# SENATE COMMITTEE ON PUBLIC SAFETY

Senator Loni Hancock, Chair
2011-2012 Regular Session

S
B

1
4
3
4

SB 1434 (Leno)
As Amended April 9, 2012
Hearing date: April 24, 2012
Penal Code
MK:dl

LOCATION INFORMATION:

WARRANTS

HISTORY

Source: American Civil Liberties Union; Electronic Frontier Foundation

Prior Legislation: SB 914 (Leno) - Vetoed, 2011

Support: California Public Defenders Association

Opposition: CTIA-the Wireless Association

(Note: This analysis reflects author's amendments to be offered in Committee. See Comment 7.)

KEY ISSUE

SHOULD THE LAW PROVIDE THAT NO GOVERNMENT ENTITY SHALL OBTAIN THE LOCATION INFORMATION OF AN ELECTRONIC DEVICE WITHOUT A VALID SEARCH WARRANT ISSUED BY A DULY AUTHORIZED MAGISTRATE?

***PURPOSE***

***The purpose of the bill is to provide that no government entity shall obtain the location information of an electronic device without a valid search warrant issued by a duly authorized magistrate.***

(More)

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. (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 tow 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 as subscriber to or 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 of 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.)

This bill provides that no government entity shall obtain the location information of an electronic device without a valid search warrant issued by a duly authorized magistrate.

This bill would provide that no search warrant shall issue for the location of an electronic device pursuant to this section for a period of time longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days, commencing on the day of the initial obtaining of location information, or 10 days after the issuance of the warrant, whichever comes first.

This bill, as proposed to be amended, provides that extensions of a warrant may be granted, but only upon a finding of continuing probable cause by the judge or magistrate, and that the extension is necessary to achieve the objective of the authorization. Each extension granted for a warrant pursuant to this subdivision, shall be for no longer than the authorizing judge or magistrate deems necessary to achieve the purposes for which the warrant was originally granted, but in any event, shall be for no longer than 30 days.

This bill provides that a government entity does not need a warrant to obtain location information in the following circumstances:

- In order to respond to the user's call for emergency services.
- With the informed, affirmative consent of the owner or user of the electronic device concerned, provided however that the owner or user may not consent to the disclosure of location information if the device is known or believed to be in the possession of or attached to a possession of a third party known to the owner or user.
- Pursuant to a request by a government entity that asserts that the governmental entity reasonably believes that an emergency involving immediate danger of death or serious physical injury to the owner or user requires the immediate access to location information and there is insufficient time to obtain a warrant. The government entity seeking the location information pursuant to this paragraph shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency no later than 48 hours after seeking disclosure.

This bill provides that unless the disclosure of information pertaining to a particular request or set of requests is specifically prohibited by law, a provider shall prepare a report which shall be made publicly available on the internet and shall include all of the following information; to the extent it can be reasonably determined:

- The number of federal and state warrants for location information and the number of requests for location information made with the informed consent of the user or emergency requests received by the provider from January 1 to December 31 of the previous year.
- The total number of disclosures made by the provider pursuant to this bill from January 1 to December 31 of the previous year.
- For each category of demand or disclosure, the provider shall include all of the following information:
    - The number of times location information has been disclosed by the provider.
    - The number of times no location information has been disclosed by the provider.
    - The number of times the provider contests the demand.
    - The number of users whose location information was disclosed by the provider.

This bill provides that except as proof of violation of this section, no evidence obtained in violation of this section shall be admissible in a civil or administrative proceeding.

This bill defines electronic communication service as a service that provides to users thereof the ability to send or receive wire or electronic communications.

This bill defines electronic device means a device that enables access to, or use of, an electronic communication service, remote computing service, or location information service.

This bill defines government entity to mean a state or local agency, including, but not limited to, a law enforcement entity or any other investigative entity, agency, department, division, bureau , board, or commission, or an individual acting or purporting to act for or on behalf of a state or local agency.

This bill defines location information as information, concerning the location of an electronic device including both the current location of the device, and any prior location(s) that in whole or in part, is generated, derived from, or obtained by the operation of an electronic device.

This bill defines location information service to mean the provision of a global positioning service or other mapping, locational or directional information service.

This bill defines owner as the person or entity recognized by the law as the legal title, claim, or right to, an electronic device.

This bill defines provider as a commercial entity offering an electronic communication service, remote computing service, or location information service.

This bill defines remote computing service as the provision of computer storage or processing service by means of an electronic communications system.

