HOUSE BILL No. 4931

August 28, 2013, Introduced by Rep. Heise and referred to the Committee on Criminal Justice.

A bill to authorize certain interceptions of communications and the use of interception devices for certain offenses; to provide for and regulate the application, issuance, and execution of interception orders; to prescribe the powers and duties of certain agencies, officers, and employees; to regulate the use and disclosure of communications and evidence intercepted or obtained under this act; to provide remedies and exemptions from liability; and to prescribe penalties.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

- Sec. 1. This act shall be known and may be cited as the "criminal communications intercept act".
 - Sec. 1a. As used in this act:
 - (a) "Aggrieved person" means a person who was a party to an

- 1 intercepted wire, oral, or electronic communication or a person
- 2 against whom the interception was directed.
- 3 (b) "Aural transfer" means a transfer containing the human
- 4 voice at any point between the point of origin and the point of
- 5 reception, including those points.
- 6 (c) "Communication common carrier" means a person engaged as a
- 7 common carrier for hire in communication by wire or radio or in
- 8 radio transmission of energy. A person engaged in radio
- 9 broadcasting is not a communication common carrier while so
- 10 engaged.
- 11 (d) "Computer trespasser" means a person who accesses a
- 12 computer without authorization and thus has no reasonable
- 13 expectation of privacy in any communication transmitted to,
- 14 through, or from the computer.
- 15 (e) "Contents" means any information concerning the substance,
- 16 purport, or meaning of a wire, oral, or electronic communication.
- 17 (f) "Electronic communication" means a transfer of signs,
- 18 signals, writing, images, sounds, data, or intelligence of any
- 19 nature transmitted in whole or in part by a wire, radio,
- 20 electromagnetic, photoelectronic, or photooptical system.
- 21 Electronic communication does not include any of the following:
- 22 (i) A wire or oral communication.
- 23 (ii) A communication made through a tone-only paging device.
- 24 (iii) A communication from an electronic or mechanical device
- 25 that permits the tracking of an individual's or object's movement.
- 26 (iv) Electronic transfer information stored by a financial
- 27 institution in a communication system used for electronic storage

- 1 and transfer of funds.
- 2 (v) Stored electronic or stored wire communication governed by
- **3** 18 USC 2703.
- 4 (g) "Electronic communication service" means a service that
- 5 provides to the service's users the ability to send or receive wire
- 6 or electronic communications.
- 7 (h) "Electronic communications system" means wire, radio,
- 8 electromagnetic, photooptical, or photoelectronic facilities for
- 9 transmitting wire or electronic communications and computer
- 10 facilities or related electronic equipment for the electronic
- 11 storage of wire or electronic communications.
- 12 (i) "Electronic storage" means either of the following:
- 13 (i) Temporary, intermediate storage of a wire or electronic
- 14 communication incidental to its electronic transmission.
- 15 (ii) Storage of a wire or electronic communication by an
- 16 electronic communication service for backup protection of the
- 17 communication.
- 18 (j) "Interception device" means a device, computer software,
- 19 or apparatus that can be used to intercept a wire, oral, or
- 20 electronic communication. Interception device does not include any
- 21 of the following:
- 22 (i) A telephone or telegraph instrument, equipment, or facility
- 23 or any component of that instrument, equipment, or facility that is
- 24 1 or more of the following:
- 25 (A) Furnished to the user by an electronic communication
- 26 service provider in the ordinary course of its business and being
- 27 used in the ordinary course of the user's business.

- 1 (B) Furnished by the user for connection to the facilities of
- 2 an electronic communication service provider and being used in the
- 3 ordinary course of the user's business.
- 4 (C) Being used by an electronic communication service provider
- 5 in the ordinary course of its business.
- **6** (D) Being used by an investigative or law enforcement officer
- 7 in the ordinary course of the officer's duties.
- 8 (ii) A hearing aid or similar device used to correct subnormal
- 9 hearing to not better than normal.
- 10 (k) "Intercept" or "interception" means the aural or other
- 11 acquisition of the contents of a wire, oral, or electronic
- 12 communication through the use of an interception device.
- 13 (l) "Investigative or law enforcement officer" means an officer
- 14 of this state or a political subdivision who is empowered by law to
- 15 conduct investigations of or to make arrests for offenses described
- 16 in section 7 and who is certified under section 11.
- 17 Sec. 2. As used in this act:
- 18 (a) "Judge of competent jurisdiction" means a judge appointed
- 19 under section 2a.
- 20 (b) "Oral communication" means a communication uttered by a
- 21 person with a reasonable expectation that the communication is not
- 22 subject to interception. Oral communication does not include an
- 23 electronic communication.
- (c) "Pen register" means a device that records or decodes
- 25 electronic or other impulses which identify the numbers dialed or
- 26 otherwise transmitted on the telephone line to which the device is
- 27 attached, but does not include any device used by a provider or

- 1 customer of a wire or electronic communication service for billing,
- 2 or recording as an incident to billing, for communications services
- 3 provided by that provider or any device used by a provider or
- 4 customer of a wire communication service for cost accounting or
- 5 other substantially similar purposes in the ordinary course of its
- 6 business.
- 7 (d) "Person" means an employee or agent of this state or a
- 8 political subdivision or an individual, partnership, association,
- 9 limited liability company, corporation, or other legal entity.
- 10 (e) "Political subdivision" means a county, city, township, or
- 11 village of this state.
- 12 (f) "Prosecutor" means the attorney general of this state or 1
- 13 assistant attorney general he or she designates or the principal
- 14 prosecuting attorney of the county in which the facility or place
- 15 where the communication to be intercepted is located or 1 assistant
- 16 prosecuting attorney of that county he or she designates.
- 17 (g) "Readily accessible to the general public" means the
- 18 communication is not any of the following:
- 19 (i) Scrambled or encrypted.
- 20 (ii) Transmitted using modulation techniques whose essential
- 21 parameters have been withheld from the public to preserve the
- 22 communication's privacy.
- 23 (iii) Carried on a subcarrier or other signal subsidiary to a
- 24 radio transmission.
- 25 (iv) Transmitted over a communication system provided by a
- 26 communication common carrier, unless the communication is a tone-
- 27 only paging system communication.

