Senate Fiscal Agency P. O. Box 30036 Lansing, Michigan 48909-7536



Telephone: (517) 373-5383 Fax: (517) 373-1986 TDD: (517) 373-0543

Senate Bill 633 (as introduced 6-26-97)

Sponsor: Senator Jon Cisky Committee: Judiciary

Date Completed: 9-29-97

CONTENT

The bill would create a new act to permit the interception of wire, oral, or electronic communication pursuant to judicial authorization in the investigation of specific drug-related offenses and to do the following:

- Permit applications for the interception of communication to be authorized by a prosecutor, and approved by the judge, if other investigative techniques had failed.
- -- Permit the contents of an intercepted communication or evidence derived from it to be used or disclosed by an investigative or law enforcement officer in the performance of his or her duties, or to be disclosed by a person giving testimony.
- -- Prohibit the disclosure or use of the contents of a communication that was wrongfully intercepted.
- Prohibit the manufacture, possession or sale (except by providers of an electronic communication service and governmental officials and employees), or the advertisement of devices primarily used for the interception of communication.
- Require that persons named in an order be given notice of its approval and implementation after the judge was notified of the investigation's termination.
- -- Allow a party to an intercepted communication, or a person against whom interception was directed, to move to suppress evidence of the contents of the communication or evidence derived from it.
- Require the development of a communication interception training program for law enforcement officers.
- -- Establish various reporting requirements.

- -- Require employees of a provider of electronic communication service to report the existence of an interception device to local prosecutors.
- Create a civil cause of action for victims of a wrongful interception and make good faith reliance on an authorization a defense to civil or criminal liability.
- Require that purchases of any interception device be recorded as a separate line item on any State or local appropriation bill.
- -- Repeal eavesdropping provisions of the Michigan Penal Code.

The bill includes an effective date of January 1, 1998, and would be repealed on January 1, 2001.

Definitions

An "oral communication" would be something "uttered by a person with a reasonable expectation that the communication is not subject to interception", but would not include electronic communication. "Electronic communication" would be defined as "a transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system". Electronic communication would not include a wire or oral communication; a communication made through a tone-only paging device; or a communication from an electronic or mechanical device that permits the tracking of an individual's or object's movement. communication" would be "an aural transfer made in whole or in part through the use of facilities for transmitting communications by wire, cable, or other substantially similar connection between the point of origin and the point of reception that are

Page 1 of 10 sb633/9798

furnished or operated by a person engaged in providing or operating those facilities for the transmission of communications". Wire communication also would include an electronic storage of such a communication, but would not include an electronic communication.

An "aural transfer" would be "a transfer containing the human voice at any point between the point of origin and the point of reception, including those points". "Intercept" would mean "the aural or other acquisition of the contents of a wire, oral, or electronic communication through the use of an interception device". "Contents" would mean "any information concerning the substance, purport, or meaning of a wire, oral, or electronic communication".

An "electronic communication service" would be "a service that provides to the service's users the ability to send or receive wire or electronic communications". "Electronic storage" would mean either the temporary, intermediate storage of a wire or electronic communication incidental to electronic transmission or storage of a wire or electronic communication by an electronic communication service for backup protection of the communication.

"Interception device" would mean "a device or apparatus that can be used to intercept a wire, oral, or electronic communication". Interception device would not include either of the following:

- -- A telephone or telegraph instrument, equipment, or facility or any component that was furnished or used in the ordinary course of legitimate business.
- -- A hearing aid or similar device used to correct subnormal hearing to not better than normal.

Interception/Disclosure

Except as otherwise provided in the bill, or as authorized or approved under Federal law, it would be a felony, punishable by up to four years' imprisonment and/or a maximum fine of \$2,000, intentionally to do or attempt to do any of the following:

- -- Intercept, or attempt to intercept, any wire, oral, or electronic communication, or solicit another to do so.
- Disclose or attempt to disclose to another the contents of a wire, oral, or electronic communication, knowing or having reason to

- know that the information was obtained through the prohibited interception of such a communication.
- -- Use or attempt to use the contents of a wire, oral, or electronic communication, knowing or having reason to know that it was intercepted in violation of the bill.