***RECEIVERSHIP/OVERCROWDING CRISIS AGGRAVATION ("ROCA")***

In response to the unresolved prison capacity crisis, since early 2007 it has been the policy of the chair of the Senate Committee on Public Safety and the Senate President pro Tem to hold legislative proposals which could further aggravate prison overcrowding through new or expanded felony prosecutions. Under the resulting policy known as "ROCA" (which stands for "Receivership/Overcrowding Crisis Aggravation"), the Committee has held measures which create a new felony, expand the scope or penalty of an existing felony, or otherwise increase the application of a felony in a manner which could exacerbate the prison overcrowding crisis by expanding the availability or length of prison terms (such as extending the statute of limitations for felonies or constricting statutory parole standards). In addition, proposed expansions to the classification of felonies enacted last year by AB 109 (the 2011 Public Safety Realignment) which may be punishable in jail and not prison (Penal Code section 1170(h)) would be subject to ROCA because an offender's criminal record could make the offender ineligible for jail and therefore subject to state prison. Under these principles, ROCA has been applied as a content-neutral, provisional measure necessary to ensure that the Legislature does not erode progress towards reducing prison overcrowding by passing legislation which could increase the prison population. ROCA will continue until prison overcrowding is resolved.

For the last several years, severe overcrowding in California's prisons has been the focus of evolving and expensive litigation. On June 30, 2005, in a class action lawsuit filed four years

earlier, the United States District Court for the Northern District of California established a Receivership to take control of the delivery of medical services to all California state prisoners confined by the California Department of Corrections and Rehabilitation ("CDCR"). In December of 2006, plaintiffs in two federal lawsuits against CDCR sought a court-ordered limit on the prison population pursuant to the federal Prison Litigation Reform Act. On January 12, 2010, a three-judge federal panel issued an order requiring California to reduce its inmate population to 137.5 percent of design capacity -- a reduction at that time of roughly 40,000 inmates -- within two years. The court stayed implementation of its ruling pending the state's appeal to the U.S. Supreme Court.

On May 23, 2011, the United States Supreme Court upheld the decision of the three-judge panel in its entirety, giving California two years from the date of its ruling to reduce its prison population to 137.5 percent of design capacity, subject to the right of the state to seek modifications in appropriate circumstances. Design capacity is the number of inmates a prison can house based on one inmate per cell, single-level bunks in dormitories, and no beds in places not designed for housing. Current design capacity in CDCR's 33 institutions is 79,650.

On January 6, 2012, CDCR announced that California had cut prison overcrowding by more than 11,000 inmates over the last six months, a reduction largely accomplished by the passage of Assembly Bill 109. Under the prisoner-reduction order, the inmate population in California's 33 prisons must be no more than the following:

- 167 percent of design capacity by December 27, 2011 (133,016 inmates);
- 155 percent by June 27, 2012;
- 147 percent by December 27, 2012; and
- 137.5 percent by June 27, 2013.

This bill does not aggravate the prison overcrowding crisis described above under ROCA.

COMMENTS

1. Need for This Bill

According to the author:

> SB 1434 updates California privacy law to reflect the modern mobile world of today by providing needed protection against warrantless government access to a person's location information that is generated, derived from, or obtained by the operation of an electronic device.
>
> Most Californians are now carrying tracking devices on their person every day- their mobile phones, tablets, and more. While the location data from these devices can make it easy to get directions or locate the closest coffee shop, that location data also says a lot about them – where they go, what they do, and who they know. Many location-aware technologies can pinpoint and track a person's location in real

time, as well as record data to create a detailed log of a person's whereabouts for months or even years.

State public records act requests have revealed that law enforcement is increasingly taking advantage of outdated privacy laws, written before GPS and other location-aware technologies even existed, to access this sensitive location information without adequate judicial oversight.

Without strong safeguards for location information such as those provided in SB 1434, Californians are left to wonder and worry that if they use mobile technology, their personal information will be left unprotected. By creating clear and robust safeguards for location information, SB 1434 will be good for both consumers and providers of new technology.
In recent months, there has been considerable public outcry over the issue of location data, privacy, and the techniques of government surveillance. The subject has even risen to the level of action by the highest court in the nation. In January of this year, the United States Supreme Court ruled unanimously in *United States v. Jones* that a warrantless installation of a GPS device to track a vehicle's movements constituted a search in violation of the Fourth Amendment.

