SENATE COMMITTEE ON PUBLIC SAFETY

Senator Loni Hancock, Chair
2015 - 2016 Regular

Bill No:	SB 178	**Hearing Date:**	March 24, 2015
Author:	Leno		
Version:	March 16, 2015		
Urgency:	No	**Fiscal:**	Yes
Consultant:	MK		

Subject: Privacy: Electronic Communications: Search Warrants

HISTORY

Source: ***American Civil Liberties Union and California Newspaper Publishers Association***

Prior Legislation: SB 467 (Leno) – Vetoed (2013)
SB 914 (Leno) – Vetoed (2012)
SB 1434 (Leno) – Vetoed (2012)
SB 662 (Figueroa) – Chapter 896, Stats. 1999

Support: Adobe; Apple Inc.; Asian Americans Advancing Justice; California Attorneys for Criminal Justice; The California Chapter of the Council on American-Islamic Relations; California Immigrant Policy Center; California Library Association; California Public Defenders Association; Consumer Action; Consumer Federation of California; Electronic Frontier Foundation; Engine; Facebook; Foursquare; Google; The Internet Archive; Internet Association; LinkedIn; Media Alliance; Mozilla; Namecheap, Inc.; National Center for Lesbian Rights; Open Technology Institute; Privacy Rights Clearinghouse; Restore the Fourth Bay Area Chapter; Small Business California; Twitter; TechFreedom; TURN

Opposition: California District Attorneys Association; California State Sheriffs' Association

PURPOSE

The purpose of this bill is to require a search warrant or wiretap order for access to all aspects of electronic communications except where federal law allows voluntary disclosure.

The US Constitution provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched an the persons or things to be seized." (4th Amendment of the U.S. Constitution.)

The California Constitution provides that "the right of the people to be secure in their persons, houses, papers and effects against unreasonable seizures and searches may not be violated; and a warrant may not issue except on probable cause, supported by oath or affirmation, particularly

describing the place to be searched and the persons and things to be seized." (Article I, Section 13 of the California Constitution.)

Existing law defines a "search warrant" as an order in writing in the name of the People, signed by a magistrate, directed to a peace officer, commanding him or her to search for a person or persons, a thing or things, or personal property, and in the case of a thing or things or personal property, bring the same before the magistrate. (Penal Code § 1523.)

Existing law provides that a search warrant may be issued upon any of the following grounds:

a) When the property was stolen or embezzled;

b) When the property or things were used as the means of committing a felony;

c) When the property or things are in the possession of any person with the intent to use them as a means of committing a public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing them from being discovered;

d) When the property or things to be seized consist of any item or constitute any evidence that tends to show a felony has been committed, or tends to show that a particular person has committed a felony;

e) When the property or things to be seized consist of evidence that tends to show that sexual exploitation of a child, or possession of matter depicting sexual conduct of a person under the age of 18 years, has occurred or is occurring;

f) When there is a warrant to arrest a person;

g) When a provider of electronic communication service or remote computing service has records or evidence, showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery;

h) When the property to be seized includes evidence of a violation of specified Labor Code sections;

i) When the property to be seized includes a firearm or deadly weapon or any other deadly weapon at the scene of a domestic violence offense;

j) When the property to be seized includes a firearm or deadly weapon owned by a person apprehended because of his or her mental condition;

k) When the property to be seized is a firearm in possession of a person prohibited under the family code;

l) When the information to be received from the use of a tracking device under shows a specified violation of the Fish and Game Code or Public Resources Code;

m) When a sample of blood would show evidence of a DUI; or,

n) Starting January 1, 2016, when the property to be seized is a firearm owned by a person subject to a gun violence restraining order. (Penal Code § 1524(a).)

Existing law sets forth procedures for a search warrant issued for records of a foreign corporation that provides electronic communication services or remote computing services to the general public, where those records would reveal the identity of the customers using services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications. (Penal Code § 154.2)

Existing law provides that a provider of electronic communication or remote computing service shall disclose to a governmental prosecuting or investigating agency the name, address, local and long distance toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to a customer of that service and types of services the subscriber or customer utilized when the governmental entity is granted a search warrant. (Penal Code § 1524.3(a))

Existing law provides that a provider of wire or electronic communication services or a remote computing service, upon the request of a peace officer, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a search warrant or a request in writing and an affidavit declaring an intent to file a warrant to the provider. Records shall be retained for a period of 90 days which shall be extended for an additional 90-day upon a renewed request by the peace officer. (Penal Code § 1524.3(d))

Exiting law provides that a search warrant cannot be issued but upon probable cause, supported by affidavit, naming or describing the person to be searched or searched for, and particularly describing the property, thing or things and the place to be searched. (Penal Code § 1525.)