- 1 (v) Transmitted on a frequency allocated under 47 CFR part 25
- 2 or subpart D, E, or F of 47 CFR part 74 unless, in the case of a
- 3 communication transmitted on a frequency allocated under 47 CFR
- 4 part 74 that is not exclusively allocated to broadcast auxiliary
- 5 services, the communication is a 2-way voice communication by
- 6 radio.
- 7 (h) "Trap and trace device" means a device that captures the
- 8 incoming electronic or other impulses that identify the originating
- 9 number of an instrument or device from which a wire or electronic
- 10 communication was transmitted.
- 11 (i) "User" means a person who subscribes to or uses an
- 12 electronic communication service and is authorized to engage in
- 13 that use.
- 14 (j) "Wire communication" means an aural transfer made in whole
- 15 or in part through the use of facilities for transmitting
- 16 communications by wire, cable, or other substantially similar
- 17 connection between the point of origin and the point of reception
- 18 that are furnished or operated by a person engaged in providing or
- 19 operating those facilities for the transmission of communications
- 20 and includes the use of such a connection in a switching station.
- 21 Wire communication does not include storage of that communication,
- 22 electronic or otherwise. Wire communication does not include
- 23 electronic communication.
- 24 Sec. 2a. The supreme court shall appoint not less than 5
- 25 circuit court judges in each of the judicial districts designated
- 26 for the election of judges of the court of appeals as judges of
- 27 competent jurisdiction under this act.

- 1 Sec. 3. (1) Except as otherwise provided in this act or as
- 2 authorized or approved under 18 USC 2510 to 2522, a person shall
- 3 not intentionally do any of the following:
- 4 (a) Intercept, attempt to intercept, or solicit another person
- 5 to intercept or attempt to intercept a wire, oral, or electronic
- 6 communication.
- 7 (b) Disclose or attempt to disclose to another person the
- 8 contents of a wire, oral, or electronic communication knowing or
- 9 having reason to know that the information was obtained through the
- 10 interception of a wire, oral, or electronic communication in
- 11 violation of this act.
- 12 (c) Use or attempt to use the contents of a wire, oral, or
- 13 electronic communication knowing or having reason to know the
- 14 information was obtained through the interception of a wire, oral,
- 15 or electronic communication in violation of this act.
- 16 (2) Except as provided in subsection (3), a person who
- 17 violates subsection (1) is quilty of a felony punishable by
- 18 imprisonment for not more than 4 years or a fine of not more than
- **19** \$5,000.00, or both.
- 20 (3) If both of the following apply, conduct prohibited by
- 21 subsection (1) is not punishable under subsection (2) unless it is
- 22 for direct or indirect commercial advantage or private financial
- 23 qain:
- 24 (a) The conduct consists of or relates to the interception of
- 25 a satellite transmission that is not encrypted or scrambled.
- 26 (b) Either of the following applies:
- 27 (i) The satellite transmission is transmitted to a broadcasting

- 1 station for retransmission to the general public.
- 2 (ii) The satellite transmission is transmitted as an audio
- 3 subcarrier intended for redistribution to facilities open to the
- 4 public but is not a data transmission or telephone call.
- 5 (4) A person who trespasses on property owned or under the
- 6 control of another person with the intent to intercept or
- 7 facilitate intercepting a wire, oral, or electronic communication
- 8 is guilty of a misdemeanor punishable by imprisonment for not more
- 9 than 90 days or a fine of not more than \$100.00, or both.
- 10 (5) This act does not prohibit any of the following:
- 11 (a) Interception, disclosure, or use of a wire or electronic
- 12 communication by a switchboard operator or an officer, employee, or
- 13 agent of an electronic communication service provider in the normal
- 14 course of his or her duties or employment while engaged in an
- 15 activity necessarily incident to rendering service or protecting
- 16 the provider's rights or property, unless the interception results
- 17 from the provider's use of service observing or random monitoring
- 18 for purposes other than mechanical or service quality control
- 19 checks, or the interception is in adherence to federal or state
- 20 laws pertaining to the monitoring and reporting of illegal
- 21 terrorist activity under federal law.
- 22 (b) Interception of a wire or electronic communication, or an
- 23 oral communication transmitted by radio, or disclosure or use of
- 24 the information obtained through the interception by an officer,
- 25 employee, or agent of the federal communications commission in the
- 26 normal course of his or her employment and the commission's
- 27 monitoring responsibilities to enforce the communications act of

