

HOUSE No. 3671

The Commonwealth of Massachusetts



CHARLES D. BAKER
GOVERNOR

OFFICE OF THE GOVERNOR
COMMONWEALTH OF MASSACHUSETTS
, MA

KARYN POLITO
LIEUTENANT GOVERNOR

May 2, 2017

To the Honorable Senate and House of Representatives,

Next year will mark the fiftieth anniversary of our state’s wiretap statute. Despite significant advances in technology and significant changes in crime and law enforcement since 1968, the statute has remained virtually unchanged. We owe crime victims an update. Accordingly, I am submitting for your consideration “An Act Modernizing the Massachusetts Wiretap Law.”

One of the most restrictive aspects of the current law is that any wiretap—or even any secret recording of a face to face meeting—must be part of an investigation of organized crime. The courts have defined “organized crime” in this context as “a continuing enterprise to supply illegal goods and services.” While organized crime in this narrow sense was and remains a significant concern for law enforcement, there are other crimes that can cause every bit as much harm to victims and to society as a whole.

Police should be able to use the same tools to solve a murder committed because of racial hatred or gang affiliation that they use to solve a murder committed in connection with organized crime. Therefore, this bill expands the authority of law enforcement to use wiretaps and secret recordings to investigate certain serious offenses that have no connection to organized crime, such as murder, rape and possession of explosive devices. The bill also updates the list of offenses for which law enforcement may use these tools when the investigation is in connection with organized crime. Some less serious offenses are eliminated; other more serious offenses that did not exist in 1968—such as human trafficking and trafficking in firearms—are added.

The bill also includes a number of provisions to bring the law into the 21st century. They are:

- Updating definitions to reference electronic communications not in use in 1968
- Explicitly covering communications between out-of-state parties regarding an in-state crime
- Explicitly authorizing Massachusetts courts to issue orders to out of state companies to implement court-ordered monitoring
- Explicitly authorizing law enforcement to use contractors, such as translators, to monitor communications
- Requiring that law enforcement obtain an ordinary warrant for interception of information that is not the content of communications rather than a special wiretap warrant
- Extending the amount of time that a court may authorize interception before requiring a renewal of a warrant so that, in appropriate cases, law enforcement need not seek renewals as frequently
- Exempting use of police body-cameras and police cruiser-cameras by readily-identifiable law enforcement personnel from the statute, so that state law does not stand in the way of police departments that wish to equip their officers with these devices

Members of all three branches of government have recognized the limitations that the 1968 statute places on law enforcement in the Commonwealth. Easing these restrictions for particularly serious crimes and modernizing the statute to take into account new technology is vital to ensuring that our law enforcement agencies have the tools they need to keep us safe and hold criminals accountable. I urge your prompt enactment of this legislation.

Respectfully submitted,

Charles D. Baker,
Governor

HOUSE No. 3671

Message from His Excellency the Governor recommending legislation relative to modernizing the Massachusetts wiretap law.

The Commonwealth of Massachusetts

In the One Hundred and Ninetieth General Court
(2017-2018)

An Act modernizing the Massachusetts wiretap law.

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. Paragraph A of section 99 of chapter 272 of the General Laws, as appearing
2 in the 2014 Official Edition, is hereby amended by striking out the third subparagraph and
3 inserting in place thereof the following 2 subparagraphs:-

4 The general court further finds that in certain circumstances normal investigative
5 procedures may not be effective in the investigation of specific illegal acts not associated with
6 organized crime as enumerated in clause (b) of subparagraph 7 of paragraph B of this section.
7 Therefore, law enforcement officials may be permitted to use modern methods of electronic
8 surveillance, under strict judicial supervision, when investigating these specific enumerated
9 crimes.

10 The general court further finds that the uncontrolled development and unrestricted use of
11 modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the
12 commonwealth. Therefore, the secret use of such devices by private individuals must be
13 prohibited. The use of such devices by law enforcement officials must be conducted under strict

14 judicial supervision and must be limited to the investigation of designated offenses as defined in
15 subparagraph 7 of paragraph B of this section. Because the commonwealth has a substantial
16 interest in the investigation and prosecution of designated offenses committed within its borders,
17 this section shall authorize, under appropriate judicial supervision, the interception of electronic
18 communications between parties located outside the commonwealth, so long as the designated
19 offense under investigation is one over which the commonwealth has jurisdiction, and the
20 listening post is within the commonwealth.

