# SENATE COMMITTEE ON PUBLIC SAFETY

**Senator Aisha Wahab, Chair**
**2023 - 2024 Regular**

| | | | |
|---|---|---|---|
| **Bill No:** | AB 793 | **Hearing Date:** | June 27, 2023 |
| **Author:** | Bonta | | |
| **Version:** | April 19, 2023 | | |
| **Urgency:** | No | **Fiscal:** | Yes |
| **Consultant:** | SC | | |

**Subject:** ***Privacy: reverse demands***

## HISTORY

Source: ACLU California Action
If/When/How
Electronic Frontier Foundation

Prior Legislation: Proposition 1, approved by California voters on Nov. 8, 2022
SB 107 (Wiener), Ch. 810, Stats. 2022
AB 1242 (Bauer-Kahan), Ch. 627, Stats. 2022
AB 1666 (Bauer-Kahan), Ch. 42, Stats. 2022
AB 2091 (Bonta), Ch. 628, Stats. 2022
SB 178 (Leno), Ch. 651, Stats. 2015

Support: Access Reproductive Justice; All Above All; All Family Legal; American Atheists; American Association of University Women – California; American Nurses Association/California; Asian Americans Advancing Justice - Asian Law Caucus; Atheists United Los Angeles; Black Women for Wellness Action Project; California Church Impact; California Coalition for Women Prisoners; California Immigrant Policy Center; California Latinas for Reproductive Justice; California LGBTQ Health and Human Services Network; California News Publishers Association; California Nurse Midwives Association (CNMA); California Public Defenders Association; Chamber of Progress; Citizens for Choice; Consumer Attorneys of California; Electronic Privacy Information Center (EPIC); Equal Rights Advocates; Equality California; Grace - End Child Poverty in California; Lawyering for Reproductive Justice; Indivisible CA Statestrong; Indivisible California Statestrong; Lawyers Committee for Civil Rights of The San Francisco Bay Area; Media Alliance; Mujeres Unidas Y Activas; Mya Network; Naral Pro-Choice California; Oakland Privacy; Planned Parenthood Affiliates of California; Privacy Rights Clearinghouse; Reproductive Health Access Project (RHAP); Restore the Fourth; San Francisco Black & Jewish Unity Coalition; Santa Monica Democratic Club; Secure Justice; St James Infirmary; Starting Over, INC.; Technet-technology Network; TGI Justice Project; The Greenlining Institute; The Women's Building; Training in Early Abortion for Comprehensive Healthcare (TEACH); Women's Foundation California; Women's Health Specialists

Opposition: Arcadia Police Officers' Association; Burbank Police Officers' Association; California Association of Highway Patrolmen; California District Attorneys Association (oppose unless amended); California Police Chiefs Association;

California State Sheriffs' Association (oppose unless amended); California Reserve Peace Officers Association; Claremont Police Officers Association; Corona Police Officers Association; Culver City Police Officers' Association; Deputy Sheriffs' Association of Monterey County; Fullerton Police Officers' Association; Murrieta Police Officers' Association; Newport Beach Police Association; Novato Police Officers Association; Palos Verdes Police Officers Association; Peace Officers Research Association of California (PORAC); Placer County Deputy Sheriffs' Association; Pomona Police Officers' Association; Riverside Police Officers Association; Riverside Sheriffs' Association; Santa Ana Police Officers Association; Upland Police Officers Association

Assembly Floor Vote: 54 - 15

## PURPOSE

***The purpose of this bill is to ban reverse-location searches, also known as a "geofence warrant" which allow law enforcement agencies to obtain cell phone data about unspecified individuals near a certain location, and reverse-keyword searches, which allow law enforcement agencies to obtain data about unspecified individuals who used certain search terms on an internet website.***

*Existing law* 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, and the persons or things to be seized. (U.S. Const., 4th Amend.; Cal. Const., art. I, § 13.)