- 1 1934, 47 USC 151 to 621.
- 2 (c) A person intercepting a wire, oral, or electronic
- 3 communication while acting under color of law if the person is a
- 4 party to the communication or 1 of the parties to the communication
- 5 gives prior consent to the interception.
- 6 (d) A person intercepting a wire, oral, or electronic
- 7 communication while not acting under color of law if the person is
- 8 a party to the communication or 1 of the parties to the
- 9 communication gives prior consent to the interception, unless the
- 10 communication is intercepted to commit a criminal or tortious act
- 11 in violation of the constitution or laws of the United States or
- 12 this state.
- 13 (e) Electronic surveillance as defined in 50 USC 1801,
- 14 conducted by an officer, employee, or agent of the United States in
- 15 the normal course of his or her official duty to conduct that
- 16 surveillance.
- 17 (f) Intercepting or accessing an electronic communication made
- 18 through an electronic communication system that is configured so
- 19 the electronic communication is readily accessible to the general
- 20 public.
- 21 (g) Intercepting a radio communication transmitted by any of
- 22 the following:
- 23 (i) A station if the communication is for the general public's
- 24 use or relates to a ship, aircraft, vehicle, or person in distress.
- 25 (ii) A governmental, law enforcement, civil defense, private
- 26 land mobile, fire, or public safety communications system that is
- 27 readily accessible to the general public.

- 1 (iii) A station operating on an authorized frequency within the
- 2 bands allocated to amateurs, citizens band, or general mobile radio
- 3 services.
- 4 (iv) A marine or aeronautical communications system.
- (h) Engaging in conduct that is prohibited under 48 USC 553 or
- 6 605.
- 7 (i) Intercepting a wire or electronic communication whose
- 8 transmission is causing harmful interference to a lawfully
- 9 operating station or consumer electronic equipment to the extent
- 10 necessary to identify the source of the interference.
- 11 (j) Interception by other users of the same frequency of a
- 12 radio communication made through a system that utilizes frequencies
- 13 monitored by individuals engaged in providing or using the system
- 14 if the communication is not scrambled or encrypted.
- 15 (k) Using a pen register.
- 16 (l) Using a trap and trace device.
- 17 (m) An electronic communication service provider recording the
- 18 fact that a wire or electronic communication was initiated or
- 19 completed to protect the provider, another provider furnishing
- 20 service in connection with the wire or electronic communication, or
- 21 a user from fraudulent, unlawful, or abusive use of the service.
- (n) It is not unlawful under this act for a person acting
- 23 under the color of law to intercept the wire or electronic
- 24 communications of a computer trespasser if all of the following
- 25 circumstances exist:
- 26 (i) The owner or operator of the computer authorizes the
- 27 interception of the computer trespasser's communications on the

- 1 computer.
- 2 (ii) The person acting under color of law is lawfully engaged
- 3 in an investigation.
- 4 (iii) The person acting under color of law has reasonable
- 5 grounds to believe that the content of the computer trespasser's
- 6 communications will be relevant to the investigation.
- 7 (iv) The interception does not acquire communications other
- 8 than those transmitted to or from the computer trespasser.
- 9 (6) A person may provide information, facilities, or technical
- 10 assistance to a person authorized by law to intercept a wire, oral,
- 11 or electronic communication if that person was provided with a
- 12 court order described in section 8 directing that assistance. The
- 13 person assisting shall not disclose the existence of any
- 14 interception, surveillance, or interception device relating to the
- 15 order described in this subsection except as otherwise required by
- 16 lawful process and then only after notifying the prosecutor who
- 17 obtained the order before disclosure.
- 18 (7) Except as otherwise provided in subsections (8) and (9), a
- 19 person providing an electronic communication service to the public
- 20 shall not intentionally disclose the contents of a communication
- 21 while it is being transmitted on that service to a person other
- 22 than the addressee or intended recipient of the communication or an
- 23 agent of the addressee or intended recipient.
- 24 (8) Subsection (7) does not apply if the service provider or
- 25 the provider's agent is the addressee or intended recipient of the
- 26 communication.
- 27 (9) A service provider described in subsection (7) may

- 1 disclose the contents of a communication as follows:
- 2 (a) If the communication was intercepted as described in
- 3 subsection (5).
- 4 (b) As authorized under this act.
- 5 (c) With the lawful consent of the originator, an addressee,
- 6 or an intended recipient of the communication.
- 7 (d) To a person employed or authorized, or whose facilities
- 8 are used, to forward the communication to its destination.
- 9 (e) To a law enforcement agency, if the service provider
- 10 obtains the contents inadvertently and believes they pertain to the
- 11 commission of a crime.
- Sec. 4. (1) Except as provided in subsection (2) or (3) or as
- 13 authorized or approved under 18 USC 2510 to 2522, a person shall
- 14 not do any of the following:
- 15 (a) Manufacture, assemble, possess, or sell or otherwise
- 16 deliver an interception device knowing or having reason to know the
- 17 device's design renders it primarily useful for surreptitiously
- 18 intercepting wire, oral, or electronic communications.
- 19 (b) Advertise or offer to sell or otherwise deliver an
- 20 interception device knowing or having reason to know the device's
- 21 design renders it primarily useful for surreptitiously intercepting
- 22 wire, oral, or electronic communications.
- 23 (c) Advertise or offer to sell or otherwise deliver any device
- 24 by promoting the use of the device to surreptitiously intercept
- 25 wire, oral, or electronic communications.
- 26 (2) In the normal course of its business, an electronic
- 27 communication service provider or an officer, agent, or employee of

