The Commonwealth of Massachusetts

In the Year Two Thousand and 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:

SECTION 1. The General Laws, as appearing in the 2008 Official Edition, are hereby amended by adding after Chapter 267 the following new chapter: —

Chapter 267A Money Laundering.

Section 1. Definitions.

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

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

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

“Transaction”, a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, bailment, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, use of a safe deposit box, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected.

“Financial institution”, (a) any bank as defined in section one of chapter 167 ; (b) any national banking association, bank, savings and loan, savings bank, cooperative bank, building and loan, or credit union organized under the laws of the United States; (c) any banking association, bank, savings and loan, savings bank, cooperative bank, building and loan or credit union organized under the laws of any state; (d) any agency, agent, or branch of a foreign bank; (e) any currency dealer or exchange; (f) any person or business engaged primarily in the cashing of checks; (g) any person or business regularly engaged in the issuing, selling, or redeeming of traveler's checks, money orders or similar instruments; (h) any broker or dealer in securities or commodities; (i) any licensed

transmitter of funds or other person or business regularly engaged in the transmission of funds to a foreign nation for others; (j) any investment banker or investment company; (k) any insurer; (l) any dealer in precious metals, stones or jewels; (m) any pawnbroker or scrap metal dealer; (n) any telegraph or other communications company; (o) any personal property or real estate broker; (p) any dealer in vehicles, including, but not limited to, automobiles, aircraft and vessels; (q) any operator of a betting or gambling facility; (r) any travel agent; (s) any thrift institution; (t) any operator of a credit card system; or (u) any loan or finance company.

“Monetary instrument”, the currency and coin of the United States or any foreign country; any bank check, money order, stock, investment security, or negotiable instrument in bearer form or otherwise in such form that title passes upon delivery; gold, silver or platinum bullion or coins; diamonds, emeralds, rubies, or sapphires; any negotiable instrument including: bank checks, cashier's checks, traveler's checks, or monetary orders made payable to the order of a named party that have not been endorsed or which bear restrictive endorsements; poker chips, vouchers or other tokens exchangeable for cash by gaming entities; and credit cards, debit cards, gift cards, gift certificates, calling cards, or scrips.

Section 2. Money Laundering.

Whoever knowingly:

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

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

(c) directs, organizes, finances, plans, manages, supervises, or controls the transportation of or transactions in monetary instruments or other property known to be derived from criminal activity or which a reasonable person would believe to be derived from criminal activity;

is guilty of the crime of money laundering and shall be punished by imprisonment in the state prison for not more than 6 years or by a fine of not more than $250,000 or twice the value of the property transacted, whichever is greater, or by both such imprisonment and fine; and for any subsequent offense shall be punished by imprisonment in the state prison for not less than 2 years, but not more than 8 years or by a fine of not more than $500,000 or three times the value of the property transacted, whichever is greater, or by both such imprisonment and fine.

Section 3. Record Keeping.

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

Section 4. Forfeiture.

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

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

Chapter 271A Enterprise Crime.

Section 1. Definitions.

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

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

“Pattern of criminal enterprise activity”, engaging in at least two incidents of criminal enterprise activity that have the same or similar pattern, intents, results, accomplices, victims or methods of commission, or are otherwise interrelated by distinguishing characteristics and are not isolated incidents, provided at least one of the acts occurred

after the effective date of this act, and the last of the incidents occurred within five years after a prior commission of criminal enterprise activity.

“Criminal enterprise activity”, to commit, to attempt to commit, to conspire to commit, or to solicit, coerce, aid, abet, or intimidate another to commit any of the following criminal activity under the laws of the commonwealth or equivalent crimes under the laws of any other jurisdiction:

murder; rape; manslaughter; assault; assault and battery; mayhem; robbery; extortion; stalking; criminal harassment; kidnapping; arson; burglary; malicious destruction of property; commission of a felony for hire; breaking and entering; child exploitation; poison; human trafficking; violation of constitutional rights; usury; uttering; misuse or fraudulent use of credit cards; identity fraud; misappropriation of funds; gross fraud; insurance fraud; prize fighting; boxing matches; counterfeiting; perjury; subornation of perjury; obstruction of justice; money laundering; witness intimidation; bribery; electronic eavesdropping; prostitution; receiving stolen property; larceny over $250.00; larceny by false pretenses/embezzlement; forgery; prohibited financial interest; procurement fraud; false claims; tax evasion; filing false tax return; crimes involving violations of: gambling and lottery laws; gift laws; liquor laws; tobacco laws; firearms laws; securities laws; lobbying laws; ethics laws; conflict of interest laws; child and elder abuse laws; or any conduct defined as a racketeering activity under Title 18, U.S.C. s. 1961(1)(A)(B) and (D).

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

Section 2. Enterprise Crime.

Whoever knowingly:

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

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

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

(d) conspires or attempts to violate subsections (a), (b), or (c) of this section;

is guilty of enterprise crime and shall be punished by imprisonment in the state prison for not less than 3 years and not more than 15 years or by a fine of not more than $25,000, or by both such imprisonment and fine.

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

Section 3. Forfeiture.

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

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

Section 99. Wiretap and Electronic Surveillance

Section 1. Preamble

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

Section 2. Definitions.

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

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

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

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

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

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

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

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

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

(1) any wire or oral communication;

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

(3) 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

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

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

“Electronic communications system” means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

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

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

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

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

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

"Electronic storage" means:

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

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

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

"Intercept" means the secret acquisition of aural or other secret acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire, electronic 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 any offense described in section 7, and a judicial official authorized to issue warrants pursuant to chapter 276 determines that there is probable cause that evidence of such a crime will be recorded or transmitted. Any such warrant shall be valid for no greater than 15 days from the date of issue.