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.)

This bill creates the Electronic Communications Privacy Act.

This bill provides that except as otherwise provided a government entity shall not do any of the following:

- Compel the production of or access to electronic device information from any person or entity except the authorized processor of the device;
- Compel the production of or access to electronic device information from any person or entity except the authorized processor of the device; or,

- Access electronic device information by means of physical interaction or electronic communication with the device, except with the specific consent of the authorized processor of the device.

This bill provides that a government entity may compel the production of or access to electronic communication information or electronic communication with the device information by means of physical interaction with the device only pursuant to a wiretap order or pursuant to a search warrant provided that the warrant shall not compel the production of or authorize access to the contents of any electronic communication initiated after the issuance of the warrant.

This bill provides that a government entity may access electronic device information by means of the physical interaction or electronic communication with the device only as follows:

- In accordance with a wiretap order or search warrant issued pursuant to the appropriate Penal Code provision, provided that a warrant shall not authorize accessing the contents of any electronic communication initiated after the issuance of the warrant;
- With the specific consent of the owner or authorized possessor of the device, when a government entity is the intended recipient of an electronic communication initiated by the owner or authorized possessor of the device;
- With the specific consent of the owner of the device when the device has been reported lost or stolen;
- If the government entity, in good faith, believes that an emergency involving imminent danger of death or serious physical injury to any person requires access to the electronic device information; and,
- If the government entity, in good faith, believes the device to be lost, stolen, or abandoned, provided that the entity shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

This bill provides that the warrant or order shall be limited to only that information necessary to achieve the objective of the warrant or wiretap order, including specifying the target individuals or accounts, the applications or services, the types of information, and the time periods covered.

This bill provides the warrant or order shall identify the effective date upon which the warrant is to be executed, not to exceed 10 days from the date the warrant is signed, or explicitly state whether the warrant or wiretap order encompasses any information created after its issuance.

This bill provides that the warrant or order shall comply with all other provisions of California and federal law, including any provision prohibiting, limiting or imposing additional requirements on the use of search warrants or wiretap orders.

This bill provides that when issuing any warrant or wiretap order the court may do any of the following:

- Appoint a special master to ensure only information necessary to achieve the objective of the warrant or order is produced or accessed; or,
- Require any information obtained through the execution of the warrant or order that is unrelated be destroyed.

This bill provides that a service provider may disclose, but is not required to disclose, electronic communication information or subscriber information when disclosure is not otherwise prohibited by law.

This bill provides that if a government entity receives electronic communication without a warrant or order, it shall delete the information within 90 days unless the entity has or obtains the specific consent or the sender of the sender or recipient about which the information was disclosed or obtains a court order authorizing the retention of the information, and specifies when the court shall order a retention order.

This bill provides that if a government entity requests that a service provider disclose information or if the government entity obtains information involving the danger of death or serious physical injury to a person, that requires access to the electronic information without delay, the entity shall within three days after seeking the disclosure, file with the court a motion seeking approval of the requested emergency disclosures and shall set forth the facts giving rise to the emergency. If the court finds the facts did not give rise to the emergency the court shall order the information destroyed.

This bill provides that it does not limit the authority of a government to use administrative, grand jury, trial or civil discovery subpoena to do either of the following:

- Require an originator, addressee, or intended recipient of an electronic communication to disclose any electronic communication information associated with that communication; or,
- Require an entity that provides electronic communications services to its officers, directors, employees, or agents to disclose electronic communication information associated with an electronic communication to or from an officer, director, employee or agent of the entity.

This bill provides that except as otherwise provided the government entity that executes a warrant or wiretap order or issues and emergency request shall contemporaneously notice the identified targets that the information about the recipient has been compelled or requested and states with reasonable specificity the nature of the government investigation under which the information is sought.

This bill provides that if there is no identified target of the warrant or order or emergency request, the government shall take reasonable steps to provide notice within three days to all individuals about whom information was obtained.

This bill provides that when a wire tap order or search warrant is sought the government entity may submit a request supported by an affidavit for an order delaying notification and prohibiting any party from providing information or notifying any party it is being sought. If the court determines notification may have an adverse impact the court may delay notification for up to 90 days with subsequent extensions for 90 days.