- 1 or a person under contract with that service provider may
- 2 manufacture, assemble, possess, or sell an interception device
- 3 knowing or having reason to know the device's design renders it
- 4 primarily useful for surreptitiously intercepting wire, oral, or
- 5 electronic communications.
- 6 (3) Under a warrant or order issued by a court of competent
- 7 jurisdiction or a comparable court of the United States, an
- 8 officer, agent, or employee of the United States, this state, or a
- 9 political subdivision may manufacture, assemble, possess, or sell
- 10 an interception device knowing or having reason to know the
- 11 device's design renders it primarily useful for surreptitiously
- 12 intercepting wire, oral, or electronic communications.
- 13 (4) A person who violates subsection (1) is quilty of a felony
- 14 punishable by imprisonment for not more than 4 years or a fine of
- 15 not more than \$5,000.00, or both.
- 16 Sec. 5. If a wire, oral, or electronic communication is
- 17 intercepted, its contents and any evidence derived from the
- 18 communication shall not be received in evidence in a trial,
- 19 hearing, or other proceeding before a court, grand jury, tribunal,
- 20 department or regulatory agency, legislative committee, or other
- 21 authority of this state or a political subdivision if disclosure of
- 22 the communication or evidence would violate this act unless
- 23 otherwise authorized by federal law or the law of this state.
- 24 Sec. 6. (1) An investigative or law enforcement officer who
- 25 knows the contents of a wire, oral, or electronic communication or
- 26 evidence derived from the communication may do any of the following
- 27 if he or she obtained that knowledge by a means authorized under

- 1 this act:
- 2 (a) Disclose the contents or evidence to another investigative
- 3 or law enforcement officer or to an officer, agent, or official of
- 4 a law enforcement agency of the United States government to the
- 5 extent appropriate for proper performance of the official duties of
- 6 the person making or receiving the disclosure.
- 7 (b) Use those contents or the evidence to the extent
- 8 appropriate for proper performance of his or her official duties.
- 9 (2) A person who receives information concerning a wire, oral,
- 10 or electronic communication intercepted in accordance with this act
- 11 or evidence derived from the communication may disclose the
- 12 contents or evidence while giving testimony under oath or
- 13 affirmation in a proceeding held under the authority of the United
- 14 States, this state, or a political subdivision or in a civil
- 15 proceeding under section 13 if the person received the information
- 16 by a means authorized under this act.
- 17 (3) A privileged wire, oral, or electronic communication
- 18 intercepted in accordance with or in violation of this act does not
- 19 lose its privileged character by that interception.
- 20 (4) Except as otherwise provided in this subsection, if an
- 21 investigative or law enforcement officer intercepting wire, oral,
- 22 or electronic communications in the manner authorized by this act
- 23 intercepts a wire, oral, or electronic communication relating to an
- 24 offense other than an offense specified in the order under section
- 25 7, the communication's contents and evidence derived from the
- 26 communication may be disclosed or used as provided in subsection
- 27 (1) or (2). The communication's contents and any evidence derived

- 1 from the communication may be used under subsection (3) if
- 2 authorized or approved by a judge of competent jurisdiction on
- 3 subsequent application after determining that the contents were
- 4 otherwise intercepted in accordance with this act. The subsequent
- 5 application shall be made as soon as practicable after intercepting
- 6 the communication. This subsection does not authorize the
- 7 disclosure or use in any manner of the contents of or evidence
- 8 derived from a wire, oral, or electronic communication relating to
- 9 an offense punishable by imprisonment for 4 years or less or
- 10 punishable only by a fine.
- 11 (5) A person who violates this section is guilty of a felony
- 12 punishable by imprisonment for not more than 4 years or a fine of
- 13 not more than \$5,000.00, or both.
- 14 Sec. 7. (1) A prosecutor may authorize an application to a
- 15 judge of competent jurisdiction for an order authorizing or
- 16 approving the interception of wire, oral, or electronic
- 17 communications by the investigative or law enforcement officer
- 18 responsible for the investigation of the offense for which the
- 19 application is made if the interception may provide or has provided
- 20 evidence of any of the following offenses:
- 21 (a) Gang-related activity in violation of section 411u or 411v
- 22 of the Michigan penal code, 1931 PA 328, MCL 750.411u and 750.411v.
- 23 (b) Human trafficking in violation of chapter LXVIIA of the
- 24 Michigan penal code, 1931 PA 328, MCL 750.462a to 750.462j.
- 25 (c) Attempting or conspiring to commit an offense described in
- 26 subdivision (a) or (b).
- 27 (2) The principal prosecuting attorney for a county or his or

- 1 her designated assistant prosecuting attorney shall not authorize
- 2 an application for a violation unless the attorney general or his
- 3 or her designated assistant attorney general approves the
- 4 authorization. The attorney general or his or her designated
- 5 assistant attorney general shall approve or deny the authorization
- 6 within 7 days after the request for authorization is made.
- 7 (3) Unless the investigative or law enforcement officer
- 8 described in subsection (1) is employed by the department of state
- 9 police, the prosecutor authorizing the application shall notify the
- 10 director of the department of state police, or a person the
- 11 director designates, of the application and the information
- 12 described in section 8(1)(b)(ii) and (iv). If the proposed
- interception will overlap, conflict with, hamper, or interfere with
- 14 another interception proposed or authorized, the director or his or
- 15 her designee shall advise the judge of competent jurisdiction for
- 16 each application and shall coordinate any subsequent interceptions.
- 17 Sec. 8. (1) An application for an order authorizing or
- 18 approving the interception of a wire, oral, or electronic
- 19 communication shall be in writing upon oath or affirmation to a
- 20 judge of competent jurisdiction and shall state the applicant's
- 21 authority to apply. An application shall include all of the
- 22 following information:
- 23 (a) The identity of the investigative or law enforcement
- 24 officer applying and the prosecutor authorizing the application.
- 25 (b) A comprehensive statement of the facts and circumstances
- 26 the applicant relies upon to justify his or her belief that an
- 27 order should be issued, including all of the following:

