House
Legislative
Analysis
Section

House Office Building, 9 South
Lansing, Michigan 48909
Phone: 517/373-6466

WIRETAPPING AUTHORIZATION

Senate Bill 803 (Substitute H-1)
Senate Bill 806 as passed by the Senate

Sponsor: Sen. William Van Regenmorter
House Committee: Criminal Justice
Senate Committee: Judiciary

First Analysis (3-5-02)

THE APPARENT PROBLEM:

Wiretapping – recording telephone calls and other electronic communications – has long been used by federal law enforcement officers in efforts to stem organized crime and the illicit drug trade. Federal law permits federal agents to obtain wiretapping authorization (18 U.S.C. 2510 et seq.), and Michigan law enforcement agencies may work in conjunction with the FBI on occasion as well as use federal evidence in state court. However, these cases generally involve interstate or international operations: for a crime or operation affecting only this state and its residents, no mechanism exists for state or local law enforcement agencies to obtain judicial authorization to conduct wiretaps.

Wiretaps are seen by many to be an effective investigative tool in gathering evidence to combat the illegal drug trade – especially with regard to evidence that can be used to successfully prosecute suppliers and distributors, the so-called "kingpins". Additionally, after the September 11th attack on the Pentagon and the World Trade Center, many also believe that wiretaps could expose other terrorist plots while still in the planning stages, perhaps preventing destruction of buildings or infrastructure and saving lives.

Further, wiretapping could prove useful in discovering members of crime rings involving child pornography and molestation, whose members often use computers and the Internet to communicate with each other (even to the extent of transmitting real-time videos of sexual molestations of young children in progress). According to a recent Lansing *State Journal* article (2-7-02), a Michigan State Police detective said he was "confident wiretapping would have helped secure cases and convictions against as many as 30 suspects" in a 1997 child sexual abuse ring in Ypsilanti whose members communicated by telephone. Instead, charges and convictions could only be brought against 10 of the members.

Though federal law authorizes state prosecutors to apply to state judges for wiretapping orders, that authorization is contingent upon a state's passing legislation that provides for such an application and requires specific procedures to be adhered to for approval. Michigan is one of only six states that does not authorize wiretapping independently of the FBI. For roughly 15 years, legislative attempts to allow wiretaps in the state have failed. However, in light of the growing sophistication of criminals to disguise illegal activities, and the harm and destruction that acts of terrorism could wreak, many people believe that the time has come for Michigan to authorize judicially-reviewed wiretaps for state and local law enforcement officials.

THE CONTENT OF THE BILLS:

Senate Bill 803 would create the "Criminal Communications Intercept Act" to permit the interception of wire, oral, or electronic communication pursuant to attorney general approval and judicial authorization in the investigation of certain crimes, including: specific drug-related offenses; using a computer or the Internet to commit certain crimes; certain explosives violations; violations of the "Michigan Anti-Terrorist Act" (proposed by Senate Bill 930); assault with intent to murder; attempted murder; solicitation to commit murder; first- or second-degree murder; kidnapping; kidnapping a child under 14; or a poisoning offense that resulted in serious impairment or death (as proposed by House Bill 5507). The bill also would:

- Require the state supreme court to appoint at least five circuit court judges in each court of appeals district who could authorize communication intercept applications.

- Provide that, before a prosecuting attorney authorized an application for a communications

intercept, the attorney general's office would have to approve or deny the authorization within seven days.

• Permit the interception of communication only if other investigative techniques had failed or reasonably appeared to be unlikely to succeed, if tried, or reasonably appeared to be dangerous.

• Allow entry of the premises covered by an interception order to install, maintain, or remove an interception device.

• 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 a wrongfully intercepted communication.

• Prohibit the manufacture, possession or sale (except by providers of an electronic communication service and governmental officials and employees) or 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 communication.

• Require the development of a communication interception training program for law enforcement officers.

• Establish various reporting requirements.

• 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.

• Require the director of the Department of State Police and county sheriffs to maintain custody of interception devices used by state and local law enforcement, respectively, during periods when the devices were not used under court order.

• Specify penalties for violations of the proposed act.