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

"Judge of competent jurisdiction" means any judge of the superior court of the commonwealth.

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

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

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

"Readily accessible to the general public" means, with respect to a radio communication, that such communication is not:

(1) scrambled or encrypted;

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

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

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

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

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

“User” means any person or entity who:

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

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

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

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

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

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

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

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

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

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

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

(5) edit, alter or tamper with any tape, transcription or recording of wire, oral, or electronic communications by any means, or attempt to edit, alter or tamper with any tape, transcription or recording of wire, oral, or electronic communications by any means with the intent to present in any judicial proceeding or proceeding under oath, or present such recording or permit such recording to be presented in any judicial proceeding or

proceeding under oath, without fully indicating the nature of the changes made in the original state of the recording.

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

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

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

(1) an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of that person's employment while engaged in any activity which is a necessary incident to the rendition of that person's service or to the protection of the rights or property of the provider of that service, or which is necessary to prevent the use of such facilities in violation of section fourteen A of chapter two hundred and sixty-nine of the general laws; except that a provider of wire or electronic communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks;

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

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

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

(B) No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this section, except as may otherwise be required by legal process and

then only after prior notification to the attorney for the state as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 17.

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

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

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

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

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

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

(D) by any marine or aeronautical communications system;

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

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

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

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

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

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

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

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

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

(12) investigative or law enforcement officers to violate the provisions of this section for the purposes of ensuring the safety of any law enforcement officer or agent thereof who is acting in an undercover capacity, or as a witness for the commonwealth; provided, however, that any such interception which is not otherwise permitted by this section shall be deemed unlawful for purposes of section 9(o);

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

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

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

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

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

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

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

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

(16) for an employee of:

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

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

(e) (1) Except as provided in paragraph (2) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication, other than one to such person or entity, or an agent thereof, while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(b) Any person who has received, by any means authorized by this section, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom, intercepted in accordance with the provisions of this section may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding in any court of the United States or of any state or in any federal or state grand jury proceeding.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(c) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application. A verbatim transcript of every such interrogation

or examination must be taken, and a transcription of the same, sworn to by the stenographer, shall be attached to the application and be deemed a part thereof.

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

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

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

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

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

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

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

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

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

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

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

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

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

(f) An order authorizing the interception of a wire, oral, or electronic communication under this section shall, upon request of the applicant, direct that a provider of wire or

electronic communication 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 such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance.

(g) An order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for the shorter of 30 days or the period necessary to achieve the objective of the authorization. Such 30 day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered, whichever occurs earliest. Extensions of an order may be granted only upon application for an extension made in accordance with subsection (b) of this section and the court making the findings required by subsection (d) of this section. The period of extension shall be the shorter of 30 days or the time the authorizing judge deems necessary to achieve the purposes for which it was granted. 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 section, and must terminate upon the earlier of 30 days or the attainment of the authorized objective. In the event the intercepted communication is in a code or a 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 of the communication in full.

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

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

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

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

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

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

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

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

The recordings shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Notice prior to the destruction shall be given to the applicant attorney general or his successor or the applicant district attorney or his successor and upon a showing of good cause to the chief justice, the application, warrant, renewal and return may be kept for such additional period as the chief justice shall determine but in no event longer than the longest period of limitation for any designated offense specified in the warrant, after which time they must be destroyed by a person designated by the chief justice. Duplicate recordings may be made for use or disclosure pursuant to the provisions of section 8(a) or (b) of this section

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

(3) Except as otherwise provided in subparagraph (a), within a reasonable time, not to exceed 90 days, after the filing of an application for an order of approval under subsection (l) which is denied, or the termination of the period of an order or extensions thereof, an investigative or law enforcement officer of the commonwealth shall serve an attested copy of the warrant or the renewal on the persons named in the warrant, and such other aggrieved persons who shall reasonably be known to the person who obtained the warrant as a result of information obtained from an authorized interception. The attested

copy of the warrant shall be served by leaving the same at his usual place of abode, or in hand, or if this is not possible by mailing the same by certified or registered mail to his last known place of abode. A return of service shall be made to the issuing judge, except, that if such service is postponed as provided in this subparagraph, it shall be made to the chief justice. The return of service shall be deemed a part of the return of the warrant and attached thereto.

(a) Upon an ex parte showing of important special facts which set forth the need for continued secrecy to the satisfaction of the issuing judge, said judge may direct that the attested copy of the warrant be served on such parties as are required by this subsection at such time as may be appropriate in the circumstances but in no event may he it to be served later than three years from the time of expiration of the warrant or the last renewal thereof.

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

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

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

(1) the communication was unlawfully intercepted;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 10. Warrant Return

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

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

(b) The periods of time during which such interceptions were made; and

(c) The names of the parties to the communications intercepted if known; and

(d) The original recording of the oral, wire or electronic communications intercepted, if any; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) In general:

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

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

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

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

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

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

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

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

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

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

(b) An order issued under this section:

(1) shall specify:

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

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

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

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

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

(c) An order issued under this section:

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

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

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

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

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

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

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

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

(b) Upon the request of the attorney for the state or an investigative or law enforcement officer authorized to receive the results of a trap and trace device under this section, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line or facility and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the

court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 13(b)(2) of this section. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 13(b) or section 12 of the act, to the attorney for the state or the investigative or law enforcement officer, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(B) the name of the applicant;

(C) the number of wiretap warrants issued;

(D) the effective period of the wiretap warrants;

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

(i) the number of renewals,

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

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

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

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

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

Section 17. Authorized Recovery of Civil Damages.

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

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

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

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

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

(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

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

(3) $1,000.

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

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

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

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

(e) A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation

Section 18. Severability.

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