Conduct listed above would not be punishable unless it were for the purpose of direct or indirect commercial advantage or private or financial gain and both 1) the conduct consisted of or related to the interception of a satellite transmission that was not encrypted or scrambled, and 2) the satellite transmission was sent either to a broadcasting station for retransmission to the general public or as an audio subcarrier intended for redistribution to facilities open to the public but was not a data transmission or telephone call.

It would be a misdemeanor to trespass on another's property with the intent to intercept or facilitate intercepting a wire, oral, or electronic communication. The trespassing offense would be punishable by up to 90 days' imprisonment, a maximum fine of \$100, or both.

The bill specifies that it would <u>not</u> prohibit any of the following:

- -- Intercepting, using, or disclosing a wire communication by a switchboard operator, or an employee, officer, or agent of a provider of an electronic communication service, if the activity were in the normal course of his or her duties or employment while engaged in an activity that was "necessarily incident to rendering service or protecting the provider's rights or property", unless the interception resulted from the service provider's observation or random monitoring for purposes other than mechanical or service quality control checks.
- -- Intercepting a wire or electronic communication, or a radio-transmitted oral communication, or disclosing or using such information, by an officer, employee, or agent of the Federal Communications Commission (FCC) in the course of performing his or her monitoring responsibilities in the enforcement of the Federal Communications Act (48 Stat. 1064).
- -- Intercepting a wire, oral, or electronic communication by a person acting under color of law, if the person were a party to the communication or one of the parties to the

Page 2 of 10 sb633/9798

- communication had given prior consent.
- Intercepting a wire or oral communication by a person not acting under color of law, if the person were a party to the communication or one of the parties had given prior consent, unless the communication were intercepted to commit a criminal or tortious act.
- -- Conducting electronic surveillance, as defined in the Federal Foreign Intelligence Surveillance Act (50 U.S.C. 1801), by an officer, employee, or agent of the United States in the normal course of official duty to conduct that surveillance.
- Intercepting or gaining access to an electronic communication through a system configured so that the communication was readily accessible to the general public.
- -- Engaging in certain conduct that was either prohibited by or excepted from the application of sections of the Federal Communications Act (47 U.S.C. 553 and 47 U.S.C. 605).
- -- Intercepting a wire or electronic communication, whose transmission was causing harmful interference to a lawfully operating station or consumer electronic equipment, to the extent necessary to identify the interference.
- Intercepting a radio communication made through a system that used frequencies monitored by individuals engaged in the provision or use of the system, if the communication were not scrambled or encrypted.
- -- Using a pen register or a trap and trace device.
- -- Recording, by a provider of electronic communication service, the fact that a wire or electronic communication was initiated or completed, to protect the provider, another provider furnishing service, or a user of service from fraudulent, unlawful, or abusive use of the service.

The bill also would not prohibit the interception of a radio communication that was transmitted by: a station for the use of the general public or that related to a ship, aircraft, vehicle, or person in distress; a governmental, law enforcement, civil defense, private land mobile, or public safety communications system that was readily available to the general public; a station operating on an authorized frequency within bands allocated to citizens band, amateur, or general mobile radio services; or, a marine or aeronautical communications system.

A person could give information, facilities, or technical assistance to a person authorized by law to intercept a wire, oral, or electronic communication or conduct electronic surveillance, if the person had been provided with a court order authorizing such assistance. The person giving assistance could not disclose the existence of the interception or surveillance devices, except as otherwise required by legal process and only after prior notification to the Attorney General or principal prosecuting attorney of a county. The person giving assistance could not be held civilly liable for providing any information, facilities, or assistance in accordance with the terms of a court order.