21 SECTION 2. Paragraph B of said section 99 of said chapter 272, as so appearing, is
22 hereby amended by striking out the first subparagraph and inserting in place thereof the
23 following subparagraph:-

24 1. The term “wire communication” means any transfer made in whole or in part
25 through the use of facilities which allow for the transmission of communications by the aid of
26 wire, cable, wireless, electronic, digital, radio, electromagnetic, satellite, cellular, optical or other
27 technological means in order to achieve a connection between the point of origin and the point of
28 reception, regardless of whether or not such communication travels in part within a switching
29 station or other facility. The term “wire communication” shall also include: any transfer of
30 signs, signals, writing, images, photographs, videos, texts, sounds, data or intelligence of any
31 nature transmitted in whole or in part by using a cellular telephone, smartphone , personal data
32 assistant or similar device, but shall not include: (i) any communication made through a tone-
33 only paging device; (ii) any communication from a tracking device, defined as an electronic or
34 mechanical device which permits the tracking of the movement of a person or object; or (iii)
35 electronic funds transfer information stored by a financial institution in a communications system
36 used for the electronic storage and transfer of funds .

37 SECTION 3. Said paragraph B of said section 99 of said chapter 272, as so appearing, is
38 hereby further amended by striking out the third, fourth and fifth subparagraphs and inserting in
39 place thereof the following 3 subparagraphs:-

40 3. The term "intercepting device" means any device or apparatus which is capable of
41 transmitting, receiving, amplifying, or recording a wire or oral communication other than a
42 hearing aid or similar device which is being used to correct subnormal hearing to normal; and
43 other than any telephone or telegraph instrument, equipment, facility, or a component thereof, (a)
44 furnished to the subscriber or user by a communications common carrier in the ordinary course
45 of business under its tariff and being used by the subscriber or user in the ordinary course of its
46 business; or (b) being used by a communications common carrier in the ordinary course of its
47 business. No body-mounted camera with an audio recording feature shall be considered an
48 intercepting device when such an instrument is worn openly by a uniformed investigative or law
49 enforcement officer or one conspicuously displaying his or her badge of authority or other visible
50 indicator of his or her status as an investigative or law enforcement officer. No vehicle-mounted
51 camera with an audio recording feature shall be considered an intercepting device when it is
52 mounted on a marked law enforcement vehicle, or when such an instrument is used to record a
53 motor vehicle stop or other encounter involving a uniformed law enforcement officer, or one
54 conspicuously displaying his or her badge of authority or other visible indicator of his or her
55 status as a law enforcement officer.

56 4. The term "interception" means to secretly hear, secretly record, or aid another to
57 secretly hear or secretly record the contents of any wire or oral communication through the use
58 of any intercepting device by any person other than a person given prior authority by all parties
59 to such communication; provided that it shall not constitute an interception (a) for an

60 investigative or law enforcement officer to obtain information in real time concerning the
61 existence of a communication and the identity of the parties to a communication, but not the
62 contents of the communication itself, where such action has been specifically authorized by the
63 order of a court of competent jurisdiction pursuant to the procedure prescribed by 18 U.S.C. §
64 3123; or (b) for an investigative or law enforcement officer, as defined in this section, to record
65 or transmit a wire or oral communication if the officer is a party to such communication or has
66 been given prior authorization to record or transmit the communication by such a party and if
67 recorded or transmitted in the course of an investigation of a designated offense as defined
68 herein.

69 5. The term "contents", when used with respect to any wire or oral communication, means
70 any information concerning the contents, substance, purport, or meaning of that communication,
71 including any spoken words, visual images or written material.

72 SECTION 4. Said paragraph B of said section 99 of said chapter 272, as so appearing, is
73 hereby further amended by striking out the seventh subparagraph and inserting in place thereof
74 the following subparagraph:-

75 7. The term "designated offense" shall include (a) the following offenses in connection
76 with organized crime as defined in the preamble:

77 ; the illegal use, possession, theft, transfer or trafficking of one or more firearms, rifles,
78 shotguns, sawed-off shotguns, machine guns, assault weapons, large capacity weapons, covert
79 weapons as defined by section 121 of chapter 140, or silencers; any arson; assault and battery
80 with a dangerous weapon; bribery; any felony burglary; money laundering in violation of chapter
81 267A; enterprise crime in violation of chapter 271A; extortion; forgery; gaming in violation of

82 sections 38, 39, 40, 41 and 43 of chapter 23K and sections 16A and 17 of chapter 271;
83 kidnapping; any felony larceny; lending of money or things of value in violation of the general
84 laws; perjury; any felony involving prostitution; robbery; subornation of perjury; any violation of
85 section 13B of chapter 268; any violation of sections 29A, 29B and 105 of chapter 272; any
86 violation of this section; being an accessory to any of the foregoing offenses; and conspiracy,
87 attempt or solicitation to commit any of the foregoing offenses; and (b) the following offenses,
88 whether or not in connection with organized crime, as referenced in paragraph 3 of the preamble:
89 any murder or manslaughter, except under section 13 ½ of chapter 265; rape as defined in
90 sections 22, 22A, 22B, 22C, 23, 23A, 23B, 24 and 24B of chapter 265; human trafficking in
91 violation of sections 50 through 53 of chapter 265; any violation of chapter 94C involving the
92 trafficking, manufacture, distribution of, or intent to distribute controlled substances; illegal
93 trafficking in weapons; the illegal use or possession of explosives or chemical, radiological or
94 biological weapons; civil rights violation causing bodily injury; intimidation of a witness or
95 potential witness, or a judge, juror, grand juror, prosecutor, defense attorney, probation officer or
96 parole officer; being an accessory to any of the foregoing offenses; and conspiracy, attempt or
97 solicitation to commit any of the foregoing offenses.