• During periods when intercept equipment is not being used, require the director of the Department of State Police or his or her designee to maintain custody and keep a custody log detailing who had access to the equipment, the purpose of the access, and if the access was pursuant to a court order (with the name of the issuing judge).

• The bill would take effect July 1, 2002.

• Senate Bill 806. The bill would amend the Code of Criminal Procedure (MCL 777.17) to specify that each of the following offenses would be a Class F felony against the public trust with a maximum sentence of imprisonment of four years:

• Unauthorized interception, disclosure, or use of wire, oral, or electronic communication.

• Unauthorized manufacture, possession, sale, delivery, or advertisement of communication interception device.

• Unauthorized disclosure of communication interception.

• The bill is tie-barred to Senate Bill 803.

HOUSE COMMITTEE ACTION:

The committee adopted a substitute for Senate Bill 803 that primarily clarified ambiguous language and made several technical corrections. In addition, the committee substitute did the following:

• Deleted a provision in the Senate-passed version that would have allowed the county sheriff or his or her designee to maintain custody of all interception devices for use by local law enforcement officer in that county during periods in which the equipment was not being used.

• In the information required for the attorney general to annually report to the administrative office of the U.S. courts, included the number of orders in which encryption had been encountered and whether that encryption prevented law enforcement from obtaining the plain text of the intercepted communications.

• Provided that if an intercepted communication is in a code or a foreign language, and an expert in that language or code is not reasonably available during the interception period, minimization (efforts to

minimize interception of communication not otherwise subject to legal interception) could be accomplished as soon as practicable after the interception.

• Clarified that pen registers and trap and trace devices are devices or processes that do not identify the contents of a communication.

• Added an effective date.

BACKGROUND INFORMATION:

There have been numerous attempts in the past 15 years to authorize wiretapping by state and local law enforcement officials. Previous bills, such as Senate Bill 986 of the 1995-1996 legislative session (which passed the Senate), focused on wiretapping as a tool to combat the illicit drug trade.

According to the Center for Democracy and Technology and the Administrative Office of the United States (as printed in the *Lansing State Journal*, 2-7-02), 75 percent of wiretaps are for drug-related crimes; 23 percent of intercepted conversations are deemed "incriminating"; on average, 1,769 conversations are intercepted per wiretap; 1,190 wiretaps were approved by federal and state authorities in 2000 (0 requests were denied); 8 wiretaps were conducted in Michigan in 2000; and the average cost of a wiretap is $54,829.

Federal law allows law enforcement officials to tap into a telephone or other electronic communication device when there is "probable cause" to believe that criminal activity is going on and a court approves the wiretap. According to the National Conference of State Legislatures, "wiretaps ordered by federal and state authorities on cellular telephones, pagers, fax machines and e-mail increased by nearly 20 percent two years ago." In addition, the U.S.A. Patriot Act, enacted by Congress after the September 11th attacks, broadened the wiretap laws to include terrorism, specified chemical weapons, and computer fraud and abuse in the list of offenses for which a federal wiretap can be obtained. The U.S.A. Patriot Act also granted roving surveillance authority (which allows investigators to, in effect, "tap" a person instead of a particular phone or computer used by that person), permitted seizure of voice-mail messages under a warrant, and allowed disclosure of communications that include foreign intelligence or counterintelligence.

FISCAL IMPLICATIONS:

According to the House Fiscal Agency, to the extent that the bills increased the numbers of criminal convictions for serious felonies, they would increase state correctional costs.

Further, the agency reports that the requirement in Senate Bill 803 to require the director of the Department of State Police and the attorney general to establish a course of training and minimum certification standards for the procedures governed by the bill would result in indeterminate costs for both agencies. Costs for the two agencies could also increase as a result of various oversight responsibilities assigned by the bill. Finally, the Department of State Police and local law enforcement agencies could incur additional operations costs to the extent that they engaged in the activities governed by the bill. (2-26-02)

ARGUMENTS:

For:

Enactment of the bill is crucial if Michigan is to effectively combat the operations of large, intrastate drug dealers and their suppliers and halt the trafficking of illegal drugs within the state. In addition, Senate Bill 803 would allow wiretaps to be obtained in investigations of terrorist activities; using a computer for certain sex-related crimes involving children; certain other computer crimes (including threatening a person via computer); certain crimes involving explosives, toxic chemicals, radioactive materials, and biological weapons; poisoning food, water supplies, or pharmaceuticals; kidnapping; first- and second degree murder; assault with intent to commit murder; and attempted murder by poisoning, strangulation, or drowning.