A person who provided electronic communication service to the public could not intentionally divulge the contents of a communication to a person or entity other than the addressee or intended recipient of the communication or an agent of the addressee or intended recipient. (This would not apply if the communication service provider were the addressee or intended recipient.) An electronic communication service provider could divulge the contents of a communication, however, if any of the following applied:

- -- The communication was intercepted under one of the circumstances specifically allowed by the bill (listed above).
- -- The information was revealed by one law enforcement officer to another as part of an investigation.
- -- The communication was revealed with the lawful consent of the originator or the addressee or intended recipient.
- -- The communication was revealed to a person employed or authorized, or whose facilities were used, to forward the communication to its destination.
- -- The contents of the communication were inadvertently obtained by the service provider and appeared to relate to the commission of a crime, if the divulgence were made to a law enforcement agency.

Prohibited Manufacture/Possession/ Advertisement

Except as provided below for providers of an electronic communication service (generally, phone companies) and governmental officers or employees, or as authorized or approved under Federal law (18 U.S.C. 2510 to 2521), it would be a felony, punishable by up to four years' imprisonment and/or a maximum fine of \$2,000, to do any of the following:

Page 3 of 10 sb633/9798

- -- Manufacture, assemble, possess, or sell or otherwise deliver any interception device, knowing or having reason to know that its design made it primarily useful for the surreptitious interception of wire or oral communication.
- Advertise or offer to sell or otherwise deliver such a device in a publication, having such knowledge or reason to know of the device's design.
- Advertise or offer to sell or otherwise deliver any device promoting the use of the device for the surreptitious interception of wire or oral communication.

An interception device could be manufactured, assembled, possessed, or sold, with knowledge or reason to know that its design made it primarily useful for the surreptitious interception of wire or oral communication, however, by either of the following:

- -- An officer, agent, or employee of the United States, this State, or a political subdivision (i.e., a county, city, township, or village) of this State, pursuant to a validly authorized warrant issued by a court of competent jurisdiction of the United States, State, or political subdivision.
- -- A provider of an electronic communication service or an officer, agent, or employee of, or a person under contract with, a service provider, in the normal course of the business of providing that service.

Interception Order: Offenses

A prosecutor (i.e., the State Attorney General or the principal prosecuting attorney of the county in which an interception was to be made, or a single designated assistant of the Attorney General or prosecutor) could authorize an application to a judge of competent jurisdiction for an order authorizing or approving the interception of a wire, oral, or electronic communication by the investigative or law enforcement officer having responsibility for the investigation of the offense for which the application was made, if the interception could provide or had provided evidence of any of the following offenses:

-- The manufacture, delivery, or possession with intent to manufacture or deliver of a controlled substance classified as a narcotic drug on Schedule 1 or 2 of Chapter 7 of the Public Health Code. (Those schedules include substances such as opium, opium

- derivatives, stimulants and depressants having potential for abuse, and cocaine.)
- -- The creation, delivery, or possession with intent to deliver, of a counterfeit substance classified as a narcotic drug on Schedule 1 or 2.
- -- The knowing or intentional possession, except pursuant to a valid prescription, of a controlled substance classified as a narcotic drug on Schedule 1 or 2 in an amount of 50 grams or more.
- -- The illegal creation, delivery, or possession with intent to deliver, of a controlled substance analogue of a Schedule 1 or 2 narcotic or cocaine.
- -- The knowing or intentional possession, except pursuant to a valid prescription, of a controlled substance analogue of a Schedule 1 or 2 narcotic or cocaine.
- -- A conspiracy to commit one of the foregoing offenses.
- -- An offense other than those described above (if communication relating to the offense were intercepted during an authorized interception).

("Judge of competent jurisdiction" would mean a judge of the Court of Appeals, or a circuit court judge.)

A county prosecuting attorney, or his or her designee, could not authorize an application under the bill unless the Attorney General, or his or her designee, approved the authorization.

Unless the investigative or law enforcement officer were employed by the Department of State Police, the prosecutor authorizing the application would have to notify the Director of the Department. If the proposed interception would overlap, conflict with, hamper, or interfere with another proposed or authorized interception, the Director or the Director's designee would have to advise the judge for each application and coordinate subsequent interceptions.

Interception Order: Application

An application for an interception order would have to be made in writing upon oath or affirmation to a judge of competent jurisdiction, would have to state the applicant's authority to apply, and would have to include the following information:

-- The identity of the investigative or law enforcement officer applying, and the prosecutor authorizing it. If approval by the

Page 4 of 10 sb633/9798

Attorney General or his or her designated assistant were required, the application would have to include a statement of that approval.