This bill provides that except as proof of a violation of this chapter, no evidence obtained or retained in violation of this chapter shall be admissible in a criminal, civil or administrative proceeding or used in an affidavit in an effort to obtain a search warrant or court order.

This bill provides that the Attorney General may commence a civil action to compel any government entity to comply with the provisions of this bill.

This bill provides that if a warrant or wiretap order does not comply with this chapter, a service provider, or any other recipient of the warrant or wiretap order, or any individual whose information is target by the warrant or wiretap order, may petition the court to void or modify the warrant or order the destruction of any information obtained in violation of the chapter.

This bill requires a government entity that obtains electronic communication information to report annually to the Attorney General specified information regarding any requests that the entity made and requires the Attorney General to publish on their website the information in a report.

This bill defines electronic communication as the transfer of signs, signals, writings, images, sounds, data or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system.

This bill defines electronic communication information as any information about an electronic communication or the use of an electronic communication service, including, but not limited to the contents, sender, recipients, format, or location of the sender or recipients at any point during the communication, the time or date the communication was created, sent or received, or any information pertaining to any individual or device participating in the communication including, but not limited to an IP address but does not include subscriber information.

This bill defines electronic communication service as a service that provides its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications or stores electronic communication information.

This bill defines electronic device as a device that stores, generates, or transmits information in electronic form.

This bill defines other appropriate terms.

RECEIVERSHIP/OVERCROWDING CRISIS AGGRAVATION

For the past eight years, this Committee has scrutinized legislation referred to its jurisdiction for any potential impact on prison overcrowding. Mindful of the United States Supreme Court ruling and federal court orders relating to the state's ability to provide a constitutional level of health care to its inmate population and the related issue of prison overcrowding, this Committee has applied its "ROCA" policy as a content-neutral, provisional measure necessary to ensure that the Legislature does not erode progress in reducing prison overcrowding.

On February 10, 2014, the federal court ordered California to reduce its in-state adult institution population to 137.5% of design capacity by February 28, 2016, as follows:

- 143% of design bed capacity by June 30, 2014;
- 141.5% of design bed capacity by February 28, 2015; and,
- 137.5% of design bed capacity by February 28, 2016.

In its most recent status report to the court (February 2015), the administration reported that as "of February 11, 2015, 112,993 inmates were housed in the State's 34 adult institutions, which amounts to 136.6% of design bed capacity, and 8,828 inmates were housed in out-of-state facilities. This current population is now below the court-ordered reduction to 137.5% of design bed capacity."(Defendants' February 2015 Status Report In Response To February 10, 2014 Order, 2:90-cv-00520 KJM DAD PC, 3-Judge Court, Coleman v. Brown, Plata v. Brown (fn. omitted).

While significant gains have been made in reducing the prison population, the state now must stabilize these advances and demonstrate to the federal court that California has in place the "durable solution" to prison overcrowding "consistently demanded" by the court. (Opinion Re: Order Granting in Part and Denying in Part Defendants' Request For Extension of December 31, 2013 Deadline, NO. 2:90-cv-0520 LKK DAD (PC), 3-Judge Court, Coleman v. Brown, Plata v. Brown (2-10-14). The Committee's consideration of bills that may impact the prison population therefore will be informed by the following questions:

- Whether a proposal erodes a measure which has contributed to reducing the prison population;
- Whether a proposal addresses a major area of public safety or criminal activity for which there is no other reasonable, appropriate remedy;
- Whether a proposal addresses a crime which is directly dangerous to the physical safety of others for which there is no other reasonably appropriate sanction;
- Whether a proposal corrects a constitutional problem or legislative drafting error; and
- Whether a proposal proposes penalties which are proportionate, and cannot be achieved through any other reasonably appropriate remedy.

COMMENTS

1. Need for This Bill

According to the author:

> SB 178 updates California law to properly safeguard the robust constitutional privacy and free speech rights of Californians, spur innovation, and support public safety by instituting clear warrant standards for government access to electronic information.
>
> Californians must use technology every day to connect, work, and learn. The state's leading technology companies rely on consumer confidence in their services to help power California's economy. California law enforcement increasingly utilizes electronic information to protect public safety. The California legislature has long been a leader in enacting laws to properly balance the rights of Californians as technology advances. But California's statutory protections for electronic information is now very outdated.

