HOUSE DOCKET, NO. 4750 FILED ON: 1/21/2022

HOUSE . . . . . No. 4347

The Commonwealth of Massachusetts

OFFICE OF THE GOVERNOR
COMMONWEALTH OF MASSACHUSETTS
STATE HOUSE · BOSTON, MA 02133
(617) 725-4000

CHARLES D. BAKER
GOVERNOR

KARYN POLITO
LIEUTENANT GOVERNOR

January 21, 2022

To the Honorable Senate and House of Representatives,

Our state's wiretap statute was enacted in 1968 yet has not been substantively revised in the past half-century. That means that this crucial law enforcement tool neither incorporates the current state of technology nor recognizes that the commission and detection of crime have greatly changed over the past fifty years. Crime victims and law enforcement deserve an up-to date version of this statute, so I am again submitting for your consideration "An Act Modernizing the Massachusetts Wiretap Law."

As I observed when I submitted this legislation several years ago, the current law permits law enforcement to use a wiretap or secretly record conversations in only a narrow set of circumstances—when there is a link to "organized crime"—and only when that "organized crime" narrowly includes "a continuing enterprise to supply illegal goods and services." These limits unnecessarily and inappropriately restrict law enforcement from investigating other crimes that are just as damaging to victims and our Commonwealth and are among the most difficult to solve using traditional methods.

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. And, for investigations that are connected to organized crime, the bill updates the list of offenses for which law enforcement

may use these tools, eliminating some less serious offenses and adding some more serious offenses that were not established in statute in 1968, such as trafficking in human beings and firearms.

As criminals and criminal organizations grow more sophisticated, additional provisions of the bill ensure that the wiretap statute is in step with the modern world:

- Updating definitions to reference electronic communications not in use in 1968, including wireless, satellite, and cellular communications;

- 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; and

- Exempting use of police body-worn cameras and cruiser-mounted 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. This exemption is particularly important because the State Police has completed implementing its body-worn camera program for all sworn troopers, and because our administration has established a 5-year, $20 million capital grant program that aims to deploy 9,000 body-worn cameras to police officers in Massachusetts' cities and towns.

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 account for 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. 4347

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Second General Court
(2021-2022)

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:

SECTION 1. Paragraph A of section 99 of chapter 272 of the General Laws, as appearing in the 2020 Official Edition, is hereby amended by striking out the third subparagraph and inserting in place thereof the following 2 subparagraphs:-

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

The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and must be limited to the investigation of designated offenses as defined in

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

K. Warrants: manner and time of execution

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

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

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

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

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

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