- 1 (i) Details of the particular offense that has been, is being,
- 2 or is about to be committed.
- 3 (ii) Except as provided in section 9, a particular description
- 4 of the nature and location of the facilities from which, or the
- 5 place where, the communication is to be intercepted.
- 6 (iii) A particular description of the type of communication
- 7 sought to be intercepted.
- 8 (iv) If known, the identity of any person committing or about
- 9 to commit the offense and whose communication is to be intercepted.
- 10 (v) A statement of the facts indicating the specific instances
- 11 of conduct demonstrating probable cause to believe the particular
- 12 offense has been, is being, or is about to be committed.
- 13 (c) Comprehensive statements of each of the following:
- 14 (i) Whether other investigative procedures have been tried and
- 15 have failed or reasonably appear to be unlikely to succeed if tried
- or to be dangerous.
- 17 (ii) The time period for which the interception must be
- 18 maintained. If the investigation's nature is such that the
- 19 authorization for interception should not automatically terminate
- 20 when the described type of communication has been obtained, the
- 21 statement shall include a particular description of the facts
- 22 establishing probable cause to believe additional communications of
- 23 the same type will occur after that time.
- 24 (iii) The legitimate investigative objective to be expected by
- 25 the interception.
- (iv) The facts concerning all previous applications known to
- 27 the individuals authorizing and making the application that were

- 1 made for authorization to intercept or for approval of an
- 2 interception of a wire, oral, or electronic communication involving
- 3 any of the same persons, facilities, or places specified in the
- 4 application and the action taken by the judge on each previous
- 5 application.
- 6 (d) If the application is for extension of an order, a
- 7 statement setting forth the results obtained from the interception
- 8 or a reasonable explanation of the failure to obtain any results.
- 9 (e) Unless the applying investigative or law enforcement
- 10 officer is employed by the department of state police, a statement
- 11 that the director of the department of state police or an
- 12 individual the director designates has been notified of the
- 13 application and the information described in subdivision (b) (ii) and
- **14** (iv).
- 15 (f) A statement of the estimated cost of the manpower and
- 16 other resources used in the interception for the period of time the
- interception is authorized.
- 18 (2) The judge of competent jurisdiction may require the
- 19 applicant to furnish additional testimony or documentary evidence
- 20 to support the application.
- 21 (3) Based upon an application under subsection (1), the judge
- 22 of competent jurisdiction may enter an ex parte order, as requested
- 23 or as modified, authorizing or approving interception of a wire,
- 24 oral, or electronic communication if the judge determines all of
- 25 the following on the basis of the facts submitted by the applicant:
- 26 (a) Probable cause exists to believe an individual is
- 27 committing, has committed, or is about to commit a particular

- 1 offense described in section 7.
- 2 (b) Except as provided in section 9, probable cause exists to
- 3 believe the facilities from which, or the place where, the wire,
- 4 oral, or electronic communication is to be intercepted are being
- 5 used, or are about to be used, in connection with the offense or
- 6 are leased to, listed in the name of, or commonly used by a person
- 7 described in subsection (1)(b)(iv).
- 8 (c) Probable cause exists to believe particular communications
- 9 concerning that offense will be obtained through the interception.
- 10 (d) Usual investigative procedures have been tried and have
- 11 failed or reasonably appear to be unlikely to succeed if tried or
- 12 to be dangerous.
- 13 (4) Each order authorizing or approving interception of a
- 14 wire, oral, or electronic communication shall specify all of the
- 15 following:
- 16 (a) If known, the identity of the person whose communication
- is to be intercepted.
- 18 (b) The nature and location of the communication facilities as
- 19 to which, or the place where, authority to intercept is granted.
- 20 (c) A particular description of the type of communication
- 21 sought to be intercepted and a statement of the particular offense
- 22 to which it relates.
- 23 (d) The legitimate investigative objective for which
- 24 authorization to intercept is granted.
- 25 (e) The agency authorized to intercept the communication and
- 26 the person authorizing the application.
- 27 (f) The time period during which interception is authorized or

- 1 approved, including a statement as to whether interception shall
- 2 automatically terminate when the described communication has been
- 3 obtained.
- 4 (5) If the application states that specific information,
- 5 facilities, or technical assistance is needed from a particular
- 6 person to accomplish the interception unobtrusively and with
- 7 minimum interference with the services that person is according a
- 8 person whose communications are to be intercepted, the order
- 9 authorizing the interception shall direct the particular person to
- 10 immediately furnish the information, facilities, or technical
- 11 assistance specified in the order to the applicant. The order shall
- 12 specify the time period during which the person is required to
- 13 provide information, facilities, or technical assistance. The
- 14 agency conducting the interception shall compensate the person
- 15 furnishing facilities or technical assistance for reasonable
- 16 expenses incurred in providing the facilities or assistance. A
- 17 person is not civilly liable for providing information, facilities,
- 18 or assistance under this subsection.
- 19 (6) An order entered under this section shall not authorize or
- 20 approve the interception of a wire, oral, or electronic
- 21 communication for longer than the time necessary to achieve the
- 22 authorized investigative objective or 30 days, whichever is
- 23 earlier. The period begins on the day an investigative or law
- 24 enforcement officer first begins to conduct an interception under
- 25 the order or 10 days after the order is entered, whichever is
- 26 earlier. The judge may grant extensions of an order only upon
- 27 application for an extension and in accordance with subsections (1)

