328 communication service, its officers, employees, or agents, landlord, custodian, or other specified



329 person for providing information, facilities, or assistance in accordance with the terms of a court  
330 order or certification under this section.

331 (3) a person to intercept or access an electronic communication made through an  
332 electronic communication system that is configured so that such electronic communication is  
333 readily accessible to the general public;

334 (4) a person to intercept any radio communication which is transmitted:

335 (A) by any station for the use of the general public, or that relates to ships,  
336 aircraft, vehicles, or persons in distress;

337 (B) by any governmental, law enforcement, civil defense, private land mobile, or  
338 public safety communications system, including police and fire, readily accessible to the general  
339 public;

340 (C) by a station operating on an authorized frequency within the bands allocated  
341 to the amateur, citizens band, or general mobile radio service; or

342 (D) by any marine or aeronautical communications system;

343 (5) a person to engage in any conduct which:

344 (A) is prohibited by Section 633 of the Communications Act of 1934; or

345 (B) is excepted from the applications of Section 705(a) of the Communications  
346 Act of 1934 by Section 705(b) of that Act;

347 (6) a person to intercept any wire or electronic communication the transmission of which  
348 is causing harmful interference to any lawfully operating station or consumer electronic  
349 equipment, to the extent necessary to identify the source of such interference;

350 (7) other users of the same frequency to intercept any radio communication made through  
351 a system that utilized frequencies monitored by individuals engaged in the provision or the use of  
352 such system, if such communication is not scrambled or encrypted;

353 (8) a person to use a pen register or a trap and trace device in accordance with the  
354 provisions defined in this section;

355 (9) a provider of electronic communication service to record the fact that a wire or  
356 electronic communication was initiated or completed in order to protect such provider, another  
357 provider furnishing service toward the completion of the wire or electronic communication, or a  
358 user of that service, from fraudulent, unlawful or abusive use of such service;

359 (10) investigative and law enforcement officers of the United States of America to violate  
360 the provisions of this section if acting pursuant to authority of the laws of the United States and  
361 within the scope of their authority;

362 (11) any person duly authorized to make specified interceptions by a warrant issued  
363 pursuant to this section;

364 (12) investigative or law enforcement officers to violate the provisions of this section for  
365 the purposes of ensuring the safety of any law enforcement officer or agent thereof who is acting  
366 in an undercover capacity, or as a witness for the commonwealth; provided, however, that any

367 such interception which is not otherwise permitted by this section shall be deemed unlawful for  
368 purposes of section 9(o);

369 (13) a financial institution to record telephone communications with its corporate or  
370 institutional trading partners in the ordinary course of its business; provided, however, that such  
371 financial institution shall establish and maintain a procedure to provide semi-annual written  
372 notice to its corporate and institutional trading partners that telephone communications over  
373 designated lines will be recorded;

374 (14) a person acting under color of law to intercept the wire or electronic communications  
375 of a computer trespasser transmitted to, through or from a computer, if:

376 (A) the owner or operator of the computer authorizes the interception of the  
377 computer trespasser's communication on the computer;

378 (B) the person acting under color of law is lawfully engaged in an investigation;

379 (C) the person acting under color of law has reasonable grounds to believe that the  
380 contents of the computer trespasser's communications will be relevant to the investigation; and

381 (D) such interception does not acquire communications other than those  
382 transmitted to or from the computer trespasser;

383 (15) any investigative or law enforcement officer, specially designated by the Attorney  
384 General or a District Attorney, who reasonably determines that an emergency situation exists that  
385 involves immediate danger of death or serious physical injury to any person, and there are  
386 grounds upon which an order could be entered under this section to authorize such interception,  
387 may intercept such wire, oral, or electronic communication if an application for an order

388 approving the interception is made in accordance with this section within forty-eight hours after  
389 the interception has occurred, or begins to occur. In the absence of an order, such interception  
390 shall immediately terminate when the communication sought is obtained or when the application  
391 for the order is denied, whichever is earlier. In the event such application for approval is denied,  
392 the contents of any wire, oral, or electronic communication intercepted shall be subject to the  
393 prohibitions set forth in section 6 and the civil remedies of section 17. No such violation shall be  
394 subject to criminal penalties.

395 (16) for an employee of:

396 (A) an ambulance service licensed pursuant to the General Laws, a fire station  
397 employing firefighters, as defined by the General Laws, a law enforcement agency as defined by  
398 this section, or any other entity with published emergency telephone numbers; or

399 (B) an agency operating an emergency telephone number "911" system  
400 established pursuant to the General Laws, to intercept and record incoming wire and electronic  
401 communications; however, such employee may intercept and record incoming wire and  
402 electronic communications to designated "911" telephone numbers and published non-  
403 emergency telephone numbers staffed by trained dispatchers at public safety answering points  
404 only. It is also lawful for such employee to intercept and record outgoing wire or electronic  
405 communications to the numbers from which such incoming wire or electronic communications  
406 were placed when necessary to obtain information required to provide the emergency services  
407 being requested.

408 (e) (1) Except as provided in paragraph (2) of this subsection, a person or entity  
409 providing an electronic communication service to the public shall not intentionally divulge the

410 contents of any communication, other than one to such person or entity, or an agent thereof,  
411 while in transmission on that service to any person or entity other than an addressee or intended  
412 recipient of such communication or an agent of such addressee or intended recipient.