- -- A comprehensive statement of the facts and circumstances relied upon by the applicant to justify his or her belief that an order should be issued, including details as to the particular offense that had been, was being, or was about to be committed; a particular description of the nature and location of the facilities or place where the communication was to be intercepted: a particular description of the type of communication in question; the identity, if known, of the person committing or about to commit the offense and whose communication was to be intercepted; and a statement of the facts indicating the specific instances of conduct that demonstrated probable cause to believe that the particular offense had been, was being, or was about to be committed.
- A comprehensive statement as to whether other investigative procedures had been tried and had failed.
- -- A comprehensive statement of the period of time for which the interception had to be maintained. If, due to the nature of the investigation, the authorization for interception should not automatically terminate when the communication had been first obtained, the statement would have to include a particular description of the facts establishing probable cause to believe that additional communications of the same type would subsequently occur.
- -- A comprehensive statement of the "legitimate investigative objective" to be achieved by the interception.
- -- A comprehensive statement of the facts concerning all known previous applications made for authorization or approval to intercept involving any of the same persons, facilities, or places, and the action taken by the judge on each application.
- -- A statement of the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain results, if the application were for the extension of an order.
- -- A statement that the Department of State Police had been notified of the application and of the information concerning the facilities and the person in question, unless the officer making the application was employed by the Department.

The judge could require the applicant to furnish additional testimony or documentary evidence to support the application.

Applications made and orders granted under the bill would have to be sealed by the judge. Custody of the applications and orders would be wherever the judge directed. The applications and orders could be disclosed only upon a showing of good cause before a judge of competent jurisdiction. They would have to be retained for one year after the judge was notified that the investigation had terminated, and could be destroyed only on order of the judge.

("Investigative or law enforcement officer" would mean any officer of this State or a political subdivision of the State empowered by law to conduct investigations of, or to make arrests for, the pertinent offenses, and certified under the proposed certification requirements.)

Interception Order: Authorization/Duration

Based upon a filed application, the judge could enter an ex parte order (without notice to or representation of an opposing party) authorizing or approving interception if the judge determined on the basis of the facts submitted by the applicant all of the following:

- -- Probable cause existed to believe that an individual was committing, had committed, or was about to commit, a particular substance abuse offense as described above.
- -- Probable cause existed to believe that the facilities or place where the interception was to be made were being or were about to be used in connection with the commission of the offense, or were leased to, listed in the name of, or commonly used by the person identified as committing the offense and whose communication was to be intercepted.
- Probable cause existed to believe that particular communications concerning the offense would be obtained through the interception.
- -- Usual investigative procedures had been tried and had failed.

An interception order would have to specify all of the following:

- -- If known, the identity of the person whose communication was to be intercepted.
- -- The nature and location of the communication facilities as to which, or the place where, authority to intercept was

Page 5 of 10 sb633/9798

granted.

- A particular description of the type of communication sought to be intercepted and a statement of the offense to which it related.
- -- The legitimate investigative objective for which the interception order was granted.
- -- The agency authorized to intercept the communication and the person authorizing the application.
- The time period during which the interception was authorized or approved, including a statement as to whether the interception would automatically terminate when the described communication had been first obtained.

An interception order would have to require reports to be made, at weekly or shorter intervals, to the issuing judge showing what progress had been made toward achieving the authorized objective and the need for continued interception.

An interception order could not authorize or approve interception for a period longer than necessary to achieve the objective of the authorization or 30 days, whichever was earlier. The 30-day period would begin on the day the interception was initiated or 10 days after the authorizing order was entered, whichever was later. Extensions of an order could be granted upon application for an extension and upon the judge's making the required findings. The period of extension could not be longer than the judge considered necessary to achieve the purposes of the order or 30 days, whichever was earlier. Only two extensions could be granted. After the termination of a second extension, the officer could apply for and receive an interception order based on the application for the terminated order only if the new application included new evidence justifying the officer's belief that an order should be issued.