- 1 and (3). The extension period shall not be longer than the time the
- 2 judge determines is necessary to achieve the purposes for which the
- 3 order was granted or 30 days, whichever is earlier. Only 2
- 4 extensions of an order may be granted. After the second extension
- 5 of an order terminates, an investigative or law enforcement officer
- 6 may apply for and be granted an order authorizing the interception
- 7 of a wire, oral, or electronic communication based on the
- 8 information contained in the application for the terminated order
- 9 only if the new application includes new evidence, in addition to
- 10 that described in the previous application, justifying the
- 11 officer's belief that an order should be issued.
- 12 (7) Each order and extension shall provide that the
- 13 authorization to intercept be executed as soon as practicable, be
- 14 conducted so as to minimize the interception of communications not
- 15 otherwise subject to interception under this act, and terminate
- 16 when the authorized objective is obtained or, in any event, after
- 17 not more than 30 days.
- 18 (8) An order authorizing interception under this act shall
- 19 require reports to the judge who issued the order showing the
- 20 progress made toward achieving the authorized objective and any
- 21 need for continued interception. The reports shall be made weekly
- 22 or at shorter intervals as the judge requires.
- 23 (9) The contents of a wire, oral, or electronic communication
- 24 intercepted as authorized by this act shall be recorded on tape or
- 25 by a comparable recording device. Recording under this subsection
- 26 shall be done in a way that protects the recording from editing or
- 27 other alterations. When an order or extension expires, all

- 1 recordings shall immediately be made available to the judge issuing
- 2 the order and sealed under his or her directions. Custody of the
- 3 recordings shall be where the judge orders. The recordings shall
- 4 not be destroyed except upon order of the judge or his or her
- 5 successor, but, except as otherwise provided in this subsection,
- 6 shall be retained for at least 10 years. However, if evidence is
- 7 not obtained from the interception within 1 year, a party
- 8 intercepted may move for destruction of the recordings. Duplicate
- 9 recordings may be made for use or disclosure of contents or
- 10 evidence under section 6(1) for investigations. The presence of the
- 11 seal or a satisfactory explanation for its absence is a
- 12 prerequisite for use or disclosure of contents or evidence under
- **13** section 6(2).
- 14 (10) The judge shall seal applications made and orders granted
- 15 under this act. Custody of the applications and orders shall be
- 16 where the judge directs. The applications and orders shall be
- 17 disclosed only upon a showing of good cause before a judge of
- 18 competent jurisdiction. The applications and orders shall not be
- 19 destroyed except on order of the judge or his or her successor, but
- 20 shall be retained for at least 10 years.
- 21 (11) Within a reasonable time, but not later than 90 days
- 22 after an order or extension terminates, the judge shall cause an
- 23 inventory to be served on the persons named in the order and on
- 24 other parties to intercepted communications as the judge determines
- 25 is in the interest of justice. Upon showing good cause, a judge may
- 26 delay the service of the inventory required under this subsection
- 27 for 1 or more periods. Each period shall not be greater than 30

- 1 days. The inventory shall include notice of all of the following:
- 2 (a) Entry of the order.
- 3 (b) The date the order was entered and the period of
- 4 authorized or approved interception.
- 5 (c) The fact that during the period wire, oral, or electronic
- 6 communications were or were not intercepted.
- 7 (12) If a person given an inventory under subsection (11)
- 8 files a motion and serves a copy of the motion on the law
- 9 enforcement agency described in subsection (11) and other parties
- 10 as required by law, the judge shall make available to the person or
- 11 his or her attorney for inspection the portions of the intercepted
- 12 communications to which the person was a party and the portions of
- 13 the applications and orders pertaining to communications to which
- 14 the person was a party.
- 15 (13) The contents of a wire, oral, or electronic communication
- 16 intercepted under this act or evidence derived from the
- 17 communication shall not be received in evidence or otherwise
- 18 disclosed in a trial, hearing, preliminary examination, or other
- 19 proceeding in a court unless each party has been furnished with a
- 20 copy of the application and order authorizing or approving the
- 21 interception before the preliminary examination or not less than 21
- 22 days before the trial, hearing, or other proceeding. In the
- 23 interest of justice, the judge may adjourn the trial, hearing, or
- 24 other proceeding to allow the defendant at least 21 days to review
- 25 that evidence.
- 26 (14) An aggrieved person in a trial, hearing, preliminary
- 27 examination, or other proceeding before a court, grand jury,