413 (2) A person or entity providing electronic communication service to the public may  
414 divulge the contents of any such communication:

415 (A) as otherwise authorized in subsection 3(d) or 8 of this section;

416 (B) with the lawful consent of the originator or any addressee or intended recipient of  
417 such communication;

418 (C) to a person employed or authorized, or whose facilities are used, to forward such  
419 communication to its destination; or

420 (D) which were inadvertently obtained by the service provider and which appear to  
421 pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

422 (f) Except as otherwise specifically provided in this section, any person who willfully  
423 commits an interception, attempts to commit an interception, or procures any other person to  
424 commit an interception or to attempt to commit an interception of any wire, oral or electronic  
425 communication shall be fined not more than ten thousand dollars, or imprisoned in the state  
426 prison for not more than five years, or imprisoned in a jail or house of correction for not more  
427 than two and one half years, or both so fined and given one such imprisonment.

428 Section 4. Unlawful Manufacture, Distribution, Possession, and Advertising of Wire,  
429 Oral, or Electronic Communication Intercepting Devices.

430 (a) Except as provided in subsection (e), it is unlawful for any person to intentionally:

431 (1) transport or transmit any electronic, mechanical, or other device, knowing or  
432 having reason to know that the design of such device renders it primarily useful for the purpose  
433 of the surreptitious interception of wire, oral, or electronic communications, or knowing or  
434 having reason to know that the device is intended for surreptitious interception of wire, oral, or  
435 electronic communications; or

436 (2) manufacture, assemble, possess, or sell any electronic, mechanical, or other  
437 device, knowing or having reason to know that the design of such device renders it primarily  
438 useful for the purpose of the surreptitious interception of wire, oral, or electronic  
439 communications, or knowing or having reason to know that the device is intended for  
440 surreptitious interception of wire, oral, or electronic communications; or

441 (3) place in any newspaper, magazine, handbill, or other publication any  
442 advertisement of:

443 (A) any electronic, mechanical, or other device, knowing or having reason to know that  
444 the design of such device renders it primarily useful for the purpose of surreptitious interception  
445 of wire, oral, or electronic communications, or knowing or having reason to know that the device  
446 is intended for surreptitious interception of wire, oral, or electronic communications; or

447 (B) any other electronic, mechanical, or other device, where such advertisement promotes  
448 the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic  
449 communications.

450 (b) A person who violates subsection (a) shall be fined not more than \$10,000, or  
451 imprisoned not more than five years in state prison or not more than two and one half year in a  
452 jail or house of correction, or both such fine and imprisonment.

453 (c) The installation of any such intercepting device by such person or with his permission  
454 or at his direction shall be prima facie evidence of possession as required by subsection (a).

455 (d) Any person who permits or on behalf of any other person commits or attempts to  
456 commit, or any person who participates in a conspiracy to commit or attempt to commit, or any  
457 accessory to a person who commits a violation of subsection (a) shall be punished in the same  
458 manner as is provided for the respective offenses as described in subsection (b).

459 (e) Notwithstanding subsection (a), it shall be lawful for a person to transport, or  
460 manufacture, assemble, possess, or sell any electronic, mechanical, or other device, knowing or  
461 having reason to know that the design of such device renders it primarily useful for the purpose  
462 of the surreptitious interception of wire, oral, or electronic communications, or knowing or  
463 having reason to know that the device is intended for surreptitious interception of wire, oral, or  
464 electronic communications, if the person is:

465 (1) a provider of wire or electronic communication service or an officer, agent, or  
466 employee of, or a person under contract with, such a provider, in the normal course of the  
467 business of providing that wire or electronic communication service; or

468 (2) an officer, agent, or employee of, or a person under contract with, bidding  
469 upon contracts with, or in the course of doing business with, the United States, a state, or a  
470 political subdivision thereof, in the normal course of the activities of the United States, a state, or  
471 a political subdivision thereof.

472 Section 5. Confiscation of Wire, Oral, or Electronic Communication Interception  
473 Devices.

474           Upon conviction of a violation of this section, any electronic, mechanical, or other device  
475 used, sent, carried, manufactured, assembled, possessed or sold in violation of this section may  
476 be confiscated by the commonwealth and forwarded, by the authority of the written order of the  
477 court to the colonel of the state police, who shall destroy said article.

478           Section 6. Prohibition of Use as Evidence of Intercepted Wire, Oral or Electronic  
479 Communications.

480           No part of the contents of any wire, oral or electronic communication intercepted in  
481 violation of this section, and no evidence derived therefrom, may be received in evidence in any  
482 trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency,  
483 regulatory body, legislative committee, or other authority of this state, or political subdivision  
484 thereof, if the disclosure of that information would be in violation of this section unless a judge  
485 determines, pursuant to section 9(o) of this act or because it is in the interest of justice, that  
486 exclusion from evidence is not required.. The prohibition of use as evidence provided in this  
487 section does not apply in cases of prosecution for criminal interception in violation of the  
488 provisions of this section.