SB 178 updates existing federal and California statutory law for the digital age and codifies federal and state constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for California law enforcement access to electronic information, including data from personal electronic devices, emails, digital documents, text messages, metadata, and location information. Each of these categories can reveal sensitive information about a Californian's personal life: her friends and associates, her physical and mental health, her religious and political beliefs, and more.[i] The California Supreme Court has long held that this type of information constitutes a "virtual current biography" that merits constitutional protection. SB 178 would codify that protection into statute. SB 178 also ensures that proper notice, reporting, and enforcement provisions are also updated and in place for government access to electronic information and to ensure that the law is followed.

2. Search and Seizure Generally

The 4th Amendment of the US Constitution and Article I, Section 13 of the California Constitution protect people against unreasonable searches and seizures. Generally, the lawfulness of a search of the items in the arrestee's immediate control is based upon the need to protect the officer and to discover evidence in the case. This has been found to include search of items when a person is booked into jail on the theories that the time lag is inconsequential; it is less of an invasion than a public search at the place of arrest; is necessary for inventory purposes; and, can protect from contraband being brought into the jail. However, if the search is remote in time and the property has been removed from the defendant's possession and is in the control of the police, then a warrantless search has been found not to be reasonable. Numerous cases have looked at this issue of when a search incident to arrest is valid. (See for example: *U.S v. Robinson* (1973) 414 U.S. 218; *U.S. V. Edwards* (1974) 415 U.S. 800*; U.S. v. Chadwick* (1977) 433 U.S. 1; *N.Y. v. Belton* (1981) 453 U.S. 454; *People v. Hamilton* (1988) 46 C. 3d 123)) After Proposition 8 (June 1982), in California, the scope of a search incident to arrest is based on federal law; thus, California courts will look to the federal courts for precedent when deciding a case.

3. Wiretap Generally

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.

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.")

Both Federal and California law requires that each wiretap application include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." (18 USC Section 2518 (1)(c); Penal Code Section 629.50(d).) Often referred to as the "necessity requirement," it exists in order to limit the use of wiretaps, which are highly intrusive. (*United States v. Bennett*, 219 F.3d 1117, 1121 (9th Cir. 2000).) The original intent of Congress in enacting such a provision was to ensure that wiretapping was not resorted to in situations where traditional investigative techniques would suffice to expose the crime.

4. Recent Supreme Court Cases

The fact that Fourth Amendment protections extends to electronic information has been recently affirmed by the United States Supreme Court.

In *United States v. Riley*, 134 S. Ct. 2473 (2014) involved two cases. In the first case, the defendant (Riley) was stopped for a traffic violation which lead to his arrest on a misdemeanor firearms charge. In the search incident to his arrest the officer searched his phone and noticed terminology related to gangs. The phone was further searched at the police station and photos and videos on the phone lead to Riley being charged in connection with a shooting and the phone evidence being used to claim a gang enhancement. In the second case, as a result of his cell phone being searched the defendant's apartment was searched and guns and drugs were found after he was arrested during a drug sale. "These cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones." (*Id. at 2484.)* The Supreme Court refused to apply to cell phone searches the precedents established for the searches of purses and wallets because "that would be like saying a ride on horseback is materially indistinguishable from a flight to the moon." (*Id.* at 2488.) Recognizing that modern cell phones' storage capacity and multi-functionality allow them to contain "the privacies of life," the Court required law enforcement to "get a warrant" for cell phone searches. (*Id.* at 2495.)

In the case of *U.S. v. Jones* (132 S.Ct. 945(2012)), the court found that the government's attachment of a GPS device to a vehicle and its use of that device to monitor the vehicle's movements constituted a search warrant under the 4th Amendment. In *Jones*, all members of the Court found that the law enforcement's attachment and subsequent monitoring of a GPS on a vehicle violated the 4th Amendment, although with two concurring opinions, various judges reached that conclusion using different legal reasoning.

In *Jones*, the United States Supreme Court held that attaching a global positioning system (GPS) device to a person's vehicle to track his or her movements constitutes a search within the meaning of the Fourth Amendment. Authorities obtained a search warrant to install a GPS device on defendant's car as part of a drug trafficking investigation. But, the authorities did not install the device until after the warrant expired. The device was used to track the defendant's movements for almost one month. When charges were filed against defendant, he moved to suppress the GPS evidence as the product of an illegal search. The prosecution argued at trial and on appeal that a search within the meaning of the Fourth Amendment had not occurred

because Jones did not have a reasonable expectation of privacy in the location of his vehicle on public streets, which was visible to all.