Each order and extension would have to provide that the authorization to intercept would have to be executed as soon as practicable, conducted in such a way as to minimize the interception of communications not otherwise subject to interception under the bill, and terminated upon attainment of the authorized objective or, in any event, in 30 days.

If an application for an interception order stated the need for facilities, technical assistance, or specific information from a particular person, the interception order would have to direct the person to furnish the facilities, assistance, or information. The order would have to specify the time period

during which the person was required to provide information, facilities, or technical assistance. The agency conducting the interception would have to compensate the person for reasonable expenses incurred in providing the facilities or assistance.

Interception Order: Recording

The contents of an intercepted communication would have to be recorded on tape or by a comparable recording device in a way that would protect the recording from editing or other alterations. When an order or extension expired, all recordings immediately would have to be made available to the issuing judge and sealed under his or her directions. The presence of the seal, or a satisfactory explanation for the absence of a seal, would be a prerequisite for the use or disclosure by a person giving testimony as to the contents of the communication or evidence derived from it.

Custody of the recordings would be wherever the judge ordered. The recordings could not be destroyed except upon an order of the judge, and would have to be retained for at least 10 years. Duplicate recordings could be made for use or disclosure by an investigative or law enforcement officer to another officer or for use by an officer in the proper performance of his or her duties (as discussed below).

Notice to Named Persons

Within a "reasonable time", but no later than 90 days after the termination of an approved or extended order, the judge would have to cause to be served on those persons named in the order and other parties to the intercepted communication, an inventory that included notice of all of the following:

- -- The entry of the order.
- -- The date the order was entered and the period of authorized or approved interception.
- -- The fact that during that period wire, oral, or electronic communications were or were not intercepted.

If a person given an inventory filed a motion and served a copy of the motion on the law enforcement agency, the judge would have to make available to that person or his or her attorney, for inspection, the portions of the communications to which the person was a party. The person also would have to be given the portions of the applications and orders pertaining to communications to which he or she was a party.

Page 6 of 10 sb633/9798

Disclosure

The contents of an intercepted communication and any evidence derived from it could not 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 the State or a political subdivision of the State, if disclosure would violate the bill.

An investigative or law enforcement officer who, by any means authorized by the bill, had obtained knowledge of the contents of a wire or oral communication or evidence derived from it could do the following:

- Disclose the contents of the communication or the evidence to another investigative or law enforcement officer, or to an officer, agent, or official of a Federal law enforcement agency, to the extent that the disclosure was appropriate to the proper performance of the officer's official duties.
- -- Use the contents of the communication or the evidence to the extent the use was appropriate to the proper performance of the officer's official duties.

A person who received, by any authorized means, any information concerning an intercepted communication or evidence derived from it could disclose the contents of the communication or the evidence if giving testimony under oath or affirmation in any proceeding held under the authority of the United States, this State, or a political subdivision of this State, or in a civil action brought by a person whose communication was wrongfully intercepted, disclosed, or used.

If an officer, while engaged in authorized interception, intercepted a communication relating to an offense other than that specified in the interception order, the contents of the communication and derived evidence could be disclosed or used by the officer as provided above. The contents and evidence could be disclosed in testimony if authorized or approved by a judge of competent jurisdiction, if the judge found on subsequent application that the contents were otherwise intercepted in compliance with the bill. The subsequent application would have to be made as soon as practicable after the interception. The bill specifies, however, that these provisions would not authorize the disclosure or use in any manner of the contents of, or evidence derived from, a wire, oral, or electronic communication relating to an offense that is punishable by imprisonment for four years or less or by only a fine.

A privileged communication intercepted in accordance with or in violation of the bill would not lose its privileged character and could not be disclosed.

<u>Admission</u> in <u>Evidence/Suppression/</u> Appeal/Contempt

The contents of an intercepted communication or evidence derived from it could not be received in evidence or otherwise disclosed in any trial, hearing, preliminary examination, or other proceeding in a court unless each party, before the preliminary examination or not less than 21 days before the trial, hearing, or proceeding had been given a copy of the application and order.

