SENATE COMMITTEE ON PUBLIC SAFETY

Senator Aisha Wahab, Chair
2023 - 2024 Regular

Bill No:	AB 1892	**Hearing Date:**	June 25, 2024
Author:	Flora		
Version:	March 19, 2024		
Urgency:	No	**Fiscal:**	No
Consultant:	MK		

Subject: ***Interception of electronic communications***

HISTORY

Source: Sacramento County Sheriff

Prior Legislation: AB 1948 (Jones-Sawyer) Chapter 29. 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: California Association of Highway Patrolmen; California State Sheriffs' Association; Peace Officers Research Association of California (PORAC); 3 individuals

Opposition: Oakland Privacy (oppose unless amended)

Assembly Floor Vote: 69 - 0

PURPOSE

The purpose of this bill is to add specified felony offenses related to obscene materials involving minors to the list of crimes for which law enforcement may obtain an ex parte order for a wiretap.

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 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).)

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, fentanyl or its precursors, possession of a destructive device, weapons of mass destruction, restricted biological agents or human trafficking. (Penal Code § 629.52.)

Existing law makes it a felony to knowingly send or cause to be sent or brings or causes to be brought, into this state for sale or distribution, or possesses, prepares, publishes, etc. any film, disc, computer hardware etc. with the intent to distribute any image containing any obscene matter knowing that it depicts a person under the age of 18 years personally engaging in or personally simulating sexual conduct. (Penal Code § 311.2 (b))

Existing law makes it a felony to knowingly sends or cause to be sent, or brings or causes to be brought, into this state for sale or distribution or in this state possesses, prepares etc. any film, disc, computer image etc. with the intent to distribute or exhibit to a person under the age of 18 any matter that depicts a person under the age 18 years personally engaging in or personally simulating conduct. (Penal Code § (d))

This bill further authorizes a judge, upon receipt of a valid application to issue an ex parte order authorizing interception of wire or electronic communications initially intercepted within the territorial jurisdiction of the judge's court if there is probable cause to believe that an individual is committing, has committed, or is about to commit a felony related to child pornography.

COMMENTS

1. Need for This Bill

According to the author:

> Child pornography offenses are insidious and inflict devastating psychological harms on the victim. Existing law does not allow law enforcement agencies to use wiretapping or interception of electronic communication to combat it. That needs to change. Law enforcement needs to use all available legal means to investigate and prosecute these crimes. These tools will allow faster detection that these

crimes are occurring and identify more guilty offenders. If we can use these warrants to solve drug and gang crimes, we should be just as willing to use them to prevent sexual exploitation of children.

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. Addition of felony child pornography to wiretap provisions

This bill expands wiretap provisions to include felony violations of obscenity involving a minor, including the sale, production, distribution, or exhibition of child pornography; sexual exploitation of a child; employment of a minor in the sale or distribution of child pornography; advertising obscene matters depicting minors; and possession or control of child pornography.

5. Argument in Support

Sacramento Sheriff supports this bill stating:

> The number of crimes against children are unprecedented and growing. Predators prey on our children and gain access to them through their smart devices or computers, often using social media or web-based platforms. In fact, our Internet Crimes Against Children Task Force has seen a dramatic increase in child pornography on the internet and are anticipating with Artificial Intelligence the number of images will only be increasing. The production and proliferation of these images normalizes and validates the sexual exploitation of children in our communities. Studies have shown individuals who are creating and purchasing child pornography grow increasingly aggressive with their sexually motivated thoughts and behaviors greatly increasing the risk of victimization of children. This bill would give law enforcement an additional tool to assist them in catching these predators before they commit these unspeakable acts on our children.

6. Oppose (unless amended)

Oakland Privacy opposes this bill stating:

> While we agree with the author that these offenses are terrible, this bill proposes to significantly expand the ability for law enforcement to intercept communications. Due to the nature of this type of surveillance - which captures communications far beyond the initial target - it is a type of dragnet surveillance that not only poses significant threats to privacy but is incredibly resource intensive and ripe for abuse.
>
> According to the California Association of Highway Patrolmen "investigating such criminal activities can be slow, inefficient, and resource intensive".1 AB 1892 will exacerbate these problems by lowering the threshold required to issue a wiretap, while needlessly violating the privacy of many others who may not be involved in the commission of these crimes. In 2016, 3,168 wiretaps were authorized across the nation. California alone, constituted 35% of all wiretap applications approved by state judges.2 The 569 wiretaps conducted in California in 2016 intercepted 7.8 million communications from 181,000 people, with less than a fifth of these

communications being incriminating, convicting just 27 people for their alleged crimes, and at a cost of almost $30 million.3

Historically, law enforcement has been shown time and time again to have violated search
warrant and other privacy laws. for example, a law enforcement department admitted in court-filed pleadings that it never obtained a warrant to use a cell site simulator (essentially a wiretap) despite a warrant requirement and it has no records of having obtained any other kind of court order authorizing the use. 4 Another agency deceptively obtained a “pen register” court order without disclosing the true nature of the surveillance for which it was sought.5 Last year, the Homeland Security Inspector General reported that many law enforcement agencies often conducted invasive searches without obtaining the appropriate search warrants.6 Loosening the requirements to obtain a wiretap will inevitably lead to an increase in wiretaps along with an increase in costs for resource intensive activities which have historically not yielded a high rate of convictions.

If passed, AB 1892 will facilitate the collection of communications of not only of the intended target, but will scoop up the private communications of many others in communication with the target - despite the fact that those third parties are not suspected of possessing obscene matter of minors under the age of 18 as defined in the CA Penal Code § 311.1. This can include very private communications between a person and their doctor, their employer, family and others.

While wiretaps can be a tool of last resort in addressing violent crimes when there is acute potential for immediate loss of life, we believe their use is appropriately limited. We suggest that additional resources be allocated to other law enforcement tools to address obscenity which are already proving to be more effective, efficient and less invasive of innocent third parties' privacy.

-- END –