Far from encompassing every conceivable crime, the above listed crimes are those associated with acts of terrorism, serial murderers, child sexual molestation or pornography rings, organized crime, serious computer-related crimes, and crimes involving the use of materials that could endanger a large number of people at once. These crimes are often committed by individuals or organizations that are adept at evading capture or hiding evidence that would link them to a specific crime. For some crimes, wiretapping may be the only effective technique to locate an individual already indicted for a crime or to gather evidence that would support a conviction. Reportedly, prosecutors were able only to convict a third of the identified suspects in a child sexual abuse

ring operating in Ypsilanti in 1997. Had this bill been in place then, law enforcement officials may have been able to collect sufficient evidence to prosecute the remaining members of the ring.

To obtain permission to wiretap an individual suspected of criminal activity involving any of the above offenses, law enforcement officials would have to run a gauntlet of civil protections before an application for a wiretap could be approved. Law enforcement officials would have to:

- meet a long list of requirements (including demonstrating probable cause and that other investigative procedures had been tried and failed or would be too dangerous to undertake);

- check with the Department of State Police to verify that a wiretap would not interfere with or overlap any other legal wiretap currently being or about to be conducted;

- obtain the approval of the attorney general;

- if not a state police initiative, obtain approval of the county prosecutor;

- obtain approval by a judge of competent jurisdiction (the state supreme court would have to designate at least five circuit court judges in each court of appeals judicial district; these judges could require additional information to support probable cause); and

- observe a time limit of 30 days per wiretap approval with up to two thirty-day extensions for a total time limit of no more than 90 days per authorized wiretap.

- In addition, the bill would :

- require peace officers to complete a training course and certification before conducting a wiretap operation;

- require the subject of a wiretap to be notified after the wiretap is terminated that communications had or had not been intercepted along with notice of the order;

- allow the subject of a wiretap to inspect the portions of intercepted communications that apply to him or her;

- prohibit the contents of an intercepted communication from being received into evidence until each party was furnished with a copy of the application and authorization order;

- establish grounds for which an aggrieved person could move to suppress the contents of an intercepted communication;

- allow a civil cause of action to be brought against a person who conducted an illegal wiretap or illegally disclosed the contents of an intercepted communication; and,

- require weekly reports by officers conducting a wiretap to the authorizing judge; reports by an authorizing judge to the administrative office of the United States courts within 30 days of the expiration of each order or extension of an order or denial of an order; annual reports by the attorney general to the administrative office of the United States courts; and annual reports by the Department of State Police to the attorney general, governor, and legislature**.**

Response:

Recent changes to federal law under the U.S.A. Patriot Act now allow the FBI to conduct roving wiretaps. This makes sense, as many criminals use evasive measures such as changing cell phones weekly, using many different public phones to place calls, and so forth, to avoid interception of their communications by wiretaps. A roving wiretap, by comparison, allows law enforcement officials to target a specific person and so would allow interception of communications from any wire or electronic devices that the person uses. In order to increase the effectiveness of wiretapping as an investigative tool, thereby increasing convictions for upper level drug dealers and suppliers, child porn ring members, computer terrorists, and political terrorists, Michigan law enforcement officials should also be allowed to conduct roving wiretaps.

Against:

Wiretapping, and especially for such a broad number of offenses, opens up the potential for many abuses of civil liberties, especially "capturing" the communications and conversations of innocent people. This could result in more than just an annoying or embarrassing invasion of privacy. Though it would be nice to believe that prosecutors would not try to charge those who are not involved in the commission of a crime, there is much anecdotal evidence of overzealous law enforcement officers and prosecutors who try to make a chosen person fit the facts of a crime. Further, juries can easily be swayed or intimidated by prosecutors who know how to package and sell an interpretation of evidence, especially so-called evidence gleaned by very

technical devices. Statistics show that almost three-quarters of intercepted communications do not involve evidence of criminal activities. Until wiretapping devices can eliminate the inadvertent capture of conversations of nearby people or ensure that the innocent will not be unduly harassed or unfairly charged with criminal offenses, the state should continue to rely on federally authorized wiretaps (which also can be problematic, but are already legal).

