SENATE COMMITTEE ON PUBLIC SAFETY

Senator Nancy Skinner, Chair
2019 - 2020 Regular

Bill No:	SB 439	**Hearing Date:**	April 2, 2019
Author:	Umberg		
Version:	February 21, 2019		
Urgency:	No	**Fiscal:**	No
Consultant:	MK		

Subject: ***Criminal Procedure: Wiretapping: Authorization and Disclosure***

HISTORY

Source: Los Angeles County District Attorney's Office

Prior Legislation: AB 1948 (Jones-Sawyer) Chapter 294, Stats. 2018
SB 955 (Mitchell) Chapter 712, Stats. 2014
SB 61 (Pavley) – Ch. 663, Stats. 2011
SB 1428 (Pavley) – Ch. 707 Stats. 2010
AB 569 (Portantino) – Ch. 307, Stats. 2007
AB 74 (Washington) – Ch. 605, Stats. 2002
Proposition 21 – approved March 7, 2000
SB 1016 (Boatwright) – Ch. 971, Stats. 1995
SB 800 (Presley) – Ch. 548, Stats. 1993
SB 1120 (Presley) – 1991
SB 83 – amended out in part and chaptered in part as SB 1499 (1988)
SB 1499 – Ch. 111, Stats. 1988

Support: Unknown

Opposition: None known

PURPOSE

The purpose of this bill is to: allow overheard communications to be disclosed if they involve a serious felony; and, to allow overheard communications involving any crime by a peace officer to be used in administrative or disciplinary hearings.

Existing law authorizes the Attorney General, chief deputy attorney general, chief assistant attorney general, district attorney or the district attorney's designee to apply to the presiding judge of the superior court for an order authorizing the interception of wire or electronic communications under specified circumstances. (Penal Code §§ 629.50 *et. seq*.)

Existing law specifies the crimes for which an interception order may be sought: murder, kidnapping, bombing, criminal gangs, and possession for sale, sale, transportation, or manufacturing of more than three pounds of cocaine, heroin, PCP, methamphetamine or its precursors, fentanyl, possession of a destructive device, weapons of mass destruction, restricted biological agents or human trafficking. (Penal Code § 629.52.)

Existing law provides that the court may grant oral approval for an emergency interception of wire, electronic pager or electronic cellular telephone communications without an order as specified. Approval for an oral interception shall be conditioned upon filing with the court, within 48 hours of the oral approval, a written application for an order. Approval of the ex parte order shall be conditioned upon filing with the judge within 48 hours of the oral approval. (Penal Code § 629.56.)

Existing law provides that no order entered under this chapter shall authorize the interception of any wire, electronic pager or electronic cellular telephone or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days. (Penal Code §629.58.)

Existing law requires that written reports showing what progress has been made toward the achievement of the authorized objective, including the number of intercepted communications, be submitted at least every 10 days to the judge who issued the order allowing the interception. (Penal Code § 629.60.)

Existing law requires the Attorney General to prepare and submit an annual report to the Legislature, the Judicial Council and the Director of the Administrative Office of the United States Court on interceptions conducted under the authority of the wiretap provisions and specifies what the report shall include. (Penal Code § 629.62.)

Existing law provides that applications made and orders granted shall be sealed by the judge. Custody of the applications and orders shall be where the judge orders. The applications and orders shall be disclosed only upon a showing of good cause before a judge and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for 10 years. (Penal Code § 629.66.)

Existing law provides that a defendant shall be notified that he or she was identified as the result of an interception prior to the entry of a plea of guilty or *nolo contendere*, or at least 10 days, prior to any trial, hearing or proceedings in the case other than an arraignment or grand jury proceeding. Within 10 days prior to trial, hearing or proceeding the prosecution shall provide to the defendant a copy of all recorded interceptions from which evidence against the defendant was derived, including a copy of the court order, accompanying application and monitory logs. (Penal Code § 629.70.)

Existing law provides that any person may move to suppress intercepted communications on the basis that the contents or evidence were obtained in violation of the Fourth Amendment to the United States Constitution or of California electronic surveillance provisions. (Penal Code § 629.72.)

Existing law provides that the Attorney General, any deputy attorney general, district attorney or deputy district attorney or any peace officer who, by any means authorized by this chapter has obtained knowledge of the contents of any wire, electronic pager, or electronic communication or evidence derived therefrom, may disclose the contents to one of the individuals referred to in this section and to any investigative or law enforcement officer as defined in subdivision (7) of Section 2510 of Title 18 of the United State Code to the extent that the disclosure is permitted pursuant to Section 629.82 and is appropriate to the proper performance of the official duties of the individual making or receiving the disclosure. No other disclosure, except to a grand jury, of

intercepted information is permitted prior to a public court hearing by any person regardless of how the person may have come into possession thereof. (Penal Code § 629.74.)