In *Jones*, the Court recognized that advancements in technology have made it cheap and easy for law enforcement to surreptitiously access and aggregate massive amounts of location information that may unjustifiably intrude on an individual's private life. The decision and its implication with respect to location data is already being felt throughout the court system. In a two sentence order, the Ohio Supreme Court vacated a lower court's opinion that upheld the installation of a GPS device without a warrant, and ordered the court to apply *Jones*. In that case, the Electronic Frontier Foundation and a number of other civil liberties organizations filed an amicus brief urging just such a result.

After issuing its opinion in *Jones,* the Supreme Court in late February issued brief orders reversing two other decisions from federal appellate courts that had previously upheld the warrantless use of GPS tracking devices by law enforcement. One of those decisions was in *United States v. Pineda-Moreno*, where the Ninth Circuit Court of Appeals found law enforcement's installation of a GPS device on a suspect's Jeep while it was parked both on public streets and in his driveway did not violate the Fourth Amendment. In the other case, *United States v. Cuevas-Perez*, law enforcement installed a GPS device on a suspect's Jeep and tracked him through New Mexico, Texas, Oklahoma, Missouri, and Illinois. There, the Seventh Circuit Court of Appeals found the surveillance reasonable under the Fourth Amendment. The facts of these three cases fit squarely with the holding in *Jones*, and it is likely that on taking a second look, all three courts will find the installation of a GPS device without a warrant unconstitutional.

Outside of the judicial realm, location privacy and limitations on law enforcement have begun to be addressed through specific statutes as well. This is consistent with

the *Jones* decision as Justice Alito encouraged this approach by stating that in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. *A legislative body is well suited to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.*

On the congressional level, following revelations about how much location information Apple and Google had been storing about their customers, Sen. Ron Wyden (D-OR) and Rep. Jason Chaffetz (R-UT) introduced legislation, S. 1212, to protect location privacy by requiring law enforcement to get a warrant based on probable cause before accessing location information. The measure regulates the use of this information by businesses and is intended to provide a strong and clear national standard for law enforcement.

Similarly, SB 1434 heeds the call for legislative action to resolve lingering privacy concerns left unaddressed by the *Jones* Court. Under the provisions of SB 1434, no government entity shall obtain the location information of an electronic device without a warrant issued by an officer of the court. SB 1434 also guards against abuses of long-term monitoring by limiting search warrants for location information to a timeframe no longer than is necessary, and not to exceed 30 days.

The warrant requirement implemented under SB 1434 is not overly burdensome and will not deny law enforcement the information that they need to maintain public safety and fight crime. Exceptions are provided in the bill and judicial review simply ensures that authorities have good cause before proceeding. The standard required by SB 1434 is already the law in Oregon where the state's Supreme Court held that tracking is the equivalent of a search as defined by the state constitution and ten other states have pending legislation on this issue.

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. *United States v. Jones*

On January 23, 2012 the U.S. Supreme Court decided the case of *U.S. v. Jones* (132 S.Ct. 945(2012)) and 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, constitutes a search under the Fourth 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 Justices reached that conclusion using different legal reasoning. In *Jones* 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 is 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.

While the Court's decision established that the use of a tracking device qualifies as a search, the opinion left open other questions. First, the Court left open the questions of whether a warrant is required for these types of searches and whether it requires probable cause, as opposed to a lesser standard like reasonable suspicion. The Court also did not answer the question of how it might apply the Fourth Amendment to law enforcement data collection that does not require a physical intrusion, such as where GPS or toll paying devices are installed or used by the owner and the information they produce are mined by law enforcement authorities. Although, the Court did suggest that the expectation of privacy analysis would apply, and four Justices concurred with the majority that this would be the proper analysis.

4. Clarifying the Warrant Requirements in California

Because *Jones* left law enforcement in a position where they cannot use GPS to track a vehicle and left up in the air the issue about other forms of tracking technology, this bill sets forth

warrant requirements so that law enforcement can use this technology when a warrant is obtained. The bill applies to any device that enables access to, or use of, an electronic communication service, remote computing service or location information service so applies to GPS that may be installed in a car, phone or other device as well as one attached to a car.