The Supreme Court found the government's use of a GPS monitoring device was a search within the meaning of the Fourth Amendment, and therefore must be reasonable. The majority decision was not based on the reasonable expectation of privacy test for challenges to law enforcement surveillance, which is generally employed. *(Katz v. U.S.* (1967) 389 U.S. 347.) Instead, the majority based its decision on common law trespass principals, holding that attaching a GPS device to a vehicle (an "effect") for purposes of data collection constitutes a search because the government physically occupied private property for the purpose of information gathering. But five of the justices (the four members of the Alito concurrence, plus Justice Sotomayor) were critical of the trespass theory, stating the majority should have used the reasonable expectation of privacy test.

5. Warrant or Wiretap for Access to Electronic Communication or Device Information

Unless a search warrant or wiretap order is obtained, this bill would prohibit a government entity from: compelling the production of or access to electronic communications from an information service provider; compelling the production of or access to electronic device information from any person or entity except the authorized possessor of the device; or, accessing electronic device information by means of physical interaction or electronic communication with the device except with the specific consent of the authorized user.

Exceptions exist to the warrant requirement including consent of the owner of a device and when the government in good faith believes that an emergency involving imminent danger of death or serious physical injury requires access to the electronic device information or the entity reasonably believes the device is stolen.

If the government agency obtains information without a warrant or order because of an emergency the entity must within three days file a court motion seeking court approval of the requested emergency disclosures.

6. Notice to Consumer

The bill requires notice to the targets of warrant or wiretap contemporaneously with the execution of the warrant unless a court ordered delay of notice is granted for a renewable period up to 90 days.

7. Destruction of Information Obtained Voluntarily

If the government entity obtains electronic information voluntarily, this bill requires that the information be deleted in 90 days, unless the obtainer receives specific consent or obtains a court order to retain the information. The 90 day destruction requirement does not apply to information obtained by a warrant or wiretap.

8. Does not Apply to Internal Communications of a Provider

This bill provides that administrative subpoenas can still be used in an administrative, grand jury or civil discovery situation when it involves internal emails within a company. Thus, for example, in a civil action against an employer who also happens to be a service provider under this bill, emails between the plaintiff and the defendant or other information would be subject to a civil subpoena.

9. DOJ Report

This bill requires government entities that seek information under this bill to report specified information yearly to the Attorney General and requires the Attorney General to publish a report on that information on their website. This is similar to information that must be reported when a jurisdiction uses a wiretap.

10. Support

California Newspaper Publishers Association, a co-sponsor of this bill, states:

> The threat of law enforcement obtaining protected, personal information from third parties without a warrant presents serious problems for newspaper publishers, editors and working journalists. California has unique protections that allow publishers, editors, and working journalists to maintain sensitive source information and unpublished notes without being subject to routine access by law enforcement and litigants.

Twitter supports this bill, stating:

> Current federal law that extends fourth amendment right to electronic communications is nearly 30 years out of date. As technology and the nature of data transmission and storage has changed, the protections afforded by the Federal ECPA law has largely lapsed. Although there is broad support to ECPA reform in Washington, it is unclear if Congress will act in timely fashion to clarify Federal law. This leaves the responsibility of protecting consumer's rights in the hands of private communication service providers.
>
> SB 178 will modernize electronic communications protections and ensure that, in California, an individual's digital property cannot be seized without a warrant. By acting in a timely fashion, SB 178 will set a standard for protecting the rights of users everywhere that can and should be replicated across the country.

Privacy Rights Clearinghouse states in support of this bill:

> SB 178 follows the spirit of *Riley* and extends the warrant requirements to digital information that reveals personal and sensitive details about who we are, whom we communicate and associate with, and where we've been. While law enforcement will still be able to obtain this information and utilize it to solve

crimes, SB 178 provides needed oversight by requiring law enforcement obtain a search warrant in order to access this wealth of information. The bill contains reasonable exceptions that allow law enforcement to obtain digital information without a warrant in an emergency.

11. Opposition

The California District Attorneys Association opposes this bill, stating:

> This bill, the Electronic Communications Privacy Act, would establish a number of new procedures and reporting requirements for law enforcement agencies to comply with when seeking a search warrant for electronic communications. Unfortunately, in doing so, it undermines critical efforts to stop child exploitation, mandates the destruction of evidence by law enforcement, and violates the California Constitution.

The California State Sheriffs' Association opposes this bill, stating:

> This measure has a myriad of problems: it conflates existing procedures for obtaining certain electronic information under state and federal law, contains burdensome and unnecessary reporting requirements, and will undermine investigations that are fully compliant with the Fourth Amendment.

-- END –