Existing law provides that if a law enforcement officer overhears a communication relating to a crime that is not specified in the wiretap order, but is a crime for which a wiretap order could have been issued, the officer may only disclose the information and thereafter use the evidence, if, as soon as practical, he or she applies to the court for permission to use the information. If an officer overhears a communication relating to a crime that is not specified in the order, and not one for which a wiretap order could have been issued or any violent felony, the information may not be disclosed or used except to prevent the commission of a crime. No evidence derived from the wiretap can be used unless the officers can establish that the evidence was obtained through an independent source or inevitably would have been discovered. In all instances, the court may only authorize use of the information if it reviews the procedures used and determines that the interception was in accordance with state wiretap laws. (Penal Code § 629.82 (b).)

This bill would also allow a law enforcement officer to disclose the contents of an overheard communication if the information relates to a serious felony.

This bill would allow the contents of an overheard communication to be used if the contents relate to any crime involving a peace officer in an administrative or disciplinary hearing involving the employment of the peace officer.

COMMENTS

1. Need for This Bill

According to the author:

> Penal Code section 629.52(a) enumerates the offenses for which a wiretap may be authorized. This list includes certain narcotic offenses, murder, aggravated kidnapping, human trafficking, any felony violation of Penal Code section 186.22, and attempts or conspiracies to commit these enumerated offenses.
>
> Penal Code section 629.82 sets forth the procedure which is to be followed in the event that communications related to crimes that are not specified in the order of authorization are intercepted. For example, a call regarding an unrelated murder may be intercepted on a wiretap which was authorized to investigate the transportation of cocaine.
>
> If the intercepted wire or electronic communication relates to a crime that is not specified in the order of authorization but is related to a crime which is enumerated in Penal Code section 629.52(a) or is a violent felony as defined in Penal Code section 667.5(c), the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in Penal Code sections 629.74 and 629.76, and the contents and any evidence derived therefrom may be used under Section 629.78 when authorized by a judge if the judge finds, upon subsequent application, that the contents were otherwise intercepted in accordance with the provisions of this chapter. The application shall be made as soon as practicable. (Pen Code, § 629.82(a).)

Per Penal Code section 629.74, no other disclosure, except to a grand jury, of intercepted information is permitted prior to a public court hearing by any person regardless of how the person may have come into possession thereof.

However, if the intercepted communication is related to a crime that is neither enumerated in Penal Code section 629.52(a) nor is a violent felony, the contents thereof, and evidence derived therefrom, may **not** be disclosed or used as provided in Sections 629.74 and 629.76, except to prevent the commission of a public offense. The contents and any evidence derived therefrom may not be used during a criminal court proceeding or in a grand jury proceeding, except where the evidence was obtained through an independent source or inevitably would have been discovered, and the use is authorized by a judge who finds that the contents were intercepted in accordance with this chapter. (Pen Code, § 629.82(b).)

Wiretaps are subjected to a great deal of judicial and executive scrutiny. They are authorized only if a designated judge determines probable cause exists and other traditional investigative techniques have been tried and failed or are too dangerous to attempt. Before a wiretap may be submitted to the judge, the Attorney General or the District Attorney of a county as well as the chief executive officer of the investigating law enforcement agency must approve the application. Wiretaps are viewed as the investigative tool of last resort.

By placing limits on the types of crimes that could be solved and/or prosecuted if a conversation is intercepted pursuant to an otherwise lawful wiretap order, Penal Code section 629.82(b) severely curtails the potential efficacy of intercepted wire and electronic communications. An intercept related to a robbery, which is a violent felony, could be disclosed and used, but not an attempted robbery, which is neither an enumerated crime nor a violent felony. The same limitation would apply to residential burglary, unless a person was present per Penal Code section 667.5(c)(21).

Existing law also limits the use of intercepted communications involving law enforcement misconduct. California law only allows the use of intercepted communications in limited circumstances in criminal proceedings and grand jury proceedings. They may not be used in administrative hearings. Section 629.82(b)'s limitations were illustrated when Carlos Arrellano, a Los Angeles County narcotics detective, was intercepted discussing an illegal marijuana grow operation with the target of a narcotics wiretap investigation. The Los Angeles County Sheriff's Department Internal Criminal Investigations Bureau and the Drug Enforcement Administration conducted an investigation but charges could not be filed because marijuana is not listed in Penal Code section 629.52(a)(1) and use of the calls was therefore precluded by Penal Code section 629.82. Arrellano was discharged from his position as a deputy sheriff on August 29, 2011, but was reinstated because criminal charges could not be filed and the intercepted calls were not admissible at the administrative hearing. (*County of Los Angeles v. Los Angeles County Civil Service Commission [Carlos Arrellano]* (2018) B278519 (Los Angeles County Super. Ct. No. BS156018).)