489           Section 7. Authorization for Interception of Wire, Oral, or Electronic Communications.

490           (a) The attorney for the state may authorize an application to a judge of competent  
491 jurisdiction for, and such judge may grant in conformity with section 9 of this act an order  
492 authorizing the interception of wire, oral or electronic communications by an investigative or law  
493 enforcement officer, or an agency having responsibility for the investigation of the offense as to  
494 which the application is made, when such interception may provide or has provided evidence of:

495           (1) any offense which involves murder, kidnapping, robbery, or extortion;



496 (2) any of the following offenses: arson, assault and battery with a dangerous  
497 weapon, a violation of section 13 A(b) of section two hundred and sixty-five, bribery, a violation  
498 of section 2 of chapter two hundred sixty-eight A, burglary, misuse of credit cards or fraudulent  
499 use of credit cards to obtain money, goods or services, malicious destruction of property,  
500 embezzlement, enterprise crime, escape, throwing or placing explosives at or near persons or  
501 property, illegal possession or storage of explosives, possession of infernal machines, forgery,  
502 gaming violations, identity fraud in violation of section 37E of chapter two hundred sixty-six of  
503 the general laws, indecent assault and battery, insurance fraud, intimidation of witnesses or jurors  
504 or persons furnishing information in connection with criminal proceedings, larceny, lending of  
505 money or things of value in violation of the general laws, mayhem, money laundering, perjury,  
506 subornation of perjury, prostitution, rape, receiving stolen property, communicating terroristic  
507 threats, possessing or using chemical, biological or nuclear weapons, possession or use of hoax  
508 substances crimes involving violations of: gambling and lottery laws, gift laws, liquor laws,  
509 tobacco laws, firearms laws, securities laws, lobbying laws, ethics laws, or conflict of interest  
510 laws.

511 (3) any offense involving the possession or distribution of a narcotic drug,  
512 marijuana, or other dangerous drug;

513 (4) coercion of child under eighteen into criminal conspiracy, inducing person  
514 under eighteen to have sexual intercourse, possession or dissemination of matter harmful to  
515 minors, posing or exhibiting child in state of nudity or sexual conduct, dissemination of visual  
516 material of child in state of nudity or sexual conduct, purchase or possession of visual material of  
517 child depicted in sexual conduct;

518 (5) any offense punishable by imprisonment for more than one year involving the  
519 possession or distribution of firearms;

520 (6) any accessory to any offense described in this act or any conspiracy or attempt  
521 or solicitation to commit any offense described in this act;

522 (7) the location of any fugitive from justice from an offense described in this  
523 subsection

524 Section 8. Authorization for Disclosure and Use of Intercepted Wire, Oral, and Electronic  
525 Communications.

526 (a) Any investigative or law enforcement officer who, by any means authorized by this  
527 section, has obtained knowledge of the contents of any wire, oral, or electronic communication,  
528 or evidence derived therefrom, may:

529 (1) disclose such contents to another investigative or law enforcement officer to  
530 the extent that such disclosure is appropriate to the proper performance of the official duties of  
531 the officer making or receiving the disclosure; or

532 (2) use such contents to the extent such use is appropriate to the proper  
533 performance of the officer's official duties.

534 (b) Any person who has received, by any means authorized by this section, any  
535 information concerning a wire, oral, or electronic communication, or evidence derived  
536 therefrom, intercepted in accordance with the provisions of this section may disclose the contents  
537 of that communication or such derivative evidence while giving testimony under oath or

538 affirmation in any proceeding in any court of the United States or of any state or in any federal or  
539 state grand jury proceeding.

540 (c) No otherwise privileged wire, oral, or electronic communication intercepted in  
541 accordance with, or in violation of, the provisions of this section shall lose its privileged  
542 character.

543 (d) Except as otherwise specifically provided in this section, any person who willfully  
544 discloses to any person, any information concerning or contained in, the application for, the  
545 granting or denial of orders for interception, renewals, notice or return on an ex parte order  
546 granted pursuant to this section, or the contents of any document, tape, or recording kept in  
547 accordance with Section 9 (m), shall be guilty of a misdemeanor punishable by imprisonment in  
548 a jail or house of correction for not more than two years or by a fine of not more than five  
549 thousand dollars or both.

550 Section 9. Procedure for Interception of Wire, Oral, or Electronic Communications

551 (a) An application for a warrant authorized by this section must be made by an attorney  
552 for the state to a judge of competent jurisdiction in the county where the interception is to occur,  
553 or the county where the office of the applicant is located, or in the event that there is no judge of  
554 competent jurisdiction sitting in said county at such time, to a judge of competent jurisdiction  
555 sitting in Suffolk County; except that for these purposes, the office of the attorney general shall  
556 be deemed to be located in Suffolk County.

557 (b) Each application for an order authorizing or approving the interception of a wire, oral,  
558 or electronic communication under this section shall be made in writing upon oath or affirmation  
559 and shall state:

560 (1) the identity of the investigative or law enforcement officer making the  
561 application, and the officer authorizing the application;

562 (2) the applicant's authority to make such application;

563 (3) fully and completely the facts and circumstances relied upon by the applicant,  
564 to justify the applicant's belief that an order should be issued, including:

565 (A) details as to the particular offense that has been, is being, or is about to  
566 be committed;

567 (B) except as provided in subsection (p) of this section, a description of  
568 the nature and location of the facilities from which or the place where the communication is to be  
569 intercepted;

570 (C) a particular description of the type of communications sought to be  
571 intercepted and that such communications are not legally privileged; and

572 (D) the identity of the person, if known, committing the offense and whose  
573 communications are to be intercepted.