*Existing law* prohibits exclusion of relevant evidence in a criminal proceeding on the ground that the evidence was obtained unlawfully, unless the relevant evidence must be excluded because it was obtained in violation of the federal Constitution's Fourth Amendment. (Cal. Const., art. I, § 28(f)(2).)

*Existing law* establishes the Reproductive Privacy Act which provides that the Legislature finds and declares that every individual possesses a fundamental right of privacy with respect to personal reproductive decisions, which entails the right to make and effectuate decisions about all matters relating to pregnancy, including prenatal care, childbirth, postpartum care, contraception, sterilization, abortion care, miscarriage management, and infertility care. Accordingly, it is the public policy of the State of California that:

- Every individual has the fundamental right to choose or refuse birth control;
- Every individual has the fundamental right to choose to bear a child or to choose to obtain an abortion, with specified limited exceptions; and,
- The state shall not deny or interfere with a person's fundamental right to choose to bear a child or to choose to obtain an abortion, except as specifically permitted. (Health & Saf. Code, § 123462.)

*Existing law* provides that the state may not deny or interfere with a person's right to choose or obtain an abortion prior to viability of the fetus or when the abortion is necessary to protect the life or health of the person. (Health & Safe. Code § 123466, subd. (a).)

*Existing law* provides that a law of another state that authorizes a state agency to remove a child from their parent or guardian based on the parent or guardian allowing their child to receive gender-affirming health care or gender-affirming mental health care is against the public policy of this state and shall not be enforced or applied in a case pending in a court in this state. (Fam. Code, § 3452.5.)

*Existing law* prohibits law enforcement agencies from knowingly making or participating in an arrest or participating in any extradition of an individual pursuant to an out-of-state arrest warrant for violation of another state's law against providing, receiving, or allowing a child to receive gender-affirming health care of gender-affirming mental health care if the care is lawful in this state. (Pen. Code, § 819.)

*Existing law* provides that a law of another state that authorizes a state agency to remove a child from their parent or guardian based on the parent or guardian allowing their child to receive gender-affirming health care or gender-affirming mental health care is against the public policy of this state and shall not be enforced or applied in a case pending in a court in this state. (Pen. Code, § 1326.)

*Existing law* defines a "search warrant" as a written order in the name of the people, signed by a magistrate and directed to a peace officer, commanding them 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. (Pen. Code, § 1523.)

*Existing law* provides the specific grounds upon which a search warrant may be issued, including 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. (Pen. Code, § 1524.)

*Existing 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. (Pen. Code, § 1525.)

*Existing law* requires a magistrate to issue a search warrant if they are satisfied of the existence of the grounds of the application, or that there is probable cause to believe their existence. (Pen. Code, § 1528, subd. (a).)

*Existing law* provides for a process for a search warrant for records that are in the actual or constructive possession of a foreign corporation that provides electronic communication services or remote computing services to the general public, where the records would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer's usage of those services, the recipient or destination of communications sent or from those customers, or the content of those communications. (Pen. Code, § 1524.2.)

*Existing law* requires a provider of electronic communication services or remote computing services to disclose to a governmental prosecuting or investigating agency the name, address, local and long distance telephone toll billing records, telephone number or other subscriber

number or identity, and length of service of a subscriber to or customer of that service, and the types of services the subscriber or customer utilized, when the governmental entity is granted a search warrant. (Pen. Code, § 1524.3, subd. (a).)

*Existing law* states that a governmental entity receiving subscriber records or information is not required to provide notice of the warrant to a subscriber or customer. (Pen. Code, § 1524.3, subd. (b).)

*Existing law* authorizes a court issuing a search warrant, on a motion made promptly by the service provider, to quash or modify the warrant if the information or records requested are unusually voluminous in nature or compliance with the warrant otherwise would cause an undue burden on the provider. (Pen. Code, § 1524.3, subd. (c).)

*Existing law* requires a provider of wire or electronic communication services or a remote computing service, upon the request of a peace officer, to 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 period upon a renewed request by the peace officer. (Pen. Code, § 1524.3, subd. (d).)