During a 2018 wiretap investigation, a call was intercepted between a Target Subject and the Target Subject's neighbor. The neighbor was an active law

enforcement officer from a local police agency. The Target Subject asked the officer to "run" the license plate of a vehicle. The officer complied. Not only is this a violation of Penal Code sections §§ 13300 et seq., but undoubtedly a violation of the officer's departmental policy and procedure manual. The officer's agency may be able to initiate an internal affairs investigation into the officer's conduct, but the intercepted conversation cannot be used in any criminal or administrative proceedings.

2. Federal Wiretapping Law

a) The Fourth Amendment Protects Telephone Communications

The United States Supreme Court ruled in *Katz v. United States* (1967) 389 U.S. 347, 88 S.CT. 507, 19 L.ED.2D 576, that telephone conversations were protected by the Fourth Amendment to the United States Constitution. Intercepting a conversation is a search and seizure similar to the search of a citizen's home. Thus, law enforcement is constitutionally required to obtain a warrant based on probable cause and to give notice and inventory of the search.

b) Title III Allows Wiretapping Under Strict Conditions

In 1968, Congress authorized wiretapping by enacting Title III of the Omnibus Crime Control and Safe Streets Act. (See 18 USC Section 2510 et seq.) Out of concern that telephonic interceptions do not limit the search and seizure to only the party named in the warrant, federal law prohibits electronic surveillance except under carefully defined circumstances. The procedural steps provided in the Act require "strict adherence." (*United States v. Kalustian*, 529 F.2d 585, 588 (9th Cir. 1976)), and "utmost scrutiny must be exercised to determine whether wiretap orders conform to Title III.") Several of the relevant statutory requirements may be summarized as follows:

i. Unlawfully intercepted communications or non-conformity with the order of authorization may result in the suppression of evidence.
ii. Civil and criminal penalties for statutory violations.
iii. Wiretapping is limited to enumerated serious felonies.
iv. Only the highest ranking prosecutor may apply for a wiretap order.
v. Notice and inventory of a wiretap shall be served on specified persons within a reasonable time but not later than 90 days after the expiration of the order or denial of the application.
vi. Judges are required to report each individual interception. Prosecutors are required to report interceptions and statistics to allow public monitoring of government wiretapping.

c) The Necessity Requirement – Have Other Investigative Techniques Been Tried Before Applying to the Court for a Wiretap Order?

3. Wire or Electronic Communication

Under existing law, the Attorney General or a district attorney may make an application to a judge of the superior court for an application authorizing the interception of a wire, electronic pager or electronic cellular telephone. The law regulates the issuance, duration and monitoring of these orders and imposes safeguards to protect the public from unreasonable interceptions. The law also limits which crimes for which an interception may be sought to the following:

a) Importation, possession for sale, transportation or sale of controlled substances;
b) Murder or solicitation of murder or commission of a felony involving a destructive device;
c) A felony in violation of prohibitions on criminal street gangs;
d) Possession or use of a weapon of mass destruction;
e) A violation of human trafficking and,
f) An attempt or conspiracy to commit any of the above.

4. Use of overheard information not relating to crime for which interception was sought

In general when a law enforcement officer overhears information that relates to an offense not related to the information for which the wiretap order was sought it can't be used unless it is one of the offenses for which a wiretap may be authorized or a violent felony as defined by Penal Code section 667.5(c). This limitation is intended to prevent "fishing expeditions" in which law enforcement seeks a wiretap for one of the enumerated offenses when they really suspect the target of another offense.

This bill would allow information relating to a serious felony that is overheard during a wiretap to be used. Thus when listening to a wiretap information overheard relating to the following offenses could be disclosed under this bill that cannot currently be disclosed: assault with a deadly weapon on a peace officer; rape of an unconscious person; exploding a destructive device with the intent to injure or intent to murder; rape of an unconscious person or a person with a mental disorder or disability; furnishing illicit drugs to a mirror; grand theft of a firearm; attempted kidnaping; attempted carjacking; attempted rape; residential burglary (person not present).

Should information overheard during an interception of communications be able to be used when it relates to a serious felony?

5. Use of overheard information when it pertains to peace officer employment

As noted in the author's statement, there have been some incidents where misconduct by peace officers, not amounting to a violent felony or one of the listed offenses, have been overheard during an intercept but the information was not admissible in administrative proceedings against the officers so they were able to keep their jobs. This bill would provide that when any criminal misconduct by a peace officer is overheard in an intercept, that information can be used to discipline the office, even when it is inadmissible for a criminal case.

-- END –