Specifically, this bill provides that no government entity shall obtain the location information of an electronic device without a valid search warrant issued by a duly authorized magistrate. The bill provides that a warrant shall not issue for a period longer than necessary to achieve the objective but in any event no longer than 30 days, commencing on the day of the initial obtaining of the location information or 10 days after the issuance of the warrant, whichever comes first. This time limitation language is taken from the provisions allowing the intercept of electronic communications with a court order (wiretap laws). (Penal Code § 629.58) The limitation of time discourages a law enforcement entity from going on a fishing expedition. Requiring that the 30 day commence within 10 days also makes sure that the probable cause does not get stale. Similar to the wiretap laws, this bill allows for extensions of the warrant. As proposed to be amended, this bill would allow the extension granted only upon a finding of continuing probable cause by the judge or magistrate, and a finding that the extension is necessary to achieve the objective of the authorization. Each extension shall also be no longer than necessary and in no event longer than 30 days.

The bill explicitly provides that no warrant is needed to obtain location information when there is a call for emergency services, when the owner or user of the device consents or if the government entity reasonably believes that an emergency involving the immediate danger of death or serious injury to the owner requires immediate access to the location information without time to get a warrant. The government entity seeking the information because of immediate danger shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency within 48 hours.

5. Reporting Requirement

This bill would require a provider of the services to prepare a report of all the following to the extent it can be reasonably determined and is not otherwise specifically prohibited by law:

- The number of federal and state warrants for location information and the number of requests for location information made with the informed consent of the user from January 1, to December 31 of the previous year.
- The total number of disclosures the previous year.
- For each category of demand or disclosure:
    - The number of times location information has been disclosed.
    - The number of times no location information has been disclosed.
    - The number of times the provider contests the demand.
    - The number of users whose location information was disclosed.

This bill provides that the reports shall be made publicly available on line and if the provider does not have an Internet Web site, shall be sent to the Office of Privacy Protection.

Commercial Web sites subject to specified privacy requirements in the Government Code shall complete one of the following actions:

- Create a prominent hyperlink to its latest report in the disclosure section of its privacy policy.
- Post the report in the section of its Internet Web site explaining the way in which user information and privacy issues related to its service are addressed.

CTIA-The Wireless Association believes these reporting requirements in the bill would be onerous and costly. Specifically they state:

> These reporting mandates would unduly burden the wireless providers and their employees- who are working day and night to assist law enforcement to ensure the public's safety and to save lives.
>
> It is also unclear what useful purpose such reports would serve. As wireless providers are constantly working to respond to ever-changing consumer demands, it is doubtful that diverting provider resources away from meeting these demands to comply with these reporting mandates would best serve wireless consumers.

What purpose will these reports serve? If the goal is to assure consumer privacy and protection, is there a less onerous way to accomplish this?

6. Related Legislation

AB 2055 (Fuentes) also establishes procedures for search warrants for tracking devices. It passed Assembly Public Safety on April 17, 2012.

7. Amendments to be Taken in Committee

The author will take the following amendments in Committee:

- On Page 3, line 4, after device, insert the following: including both the current location of the device, and any prior location(s)
- On Page 3, line 11, strike the ultimate control over, or having
- On Page 3, line 22, after a, insert a valid search warrant
- On Page 3, lines 25-26, strike No warrant entered under this section shall authorize obtaining location information of an electronic device
- On Page 3, line 25, after (b), insert No search warrant shall issue for the location of an electronic device pursuant to this section
- On Page 3, line 26, after period, insert of time
- On Page 3, line 30, after the period, insert Extensions of a warrant may be granted, but only upon a finding of continuing probable cause by the judge or magistrate, and that the extension is necessary to achieve the objective of the authorization. Each extension granted for a warrant pursuant to this subdivision, shall be for no longer than the

authorizing judge or magistrate deems necessary to achieve the purposes for which the warrant was originally granted, but in any event, shall be for no longer 30 days.

- On Page 3, line 32m after information, insert without a search warrant, as provided in this section,
- On Page 3, line 35, strike concerned. and insert concerned, provided however that the owner or user may not consent to the disclosure of location information if the device is known or believed to be in the possession of or attached to a possession of a third party known to the owner or user.
- On Page 4, strike lines 28 through 30, inclusive.
- On Page 4, line 28, after (b), insert Reports prepared pursuant to subsection (a) shall be made publicly available in an online, searchable format on or before March 1 of each year. If the provider does not have an Internet Web site, the provider shall send the reports to the Office of Privacy Protection on or before March 1 of each year.
  (c) On or before March 1 of each year, a provider subject to Section 22575 of the Business and Professions Code shall complete one of the following actions:
  (1) Create a prominent hyperlink to its latest report prepared pursuant to subsection (a) in the disclosure section of its privacy policy; or
  (2) Post the report prepared pursuant to subsection (a) in the section of its Internet Web site explaining the way in which user information and privacy issues related to its service are addressed.

**********