An "aggrieved person" (i.e., a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed) in a trial, hearing, or other proceeding before a court, grand jury, tribunal, or department, regulatory body, legislative committee or other authority of the State or a political subdivision of the State, could move to suppress the contents of an intercepted communication on one or more of the following grounds:

- -- The communication was unlawfully intercepted.
- -- The order of authorization or approval was insufficient on its face.
- -- The interception was not made in conformity with the order.

A motion to suppress would have to be made before the proceeding unless there was not an opportunity to do so or the aggrieved person was not aware of the grounds of the motion before the proceeding. The person or his or her attorney could inspect a portion of the communication, or evidence derived the from intercepted communication, as the judge determined to be in the interests of justice. If the motion were granted, the communication or evidence would have to be treated as having been obtained in violation of the bill.

The prosecutor could appeal from an order granting a motion to suppress, or the denial of an application for an order, if the prosecutor certified

Page 7 of 10 sb633/9798

to the judge or other official granting the motion or denying the application that the appeal was not taken for delay. The prosecutor would have to take the appeal within 30 days after the date the order granting the motion was entered or the application was denied, and would have to prosecute it diligently.

The judge who approved or denied an application for interception could punish as contempt a violation of the bill's provisions relating to recording the contents of an interception, and sealing applications and orders.

Reporting Requirements

Within 30 days after the expiration of an interception order, or the extension or denial of an order, the judge would have to report all of the following to the administrative office of the United States courts and to the Department of State Police:

- -- The fact that an order or extension was applied for.
- -- The kind of order or extension applied for.
- -- The fact that the order or extension was granted as applied for, was modified, or was denied.
- -- The interception time period authorized and the number and duration of any extensions.
- -- The offense specified in the order, application, or extension.
- -- The identity of the officer and agency making the application and the authorizing prosecutor.
- The nature of the facilities from which or the place where communications were to be intercepted.

In January of each year, the Attorney General would have to report to the administrative office of the United States courts all of the following regarding applications, orders, and interceptions:

- -- The information described above with respect to each approved application for an order or extension made during the preceding year.
- -- A general description of the interceptions made, including approximations of: the nature and frequency of incriminating communications intercepted; the nature and frequency of other intercepted communications; the number of persons whose communications were intercepted; and the nature, amount, and cost of the

- manpower and other resources used in the interceptions.
- -- The number of arrests resulting from interceptions, the offenses for which arrests were made, and the number of trials resulting from interceptions.
- -- The number of motions to suppress made with respect to the interceptions and number granted or denied.
- -- The number of convictions resulting from the interceptions, the offenses for which the convictions were obtained, and a general assessment of the importance of the interceptions.

All of the preceding information regarding applications, orders, and interceptions would have to be reported to the Attorney General, the State Senate, the House of Representatives, and the Governor on or before January 10 of each year by the Department of State Police.

Law Enforcement Training/Standards

The Director of the Department of State Police would be required to establish: a course of training in the legal and technical aspects of intercepting wire, oral, or electronic communications; regulations for the training program; and minimum standards for certification and recertification of State investigative officers or officers of a law enforcement agency who were eligible to intercept wire, oral, or electronic communications under the bill. The Director would have to charge each officer who enrolled in the training program a reasonable enrollment fee to offset the costs of training.

Communication Service Provider Reporting

An officer, employee, or agent of a service provider who, in the course of employment or otherwise, learned of the existence of an interception device, would be required to report that fact to the prosecuting attorney of the county where the device was located. If the prosecutor determined that the placement of the device was not authorized by court order, he or she immediately would have to inform the person whose communication was intercepted of the device.

The bill specifies that these provisions would not diminish or excuse any obligation of the prosecuting attorney, the officer, employee, or agent of the provider, or any other person to remove the device or to take any other action required by law, regulation, or policy.

Page 8 of 10 sb633/9798

Civil Actions

Except as provided below, a person whose communication was intercepted, disclosed, or used in violation of the bill would have a civil cause of action against any person who intercepted, disclosed, used, or procured another to intercept, disclose, or use the communication or its contents. The person would be entitled to recover all of the following:

- -- Actual damages, but not less than \$1,000 a day for each day of a violation.
- -- Exemplary damages.
- -- Reasonable attorney fees and other reasonable litigation costs.