574 (4) whether or not other investigative procedures have been tried and failed or  
575 why they reasonably appear unlikely to succeed if tried or otherwise might be too dangerous;

576 (5) the period of time for which the interception is required to be maintained. If  
577 the nature of the investigation is such that the authorization for the interception should not  
578 automatically terminate when the described oral, wire, or electronic communications have been  
579 first obtained, the application must specifically state facts establishing probable cause to believe  
580 that additional oral, wire, or electronic communications of the same nature will occur thereafter;

581 (6) the facts concerning all previous applications known to the individual  
582 authorizing and making the application, made to any judge for authorization to intercept, or for  
583 approval of interceptions of, wire, oral, or electronic communications involving any of the same  
584 persons, facilities or places specified in the application, and the action taken by the judge on each  
585 such application;

586 (7) where the application is for the extension of an order, the results thus far  
587 obtained from the interception, or a reasonable explanation of the failure to obtain such results;  
588 and

589 (8) if it is reasonably necessary to make a secret entry upon a private place and  
590 premises in order to install an intercepting device to effectuate the interception, a statement to  
591 such effect.

592 (c) The judge may require the applicant to furnish additional testimony or documentary  
593 evidence in support of the application. A verbatim transcript of every such interrogation or  
594 examination must be taken, and a transcription of the same, sworn to by the stenographer, shall  
595 be attached to the application and be deemed a part thereof.

596 (d) Upon such application the judge may enter an ex parte order, as requested or as  
597 modified, authorizing or approving interception of wire, oral, or electronic communications  
598 within the state, if the judge determines on the basis of the facts submitted by the applicant that:

599 (1) there is probable cause for belief that an individual is committing, has  
600 committed, or is about to commit a particular offense enumerated in section 7 of this act;

601 (2) there is probable cause for belief that particular communications concerning  
602 that offense will be obtained through such interception;

603 (3) normal investigative procedures have been tried and failed or reasonably  
604 appear unlikely to succeed if tried or may otherwise be too dangerous; and

605 (4) except as provided in subsection (p), there is probable cause for belief that the  
606 facilities from which, or the place where, the wire, oral, or electronic communications are to be  
607 intercepted are being used, or are about to be used, in connection with the commission of such  
608 offense, or are leased to, listed in the name of, or commonly used by such person.

609 (e) Each order authorizing or approving the interception of any wire, oral, or electronic  
610 communication under this section shall specify:

611 (1) the subscription and title of the issuing judge;

612 (2) the identity of the person, if known, whose communications are to be  
613 intercepted;

614 (3) the nature and location of the communications facilities as to which, or the  
615 place where, authority to intercept is granted;

616 (4) a particular description of the type of communication sought to be intercepted,  
617 and a statement of the particular offense to which it relates;

618 (5) the identity of the agency authorized to intercept the communications, and of  
619 the person authorizing the application;

620 (6) the period of time during which such interception is authorized; and

621 (7) an express authorization to make secret entry upon a private place or premises  
622 to install a specified intercepting device, if such entry is necessary to execute the warrant.

623 (f) An order authorizing the interception of a wire, oral, or electronic communication  
624 under this section shall, upon request of the applicant, direct that a provider of wire or electronic  
625 communication service, landlord, custodian, or other person shall furnish the applicant forthwith  
626 all information, facilities, and technical assistance necessary to accomplish the interception  
627 unobtrusively and with a minimum of interference with the services that such service provider,  
628 landlord, custodian, or person is according the person whose communications are to be  
629 intercepted. Any provider of wire or electronic communication service, landlord, custodian or  
630 other person furnishing such facilities or technical assistance shall be compensated therefor by  
631 the applicant for reasonable expenses incurred in providing such facilities or assistance.

632 (g) An order entered under this section may authorize or approve the interception of any  
633 wire, oral, or electronic communication for the shorter of 30 days or the period necessary to  
634 achieve the objective of the authorization. Such 30 day period begins on the earlier of the day on  
635 which the investigative or law enforcement officer first begins to conduct an interception under  
636 the order or ten days after the order is entered, whichever occurs earliest. Extensions of an order  
637 may be granted only upon application for an extension made in accordance with subsection (b)  
638 of this section and the court making the findings required by subsection (d) of this section. The  
639 period of extension shall be the shorter of 30 days or the time the authorizing judge deems  
640 necessary to achieve the purposes for which it was granted. Every order and extension thereof  
641 shall contain a provision that the authorization to intercept shall be executed as soon as  
642 practicable, shall be conducted in such a way as to minimize the interception of communications  
643 not otherwise subject to interception under this section, and must terminate upon the earlier of 30

644 days or the attainment of the authorized objective. In the event the intercepted communication is  
645 in a code or a foreign language, and an expert in that foreign language or code is not reasonably  
646 available during the interception period, minimization may be accomplished as soon as  
647 practicable after such interception of the communication in full.

648 (h) An interception under this section may be conducted in whole or in part by federal,  
649 state, county or municipal personnel, or by an individual operating under a contract with the  
650 state, county or municipality acting under the supervision of an investigative or law enforcement  
651 officer authorized to conduct the interception.

652 (i) Whenever an order authorizing interception is entered pursuant to this section, the  
653 order may require reports to be made to the judge who issued the order showing what progress  
654 has been made toward achievement of the authorized objective and the need for continued  
655 interception. Such reports shall be made at intervals as the judge may require.