Response:

Senate Bill 803 contains many protections that previous legislative attempts have not included. It is true that wiretaps, especially those meant to intercept cellular communications, can pick up communications other than from the subject of the wiretap. It is also true that the majority of intercepted communications do not include any criminal content. However, the bill does require law enforcement officers operating the taps to minimize the "capture" of irrelevant communications. The bill would also make it a felony for anyone, including peace officers and prosecutors, to violate the provisions of the bill or to unlawfully disclose protected information. Most importantly, although only about one quarter of the intercepted communications contain information relating to criminal activities, it is reported that this information results in the successful prosecution of about 80 percent of the wiretap suspects.

Against:

Wiretaps are very expensive to conduct. Startup costs to buy equipment and train staff have been estimated at about $1 million, and each wiretap operation costs on average over $54,000. Considering the effects of the recent recession on state and local budgets, a concern must be raised over whether funds to pay for wiretap equipment and operations will further reduce funding for other essential public services. Given the high level of anxiety caused by the September terrorist attacks, it is conceivable that a rush to implement the wiretap provisions so to give the illusion of "protecting the public" from dangerous people could further strain already reduced budgets for many necessary programs and projects.

Response:

If anything, the high cost to begin to implement the bill's provisions should reassure those concerned about large scale invasions of private citizens' privacy rights. Yes, wiretaps are not cheap. The cost, added to the laundry list of hoops and hurdles of criteria that must be met to operate a wiretap legally, should ensure that only those operations deserving this type of investigation and evidence gathering would be considered or approved. It should not be forgotten that wiretaps are not, and most likely would not, be used for garden-variety crimes – even those on the approved list of offenses. Not every murder investigation warrants the expense of a wiretap. However, law enforcement officials know of groups of criminals operating over the Internet and through faxes and e-mails who engage in widespread kidnapping, sexual molestation, and murder of young children. These groups are very sophisticated, as are terrorist organizations, organized crime members, drug traffickers, and serial offenders, and operate "under the radar screen" of typical law enforcement investigative tools. Law enforcement officials must be allowed to use the latest in technology to thwart such heinous criminals and bring them to justice.

Against:

Under the governmental immunity statute, innocent people, or those who were the subject of an illegal wiretap or an unlawful disclosure of intercepted communication, would not be able to bring a civil action against the authorities operating the wiretap.

Response:

Actually, Senate Bill 803 does establish a cause of action for any individual whose wire, oral, or electronic communication was intercepted, disclosed, or used in violation of the bill. The bill specifies that this action can be brought against any "person" who violated the bill's provisions. "Person" is defined in the bill as including an employee or agent of the state or of a county, township, city, or village. Generally, a suit is filed against the employer, rather than the employee, under prevailing law. Therefore, the specific language contained in the bill authorizing a civil suit to be brought against a governmental entity would override the more general language contained in the governmental immunity act.

Against:

When wiretap equipment was not in use, the bill would allow the Michigan State Police to retain custody of the equipment or allow the director to designate someone else. This means that the director could allow equipment not in use to be kept locally by a city police department or county sheriff. Though the bill would require the custodial agency to keep a custody log, it could be argued that local custody of unused equipment could be a temptation for abuse. There have been accounts of evidence missing from secured evidence storage rooms, including drugs, money, and even weapons. Weapons listed as having been destroyed have even been used to commit new crimes. As a precaution, it would be preferable to have the state police be in

charge of equipment when not in use, even if it is owned by a local agency.

POSITIONS:

The Office of the Attorney General supports the bills. (2-26-02)

The Prosecuting Attorneys Association of Michigan supports the bills. (2-26-02)

The Department of State Police supports the bill. (2-26-02)

The American Civil Liberties Union (ACLU) opposes the bills. (2-26-02)

The Criminal Defense Attorneys of Michigan oppose the bills. (2-26-02)

Analyst: S. Stutzky

■This analysis was prepared by nonpartisan House staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.