98 SECTION 5. Paragraph I of said section 99 of said chapter 272, as so appearing, is
99 hereby amended by striking out the second subparagraph and inserting in place thereof the
100 following subparagraph:-

101 2. The date of issuance, the date of effect, and termination date which in no event shall
102 exceed 40 days from the date of effect. The warrant shall permit interception of oral or wire
103 communications for a period not to exceed 30 days. If physical installation of a device is
104 necessary, the 40 day period shall begin upon the date of installation. If the effective period of

105 the warrant is to terminate upon the acquisition of particular evidence or information or oral or
106 wire communication, the warrant shall so provide; and

107 SECTION 6. Said paragraph I of said section 99 of said chapter 272, as so appearing, is
108 hereby further amended by striking out the sixth subparagraph and inserting in place thereof the
109 following 3 subparagraphs:-

110 6. The identity of the agency authorized to intercept the communications, and of the
111 person authorizing the application; and

112 7. A statement providing for service of the warrant pursuant to paragraph L except that if
113 there has been a finding of good cause shown requiring the postponement of such service, a
114 statement of such finding together with the basis therefor must be included and an alternative
115 direction for deferred service pursuant to paragraph L, subparagraph 2.

116 8. Every order and extension thereof shall contain a provision that the authorization to
117 intercept shall be executed as soon as practicable, shall be conducted in such a way as to
118 minimize the interception of communications not otherwise subject to interception under this
119 chapter, and must terminate upon attainment of the authorized objective, or in any event in 30
120 days.

121 SECTION 7. Paragraph J of said section 99 of said chapter 272, as so appearing, is
122 hereby amended by striking out the second subparagraph and inserting in place thereof the
123 following subparagraph:-

124 2. Upon such application, the judge may issue an order renewing the warrant and
125 extending the authorization for a period not exceeding 30 days from the entry thereof. Such an

126 order shall specify the grounds for the issuance thereof. The application and an attested copy of
127 the order shall be retained by the issuing judge to be transported to the chief justice in
128 accordance with the provisions of paragraph N of this section. In no event shall a renewal be
129 granted which shall terminate later than 2 years following the effective date of the warrant.

130 SECTION 8. Said section 99 of said chapter 272, as so appearing, is hereby further
131 amended by striking out paragraph K and inserting in place thereof the following paragraph:-

132 K. Warrants: manner and time of execution

133 1. A warrant may be executed pursuant to its terms anywhere in the commonwealth, or
134 any other place that facilitates a wire communication to which at least 1 party is within the
135 commonwealth; or which otherwise involves a communication regarding a criminal offense for
136 which criminal jurisdiction would exist in the commonwealth.

137 2. Such warrant may be executed by the authorized applicant personally or by any
138 investigative or law enforcement officer of the commonwealth designated by him for the
139 purpose, or by any designated individual operating under a contract with the Commonwealth or
140 its subdivisions, acting under the supervision of an investigative or law enforcement officer
141 authorized to execute the warrant.

142 3. The warrant may be executed according to its terms during the hours specified therein,
143 and for the period therein authorized, or a part thereof. The authorization shall terminate upon
144 the acquisition of the oral or wire communications, evidence or information described in the
145 warrant. Upon termination of the authorization in the warrant and any renewals thereof, the
146 interception must cease at once, and any device installed for the purpose of the interception must

147 be removed as soon thereafter as practicable. Entry upon private premises for the removal of
148 such device is deemed to be authorized by the warrant.

149 4. In the event the intercepted communication is in a code or foreign language, and an
150 expert in that foreign language or code is not reasonably available during the interception period,
151 minimization may be accomplished as soon as practicable after such interception.

152 5. Upon request of the applicant, the issuing judge may direct that a provider of wire or
153 electronic communications service, landlord, custodian, or other person shall furnish the
154 applicant forthwith all information, facilities, and technical assistance necessary to accomplish
155 the interception unobtrusively and with a minimum of interference with the services that the
156 person so ordered by the court accords the party whose communications are to be intercepted.
157 Any provider of wire or electronic communications service, landlord, custodian or other person
158 furnishing such facilities or technical assistance shall be compensated therefore by the applicant
159 for reasonable expenses incurred in providing such facilities or assistance.