656 (j) Notwithstanding any other provision of this section, any investigative or law  
657 enforcement officer, specially designated by the attorney for the state, may intercept a wire, oral,  
658 or electronic communication prior to issuance of an order approving the interception if the  
659 officer reasonably determines that:

660 (A) an emergency situation exists that involves immediate danger of death or  
661 serious physical injury to any person or the danger of escape of a prisoner; and there are grounds  
662 upon which an order could be entered under this section to authorize such interception; and

663 (B) an application for an order approving the interception is made in accordance  
664 with this section within 48 hours after the interception has occurred, or begins to occur.



665 (k) In the absence of an order approving an interception described in subsection (j), such  
666 interception shall immediately terminate upon the earlier of obtainment of the communication  
667 sought or denial of the application.

668 (l) In the event an application for approval of an interception described in subsection (j) is  
669 denied, or in any other case where the interception is terminated without an order having been  
670 issued, the contents of any wire, oral, or electronic communication intercepted shall be subject to  
671 the prohibitions set forth in section 6 and the civil remedies of section 17. No such violation  
672 shall be subject to criminal penalties.

673 (m) (1) The contents of any wire, oral, or electronic communication intercepted by any  
674 means authorized by this section shall, if possible, be recorded on tape or wire or other  
675 comparable device. Upon examination of the return and a determination that it complies with  
676 this section, the issuing judge shall forthwith order that the application, all renewal applications,  
677 warrant, all renewal orders and the return thereto be transmitted to the chief justice by such  
678 persons as he shall designate. The application, all renewal applications, warrant, all renewal  
679 orders and the return shall be stored in a secure place which shall be designated by the chief  
680 justice, to which access shall be denied to all persons except the chief justice or such court  
681 officers or administrative personnel of the court as he shall designate.

682 The recordings shall not be destroyed except upon an order of the issuing or denying  
683 judge and in any event shall be kept for ten years. Notice prior to the destruction shall be given  
684 to the applicant attorney general or his successor or the applicant district attorney or his  
685 successor and upon a showing of good cause to the chief justice, the application, warrant,  
686 renewal and return may be kept for such additional period as the chief justice shall determine but

687 in no event longer than the longest period of limitation for any designated offense specified in  
688 the warrant, after which time they must be destroyed by a person designated by the chief justice.  
689 Duplicate recordings may be made for use or disclosure pursuant to the provisions of section 8(a)  
690 or (b) of this section

691 (2) Applications made and orders granted under this section shall be sealed by the judge.  
692 Such applications and orders shall be disclosed only upon a showing of good cause before a  
693 judge of competent jurisdiction and shall not be destroyed except on order of the issuing or  
694 denying judge, and in any event shall be kept for ten years.

695 (3) Except as otherwise provided in subparagraph (a), within a reasonable time, not to  
696 exceed 90 days, after the filing of an application for an order of approval under subsection (1)  
697 which is denied, or the termination of the period of an order or extensions thereof, an  
698 investigative or law enforcement officer of the commonwealth shall serve an attested copy of the  
699 warrant or the renewal on the persons named in the warrant, and such other aggrieved persons  
700 who shall reasonably be known to the person who obtained the warrant as a result of information  
701 obtained from an authorized interception. The attested copy of the warrant shall be served by  
702 leaving the same at his usual place of abode, or in hand, or if this is not possible by mailing the  
703 same by certified or registered mail to his last known place of abode. A return of service shall be  
704 made to the issuing judge, except, that if such service is postponed as provided in this  
705 subparagraph, it shall be made to the chief justice. The return of service shall be deemed a part  
706 of the return of the warrant and attached thereto.

707 (a) Upon an ex parte showing of important special facts which set forth the need for  
708 continued secrecy to the satisfaction of the issuing judge, said judge may direct that the attested

709 copy of the warrant be served on such parties as are required by this subsection at such time as  
710 may be appropriate in the circumstances but in no event may he it to be served later than three  
711 years from the time of expiration of the warrant or the last renewal thereof.

712 (b) The judge, upon the filing of a motion, may make available to such person or such  
713 person's counsel for inspection such portions of the intercepted communications, applications  
714 and orders as the judge determines to be in the interest of justice.

715 (n) The contents of any wire, oral or electronic communication intercepted pursuant to  
716 this section, or evidence derived therefrom, shall not be received in evidence or otherwise  
717 disclosed in any trial, hearing, or other proceeding in a court of the commonwealth unless each  
718 party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a  
719 copy of the court order and accompanying application under which the interception was  
720 authorized or approved and a complete copy of each recording or a statement under oath of the  
721 evidence overheard as a result of the transmission which the commonwealth intends to offer in  
722 evidence. This ten day period may be waived by the judge if the judge finds that it was not  
723 possible to furnish the party with the above information ten days before the trial, hearing or  
724 proceeding and that the party will not be prejudiced by the delay in receiving such information.

725 (o) Any aggrieved person who is a party in any trial, hearing, or proceeding in or before  
726 any court, department, officer, agency, regulatory body, or other authority of this state, or a  
727 political subdivision thereof, may move to suppress the contents of any wire, oral or electronic  
728 communication intercepted pursuant to this section, or evidence derived therefrom, on the  
729 grounds that:

730 (1) the communication was unlawfully intercepted;

731 (2) the application or renewal failed to set forth facts sufficient to establish  
732 probable cause for the issuance of the warrant;

733 (3) the order of authorization or approval under which it was intercepted is  
734 insufficient on its face or does not conform with the provisions of this chapter; or

735 (4) the interception was not made in conformity with the order of authorization or  
736 approval.