- 1 tribunal, department or regulatory agency, legislative committee,
- 2 or other authority of this state or a political subdivision may
- 3 move to suppress the contents of a wire, oral, or electronic
- 4 communication intercepted under this act or evidence derived from
- 5 the communication on 1 or more of the following grounds:
- 6 (a) The communication was unlawfully intercepted.
- 7 (b) The order of authorization or approval under which the
- 8 communication was intercepted is insufficient on its face.
- 9 (c) The interception was not in conformity with the order of
- 10 authorization or approval.
- 11 (15) A motion to suppress under subsection (14) shall be made
- 12 before the trial, hearing, preliminary examination, or other
- 13 proceeding unless there is no opportunity to make the motion before
- 14 the trial, hearing, preliminary examination, or other proceeding or
- 15 the aggrieved person making the motion is not aware of the grounds
- 16 of the motion before the trial, hearing, preliminary examination,
- 17 or other proceeding. If the aggrieved person files a motion, the
- 18 judge may make available to the aggrieved person or his or her
- 19 attorney for inspection any portion of the intercepted
- 20 communication or evidence derived from the intercepted
- 21 communication that the judge determines is in the interests of
- 22 justice. If the judge grants the motion to suppress under
- 23 subsection (14), the intercepted wire, oral, or electronic
- 24 communication or evidence derived from the communication shall be
- 25 treated as having been obtained in violation of this act.
- 26 (16) The prosecutor may appeal an order granting a motion to
- 27 suppress under subsection (14) or the denial of an application for

- 1 an order of approval if the prosecutor certifies to the judge or
- 2 other official granting the motion or denying the application that
- 3 the appeal is not taken for delay. The prosecutor shall take the
- 4 appeal within 30 days after the order granting the motion to
- 5 suppress is entered or the application is denied and shall
- 6 prosecute it diligently.
- 7 (17) A violation of subsection (9) or (10) may be punished as
- 8 contempt of the court that approved or denied the application for
- 9 interception.
- 10 (18) An order authorizing interception under this act shall
- 11 also authorize the entry of the premises covered under the order
- 12 for the sole purpose of installing, maintaining, or removing an
- interception device. The judge who issued the order shall be
- 14 notified within 48 hours of the time and method of each entry
- 15 allowed by this subsection.
- 16 Sec. 9. (1) The requirements of section 8(1) (b) (ii) and (3) (b)
- 17 relating to the specification of the facilities from which, or the
- 18 place where, the communication is to be intercepted do not apply if
- 19 any of the following circumstances exist:
- 20 (a) In the case of an application with respect to the
- 21 interception of an oral communication, all of the following
- 22 circumstances exist:
- (i) The application is by a state or local law enforcement
- 24 officer and is approved by the attorney general, designated
- 25 assistant attorney general, or principal prosecuting attorney or
- 26 designated assistant prosecuting attorney.
- 27 (ii) The application contains a full and complete statement as

- 1 to why the specification is not practical and identifies the person
- 2 committing the offense and whose communications are to be
- 3 intercepted.
- 4 (iii) The judge finds that the specification is not practical.
- 5 (b) In the case of an application with respect to a wire or
- 6 electronic communication, all of the following circumstances exist:
- 7 (i) The application is by a state or local law enforcement
- 8 officer and is approved by the attorney general, designated
- 9 assistant attorney general, or principal prosecuting attorney or
- 10 designated assistant prosecuting attorney.
- 11 (ii) The application identifies the person believed to be
- 12 committing the offense and whose communications are to be
- 13 intercepted and the applicant makes a showing that there is
- 14 probable cause to believe that the person's actions could have the
- 15 effect of thwarting interception from a specified facility.
- 16 (iii) The judge finds that the showing has been adequately made.
- (iv) The order authorizing or approving the interception is
- 18 limited to interception only for the time that is reasonable to
- 19 presume that the person identified in the application is or was
- 20 reasonably proximate to the instrument through which the
- 21 communication will be or was transmitted.
- 22 (2) An interception of a communication under an order with
- 23 respect to which the requirements of section 8(1)(b)(ii) and (3)(b)
- 24 do not apply under subsection (1)(a) shall not begin until the
- 25 place where the communication is to be intercepted is ascertained
- 26 by the person implementing the interception order. A provider of
- 27 wire or electronic communications service that has received an

- 1 order as provided for in subsection (1)(b) may move the court to
- 2 modify or quash the order on the ground that its assistance with
- 3 respect to the interception cannot be performed in a timely or
- 4 reasonable fashion. The court, upon notice to the government, shall
- 5 decide the motion expeditiously.
- 6 Sec. 10. (1) Within 30 days after an order or extension
- 7 entered under section 8 expires or the judge denies an order
- 8 authorizing or approving interception of a wire, oral, or
- 9 electronic communication, the judge shall report all of the
- 10 following information to the administrative office of the United
- 11 States courts and to the department of state police:
- 12 (a) The fact that an order or extension was applied for.
- 13 (b) The kind of order or extension applied for.
- 14 (c) Whether the order or extension was granted as applied for,
- 15 modified, or denied.
- 16 (d) The interception time period authorized and the number and
- 17 duration of any extensions of the order.
- 18 (e) Any offense specified in the application, order or
- 19 extension.
- 20 (f) The identity of the investigative or law enforcement
- 21 officer and agency applying and the prosecutor authorizing the
- 22 application.
- 23 (g) The nature of the facilities from which, or the place
- 24 where, communications were to be intercepted.
- 25 (2) In January of each year, the attorney general shall report
- 26 to the administrative office of the United States courts all of the
- 27 following:

- 1 (a) The information required by subsection (1) with respect to
- 2 each application for an order or extension authorizing or approving
- 3 an interception of a wire, oral, or electronic communication made
- 4 during the preceding calendar year.
- 5 (b) A general description of the interceptions made under each
- 6 order or extension described in subdivision (a), including all of
- 7 the following:
- 8 (i) The approximate nature and frequency of incriminating
- 9 communications intercepted.
- (ii) The approximate nature and frequency of other
- 11 communications intercepted.
- 12 (iii) The approximate number of persons whose communications
- 13 were intercepted.
- 14 (iv) The approximate nature, amount, and cost of the manpower
- 15 and other resources used in the interceptions.
- 16 (c) The number of arrests resulting from the interceptions
- 17 described in subdivision (b) and the offenses for which arrests
- 18 were made.
- 19 (d) The number of trials resulting from the interceptions
- 20 described in subdivision (b).
- 21 (e) The number of motions to suppress made with respect to the
- 22 interceptions described in subdivision (b) and the number granted
- 23 or denied.
- 24 (f) The number of convictions resulting from the interceptions
- 25 described in subdivision (b), the offenses for which the
- 26 convictions were obtained, and a general assessment of the
- 27 importance of the interceptions.