A good faith reliance on a court order or legislative authorization would be a defense to any civil or criminal action brought under the bill or any law.

Repeal

The bill would repeal provisions of the Michigan Penal Code (MCL 750.539a-750.539i) that do the following:

- -- Make it a misdemeanor to trespass on property of another to subject that person to eavesdropping or surveillance.
- -- Make it a misdemeanor to use any device willfully to eavesdrop.
- -- Make it a felony to install in any private place, without the consent of the person(s) entitled to privacy there, any device for observing, photographing, or eavesdropping upon the sounds or events in that place, or to use any such unauthorized installation.
- -- Make it a felony to use or divulge any information the person knows or reasonably should know was obtained in violation of the preceding prohibitions.
- -- Make it a felony to manufacture, possess, or transfer to another any device designed or commonly used for eavesdropping, knowing that it is to be so used.
- -- Create exceptions for peace officers, communication common carriers, and public utilities.
- Provide civil remedies to parties to a conversation upon which eavesdropping is practiced contrary to the Act.

Legislative Analyst: P. Affholter

require the Department of State Police to develop a wiretapping and electronic surveillance course for local law enforcement agencies and provide certification and periodic recertification of law enforcement personnel in the State who would request it. The expense to State and local law enforcement would depend to a great extent on the interest of the law enforcement community to engage in the activities authorized under the bill. The cost to a law enforcement agency to wiretap a phone involves equipment costs, phone company charges, and personnel costs. The equipment required to tap a phone could cost \$15,000, depending upon the choice of electronic hardware made by a law enforcement agency. To set up a tap, the phone company must be employed to set up a second phone line to an existing line. This involves a charge from the phone company, which is \$600 per tap for such assistance in the Chicago area. Personnel costs can amount to the single largest cost component of a phone tap, depending on the length and complexity of a tap operation. This involves live monitoring of a phone line as well as the handling and administrative requirements of dealing with a piece of legal evidence.

State Police/Law Enforcement: The bill would

Training, certification, and reporting duties assigned to the Department under the bill could require additional administrative, equipment, and supply costs for the Department, depending upon to what extent the Department would wish to use existing personnel who currently engage in similar duties. Investigative personnel would have to be trained in wiretapping and electronic surveillance in order to qualify to instruct other law enforcement personnel in the State as required under the bill.

Training costs for local law enforcement under the bill are not known, but it is possible that training sessions could cost up to \$1,000 per week, with registration funds being used to offset departmental training costs.

FISCAL IMPACT

Page 9 of 10 sb633/9798

The Department also would incur additional cost to the extent that the Department itself would take part in electronic surveillance activities. It is not known whether the Department would choose to use existing personnel within its criminal investigation division to perform these activities or whether the administration would request from the Legislature additional funds to establish a new specialty unit for this purpose.

Corrections: The repeal of certain sections of the Penal Code with a maximum penalty of two years and the addition of new penalties with a maximum term of four years in prison could result in increased costs for sanctioning violators. Also, the new penalties in the bill for disclosing the contents of a wrongfully intercepted communication, and for manufacturing, possessing or selling an interception device, could increase costs for prosecuting and sanctioning violators. Although insufficient data are available at this time to estimate the potential number of annual violators and the length of sentence imposed, the average cost per prisoner of confinement is approximately \$15,000 per year.

In addition, to the extent that the bill resulted in increased convictions, State and local criminal justice costs would increase. In 1995, there were over 8,100 convictions for a drug-related offense, nearly 1,800 (22%) receiving a prison sentence, with an average minimum sentence of 2.2 years. For example, an increase in annual convictions of 10 offenders, each receiving a two-year sentence, would cost an additional \$300,000 annually.

Fiscal Analyst: B. Baker K. Firestone B. Bowerman M. Hansen official statement of legislative intent.

S9798\S633SB

This analysis was prepared by nonpartisan Senate staff for use by the Senate in its deliberations and does not constitute an

Page 10 of 10 sb633/9798