737 Such motion shall be made before the trial, hearing, or proceeding unless there was no  
738 opportunity to make such motion or the person was not aware of the grounds of the motion. If  
739 the motion is granted, the contents of the intercepted wire or oral communication, or evidence  
740 derived therefrom, shall be suppressed.

741 (p) The requirements of subsection (d)(4) of this section relating to the specification of  
742 the facilities from which, or the place where, the communication is to be intercepted are  
743 inapplicable if:

744 (1) in the case of an application with respect to the interception of an oral  
745 communication:

746 (A) the application is by an investigative or law enforcement officer and is  
747 approved by the attorney for the state;

748 (B) the application contains a full complete statement as to why such  
749 specification is not practical and identifies the person committing the offenses and whose  
750 communications are to be intercepted; and

751 (C) the judge finds that such specification is not practical; and

752 (2) in the case of an application with respect to a wire or electronic communication:

753 (A) the application is by an investigative or law enforcement officer and is  
754 approved by the attorney for the state;

755 (B) the application identifies the person believed to be committing the offense and  
756 whose communications are to be intercepted and the applicant makes a showing of a purpose, on  
757 the part of that person, to thwart interception by changing facilities; and

758 (C) the judge finds that such purpose has been adequately shown.

759 (q) An interception of a communication under an order to which the requirements of  
760 subsection (d)(4) of this section do not apply by reason of subsection (p) shall not begin until the  
761 facilities from which, or the place where, the communication is to be intercepted is ascertained  
762 by the person implementing the interception order. A provider of wire or electronic  
763 communication service that has received an order as provided for in subsection (p)(2) may move  
764 the court to modify or quash the order on the ground that its assistance with respect to the  
765 interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the  
766 state, shall decide such a motion expeditiously.

767 Section 10. Warrant Return

768 Within seven days after termination of the warrant or the last renewal thereof, a return  
769 must be made thereon to the judge issuing the warrant by the applicant therefor, containing the  
770 following:

771 (a) A statement of the nature and location of the communications facilities, if any, and  
772 premise or places where the interceptions were made; and

773 (b) The periods of time during which such interceptions were made; and  
774 (c) The names of the parties to the communications intercepted if known; and  
775 (d) The original recording of the oral, wire or electronic communications intercepted, if  
776 any; and

777 (e) A statement attested under the pains and penalties of perjury by each person who  
778 heard oral or wire communications as a result of the interception authorized by the warrant,  
779 which were not recorded, stating everything that was overheard to the best of his recollection at  
780 the time of the execution of the statement.

781 Section 11. General Prohibition on Pen Register and Trap and Trace Device Use;  
782 Exceptions.

783 (a) Except as provided in section 15(b) of this act, no person may install or use a pen  
784 register or a trap and trace device without first obtaining a court order under section 12 of this  
785 act.

786 (b) The prohibition of subsection (a) is inapplicable with respect to the use of a pen  
787 register or a trap and trace device by a provider of electronic or wire communication service:

788 (1) relating to the operation, maintenance, and testing of a wire or electronic  
789 communication service or to the protection of the rights or property of such provider, or to the  
790 protection of users of that service from abuse of service or unlawful use of service; or

791 (2) to record the fact that a wire or electronic communication was initiated or  
792 completed in order to protect such provider, another provider furnishing service toward the

793 completion of the wire or electronic communication, or a user of that service, from fraudulent,  
794 unlawful or abusive use of service; or

795 (3) where the consent of the user of that service has been obtained.

796 (c) A government agency authorized to install and use a pen register or trap and trace  
797 device under sections 11 through 15 shall use technology reasonably available to it that restricts  
798 the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and  
799 signaling information utilized in the processing and transmitting of wire or electronic  
800 communications so as not to include the contents of any wire or electronic communications.

801 (d) A person who knowingly violates subsection (a) shall be fined not more than  
802 \$5,000.00 for each violation, or imprisoned in a jail or house of correction for not more than one  
803 year, or both such fine and imprisonment.

804 Section 12. Application for an Order for a Pen Register or Trap and Trace Device.

805 (a) A state investigative or law enforcement officer authorized by the attorney for the  
806 state may make application in writing under oath or equivalent affirmation to a court of  
807 competent jurisdiction for an order or an extension of an order under section 13 of this section  
808 authorizing or approving the installation and use of a pen register or a trap and trace device under  
809 this section.

810 (b) An application under subsection (a) shall include:

811 (1) the identity of the attorney for the state or the law enforcement or investigative  
812 officer making the application and the identity of the law enforcement agency conducting the  
813 investigation; and

814 (2) a certification under oath by the applicant that the information likely to be  
815 obtained is relevant to an ongoing criminal investigation being conducted by that agency.

816 Section 13. Issuance of an Order for a Pen Register or a Trap and Trace Device.

817 (a) In general:

818 (1) Upon an application made under section 12, the court shall enter an ex parte order  
819 authorizing the installation and use of a pen register or trap and trace device within the  
820 jurisdiction of the court, if the court finds that the State law enforcement or investigative officer  
821 has certified to the court that the information likely to be obtained by such installation and use is  
822 relevant to an ongoing criminal investigation.