- 1 (g) The information required by subdivisions (b) to (f) with
 2 respect to orders or extensions for interception of wire, oral, or
 3 electronic communications obtained in a preceding calendar year.
- 4 (3) On or before January 10 of each year, the department of 5 state police shall report to the attorney general, senate, house of 6 representatives, and governor all of the information regarding 7 applications, orders, and interceptions of wire, oral, or

electronic communications required under subsection (2).

8

19

27

costs of training.

- 9 Sec. 11. The attorney general and the director of the 10 department of state police shall establish a course of training in 11 the legal and technical aspects of intercepting wire, oral, or 12 electronic communications, regulations he or she finds necessary or appropriate for the training program, and minimum standards for the 13 14 certification and periodic recertification of investigative or law 15 enforcement officers eligible to intercept wire, oral, or electronic communications under this act. The director of the 16 17 department of state police shall charge each officer who enrolls in 18 this training program a reasonable enrollment fee to offset the
- Sec. 12. An officer, employee, or agent of an electronic communication service provider who learns of the existence of an interception device in the course of his or her employment or otherwise shall report the device's existence to the department of state police. The department of state police shall determine whether placement of the device is authorized by court order. If placement of the device is not authorized by court order, the

department of state police shall immediately inform the person

- 1 whose wire, oral, or electronic communication was intercepted or
- 2 intended to be intercepted of the device's existence. This section
- 3 does not diminish or excuse any obligation of the department of
- 4 state police, the officer, employee, or agent of the electronic
- 5 communication service provider, or any other person to remove the
- 6 device or to take any other actions required by law, regulation, or
- 7 policy.
- 8 Sec. 13. (1) Except as provided in section 8(5), a person
- 9 whose wire, oral, or electronic communication is intercepted,
- 10 disclosed, or used in violation of this act has a civil cause of
- 11 action against any person who intercepts, discloses, uses, or
- 12 procures another person to intercept, disclose, or use the
- 13 communication or its contents. In the civil cause of action, the
- 14 person is entitled to recover all of the following:
- 15 (a) Actual damages, but not less than \$1,000.00 a day for each
- 16 day of a violation.
- 17 (b) Exemplary damages.
- 18 (c) Reasonable attorney fees and other litigation costs
- 19 reasonably incurred.
- 20 (2) A good-faith reliance on a court order or a legislative
- 21 authorization is a defense to a civil or criminal action brought
- 22 under this act or any other law.
- 23 Sec. 14. Purchases of an interception device shall be recorded
- 24 as a separate line item on any state or local appropriation bill.
- 25 Sec. 15. This act does not prohibit any of the following:
- 26 (a) An interception otherwise permitted by law for a peace
- 27 officer of this state or of the federal government, or the

- 1 officer's agent, while in the performance of the officer's duties.
- 2 (b) Hearing a communication transmitted by common carrier
- 3 facilities by an employee of a communications common carrier when
- 4 acting in the course of his or her employment.
- 5 (c) The recording by a public utility of telephone
- 6 communications to it requesting service or registering a complaint
- 7 by a customer, if a record of the communications is required for
- 8 legitimate business purposes and the agents, servants, and
- 9 employees of the public utility are aware of the practice by an
- 10 employee safeguarding property owned by, or in custody of, his or
- 11 her employer on his or her employer's property.
- 12 (d) The routine monitoring, including recording, by employees
- 13 of the department of corrections of telephone communications on
- 14 telephones available for use by prisoners in state correctional
- 15 facilities, if the monitoring is conducted in the manner prescribed
- 16 by section 70 of the corrections code of 1953, 1953 PA 232, MCL
- 17 791.270, and rules promulgated under that section.
- 18 Sec. 16. Any court of criminal jurisdiction may enter an order
- 19 authorizing the use of a pen register or a trap and trace device as
- 20 provided in 18 USC 3121.
- Sec. 17. The director of the department of state police or a
- 22 person designated by the director shall maintain custody of all
- 23 interception devices to be used by state law enforcement officers
- 24 during the periods in which those devices are not being used for
- 25 interception purposes under a court order. The sheriff for a county
- 26 or a person designated by the sheriff shall maintain custody of all
- 27 interception devices to be used by local law enforcement officers

- 1 in that county during periods in which those devices are not being
- 2 used for interception purposes under a court order. The director of
- 3 state police and the sheriff for a county or their designees shall
- 4 maintain a custody log of interception devices that are in their
- 5 custody under this section. The log shall keep a record of the
- 6 following information:
- 7 (a) Each person who has been granted access to the
- 8 interception device.
- 9 (b) The inclusive dates of access.
- 10 (c) The purpose of the access.
- 11 (d) If access is pursuant to a court order, the name of the
- 12 judge who issued the order.