823 (2) (A) Where the law enforcement agency implementing an ex parte order under this  
824 subsection seeks to do so by installing and using its own pen register or trap and trace device on  
825 a packet-switched data network of a provider of electronic communication service to the public,  
826 the agency shall ensure that a record will be maintained which will identify:

827 (i) any officer or officers who installed the device and any officer or officers who  
828 accessed the device to obtain information from the network;

829 (ii) the date and time the device was installed, the date and time the device was  
830 uninstalled, and the date, time, and duration of each time the device is accessed to obtain  
831 information;

832 (iii) the configuration of the device at the time of its installation and any  
833 subsequent modification thereof; and

834 (iv) any information which has been collected by the device.



835 To the extent that the pen register or trap and trace device can be set automatically to  
836 record this information electronically, the record shall be maintained electronically throughout  
837 the installation and use of such device.

838 (B) The record maintained under subparagraph (A) shall be provided ex parte and under  
839 seal to the court which entered the ex parte order authorizing the installation and use of the  
840 device within 30 days after termination of the order (including any extensions thereof). Upon  
841 examination of the return and a determination that it complies with this section, the issuing judge  
842 shall forthwith order that the application, all renewal applications, warrant, all renewal orders  
843 and the return thereto be transmitted to the chief justice by such persons as he shall designate.  
844 Their contents shall not be disclosed except as provided in this section. The application, renewal  
845 application(s), warrant(s), the renewal order(s) and the return or any one of them or any part of  
846 them may be transferred to any trial court, grand jury proceeding of any jurisdiction by any law  
847 enforcement or investigative officer or court officer designated by the chief justice and a trial  
848 justice may allow them to be disclosed in accordance with section 8.

849 The application, all renewal applications, warrant, all renewal orders and the return shall  
850 be stored in a secure place which shall be designated by the chief justice, to which access shall  
851 be denied to all persons except the chief justice or such court officers or administrative personnel  
852 of the court as he shall designate.

853 Any violation of the terms and conditions of any order of the chief justice, pursuant to the  
854 authority granted in this paragraph, shall be punished as a criminal contempt of court in addition  
855 to any other punishment authorized by law.

856 (b) An order issued under this section:

857 (1) shall specify:

858 (A) the identity, if known, of the person to whom is leased or in whose name is listed the  
859 telephone line or other facility to which the pen register or trap and trace device is to be attached  
860 or applied;

861 (B) the identity, if known, of the person who is the subject of the criminal investigation;

862 (C) the attributes of the communications to which the order applies, including the number  
863 or other identifier and, if known, the location of the telephone line or other facility to which the  
864 pen register or trap and trace device is to be attached or applied, and, in the case of an order  
865 authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic  
866 limits of the order; and

867 (D) a statement of the offense to which the information likely to be obtained by the pen  
868 register or trap and trace device relates; and

869 (2) shall direct, upon the request of the applicant, the furnishing of information,  
870 facilities, and technical assistance necessary to accomplish the installation of the pen register or  
871 trap and trace device under section 14.

872 (c) An order issued under this section:

873 (1) shall authorize the installation and use of a pen register or a trap and trace device for a  
874 period not to exceed 60 days; and

875 (2) may be granted only upon an application for an order under section 12 of this section  
876 after a judicial finding required by subsection (a). Any period(s) of extension shall not exceed  
877 60 days.

878 (d) An order authorizing or approving the installation and use of a pen register or a trap  
879 and trace device shall direct that:

880 (1) the order be sealed until otherwise ordered by the court;

881 (2) the person owning or leasing the line or other facility to which the pen register or a  
882 trap and trace device is attached or applied, or who is obligated by the order to provide assistance  
883 to the applicant, not disclose the existence of the pen register or trap and trace device or the  
884 existence of the investigation to the listed subscriber, or to any other person, unless or until  
885 otherwise ordered by the court; and

886 (3) a violation of this subsection may be punished as a contempt of the issuing or denying  
887 court.

888 Section 14. Assistance in Installation and Use of a Pen Register or a Trap and Trace  
889 Device.

890 (a) Upon the request of the attorney for the state or an investigative or law enforcement  
891 officer authorized to install and use a pen register under this section, a provider of wire or  
892 electronic communication service, landlord, custodian, or other person shall furnish such  
893 investigative or law enforcement officer forthwith all information, facilities, and technical  
894 assistance necessary to accomplish the installation of the pen register unobtrusively and with a  
895 minimum of interference with the service that the person so ordered by the court accords the  
896 party with respect to whom the installation and use is to take place, if such assistance is directed  
897 by a court order as provided in section 13(b)(2) of this section.

898 (b) Upon the request of the attorney for the state or an investigative or law enforcement  
899 officer authorized to receive the results of a trap and trace device under this section, a provider of  
900 a wire or electronic communication service, landlord, custodian, or other person shall install such  
901 device forthwith on the appropriate line or facility and shall furnish such investigative or law  
902 enforcement officer all additional information, facilities and technical assistance including  
903 installation and operation of the device unobtrusively and with a minimum of interference with  
904 the services that the person so ordered by the court accords the party with respect to whom the  
905 installation and use is to take place, if such installation and assistance is directed by a court order  
906 as provided in section 13(b)(2) of this section. Unless otherwise ordered by the court, the results  
907 of the trap and trace device shall be furnished, pursuant to section 13(b) or section 12 of the act,  
908 to the attorney for the state or the investigative or law enforcement officer, designated in the  
909 court order, at reasonable intervals during regular business hours for the duration of the order.

910 (c) A provider of a wire or electronic communication service, landlord, custodian, or  
911 other person who furnishes facilities or technical assistance pursuant to this section shall be  
912 reasonably compensated for such reasonable expenses incurred in providing such facilities and  
913 assistance.

914 (d) No cause of action shall lie in any court against any provider of a wire or electronic  
915 communication service, its officers, employees, agents, or other specified persons for providing  
916 information, facilities or assistance in accordance with a court order under this section or request  
917 pursuant to section 12 or section 13(b) of this act.

918 (e) A good faith reliance on a court order under this section, a request pursuant to section  
919 12 of this section, a legislative authorization, or a statutory authorization is a complete defense  
920 against any civil or criminal action brought under this section.

921 (f) Any unexcused failure of the provider of an electronic or wire communications  
922 service to comply with a court order under this section or a request pursuant to section 12 may be  
923 punished as a contempt of the issuing court.

924 Section 15. Emergency Pen Register and Trap and Trace Device Installation and Use.

925 (a) Notwithstanding any other provision of this section, any investigative or law  
926 enforcement officer, specially designated by the attorney for the state, may have installed and use  
927 a pen register or trap and trace device if:

928 (1) the officer reasonably determines that an emergency situation exists that involves  
929 immediate danger of death or serious bodily injury to any person or the danger of escape of a  
930 prisoner; and

931 (2) within 48 hours after the installation has occurred, or begins to occur, an order  
932 approving the installation or use is issued in accordance with section 13 of this act.

933 (b) In the absence of an authorizing order, such use shall immediately terminate upon the  
934 earlier of obtainment of the information sought, denial of the application, or the lapse of 48 hours  
935 since the installation of the pen register or trap and trace device.

936 (c) The knowing installation or use by any investigative or law enforcement officer of a  
937 pen register or trap and trace device pursuant to subsection (a) without application for the  
938 authorizing order within 48 hours of the installation shall constitute a violation of this section

939 and shall make such person liable to the penalties outlined in section 11(d) of this act, unless a  
940 court of competent jurisdiction in its discretion determines that the failure to obtain a timely  
941 order pursuant to this section was the result of mitigating or other circumstances.

942 (d) A provider for a wire or electronic service, landlord, custodian, or other person who  
943 furnished facilities or technical assistance pursuant to this section shall be reasonably  
944 compensated for such reasonable expenses incurred in providing such facilities and assistance.

945 (e) No cause of action shall lie in any court against any provider of wire or electronic  
946 communication service, its officers, employees, or agents, landlord, custodian, or other specified  
947 person for providing information, facilities, or assistance in accordance with the terms of this  
948 section.

949 Section 16. Reports Concerning Intercepted Wire, Oral, or Electronic Communications  
950 and Pen Register and Trap and Trace Devices.

951 (a) On the second Friday of January, each year, the attorney general and each district  
952 attorney shall report to the general court:

953 (1) a general description of the interceptions made under such order or extension,  
954 including:

955 (A) the number of applications made for wiretap warrants during the previous year;

956 (B) the name of the applicant;

957 (C) the number of wiretap warrants issued;

958 (D) the effective period of the wiretap warrants;

959 (E) the number and designation of the offenses for which those wiretap applications were  
960 sought, and for each of the designated offenses the following:

961 (i) the number of renewals,

962 (ii) the number of interceptions made during the previous year,

963 (iii) the number of indictments believed to be obtained as a result of those  
964 interceptions,

965 (iv) the number of criminal convictions obtained in trials where interception  
966 evidence or evidence derived therefrom was introduced

967 (2) the number of pen register orders and orders for trap and trace devices applied for by  
968 investigative or law enforcement officers of the state.

969 (b) This report shall be a public document and be made available to the public at the  
970 offices of the attorney general and district attorneys. In the event of failure to comply with the  
971 provisions of this paragraph any person may compel compliance by means of an action of  
972 mandamus.

973 Section 17. Authorized Recovery of Civil Damages.

974 (a) Except as provided in section 3(d), any person whose wire, oral, or electronic  
975 communication is intercepted, disclosed, or intentionally used in violation of this section may in  
976 a civil action recover from the person or entity, other than the United States, the commonwealth  
977 of Massachusetts or any political subdivision thereof, which engaged in that violation such relief  
978 as may be appropriate:

979 (b) In an action under this section, appropriate relief includes:

980 (1) damages under subsection (c) and punitive damages in appropriate cases; and

981 (2) a reasonable attorney's fee and other litigation costs reasonably incurred.

982 (c) The court may assess as damages whichever is the greater of:

983 (1) the sum of the actual damages suffered by the plaintiff and any profits made by the

984 violator as a result of the violation; or

985 (2) \$100 a day for each day of violation; or

986 (3) \$1,000.

987 (d) A complete defense against any civil action brought under this section is a good faith

988 reliance on:

989 (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a

990 statutory authorization;

991 (2) a request of an investigative or law enforcement officer under section 9(j) of this

992 section; or

993 (3) a good faith determination that section 3(d) of this section permitted the conduct

994 complained of.

995 (e) A civil action under this section may not be commenced later than two years after the

996 date upon which the claimant first has a reasonable opportunity to discover the violation

997 Section 18. Severability.



998           If any provisions of this section or application thereof to any person or circumstance is  
999 held invalid, the invalidity does not affect other provisions or applications of the section which  
1000 can be given effect without the invalid provisions or application, and to this end the provisions of  
1001 this section are severable.