*Existing law* specifies that no cause of action shall be brought against any provider, its officers, employees, or agents for providing information, facilities, or assistance in good faith compliance with a search warrant. (Pen. Code, § 1524.3, subd. (e).)

*This bill* prohibits a governmental entity from making a reverse-location demand or a reverse-keyword demand and prohibits a governmental agency from seeking, from any court, a compulsory process to enforce a reverse-location demand or a reverse-keyword demand.

*This bill* prohibits a court subject to the laws of California from enforcing, including through a compulsory process, a reverse-location demand or a reverse-keyword demand.

*This bill* provides that a government entity shall not seek, secure, obtain, borrow, purchase, use, or review any information or data obtained through a reverse-location demand or a reverse-keyword demand.

*This bill* states that a person in this state or a California entity shall not be obligated to comply with a reverse-location demand or a reverse-keyword demand issued by the State of California or a political subdivision thereof or any other state or a political subdivision thereof.

*This bill* states that a court or government entity of the State of California, or a political subdivision thereof, shall not support, assist, or enforce a reverse-location demand or reverse-keyword demand issued by the State of California or a political subdivision thereof, or any other state or a political subdivision thereof, including the domestication of any such demand.

*This bill* states that a government entity shall not seek the assistance of a nongovernmental entity, an agency of the federal government, or an agency of the government of another state or subdivision thereof in obtaining information or data from a reverse-location demand or reverse-keyword demand if the government entity would be barred from directly seeking that information under the provisions of this bill.

*This bill* provide the following definitions:

- "Government entity" means a department or agency of the state or a political subdivision thereof, or an individual acting for or on behalf of the state or a political subdivision thereof.

- "California entity" means a California corporation or a corporation whose principal executive offices are located in California.

- "Compulsory process" means any court order, including a search warrant, a subpoena or administrative subpoena, or any other legal process seeking to compel the disclosure of records or information.

- "Reverse-keyword demand" means any action by any government entity, seeking or obtaining records or information capable of identifying persons who electronically searched or queried for a particular word or words, phrase or phrases, character string or strings, or website or websites, or who visited a particular website through a link returned in response to such a search or query, regardless of whether the request is limited to a specific geographic area or timeframe. "Reverse-keyword demand" includes any compulsory process seeking such records or information and any action seeking to obtain such records or information in exchange for valuable consideration.

- "Reverse-location demand" means any action by a government entity, seeking records or information pertaining to the location of unspecified electronic devices or their unspecified users or owners, whose scope extends to the electronic devices present in a given geographic area at a given time, whether such device location is measured via global positioning system coordinates, cell tower connectivity, Wi-Fi positioning, or any other form of location detection. "Reverse-location demands" shall include any compulsory process seeking such records or information and any action seeking to obtain such records or information in exchange for valuable consideration.

*Existing law* provides that a defendant may move to suppress as evidence any tangible or intangible thing obtained a result of a search or seizure on either of the following grounds:

- The search or seizure without a warrant was unreasonable; or

- The search or seizure with a warrant was unreasonable because of any of the following:

    - The warrant is insufficient on its face;

    - The property or evidence obtained is not that described in the warrant;

    - There was not probable cause for the issuance of the warrant;

    - The method of execution of the warranted violated federal or state constitutional standards; or,

    - There was any other violation of federal or state constitutional grounds. (Pen. Code, § 1538.5, subs. (a)(1).)

*This bill* specifies that a person in a trial, hearing, or proceeding claiming that information was obtained or retained in violation of the California or United States Constitution or the provisions of this bill may file a motion to suppress and any information found to have been obtained or retained in violation of the law shall be suppressed.

*This bill* authorizes the Attorney General (AG) to commence a civil action to compel a government entity to comply with the provisions of this bill.

*This bill* authorizes an individual whose information is disclosed in a manner that is inconsistent with this chapter or the California or United States Constitutions, or a service provider or any other recipient of the reverse-location demand or reverse-keyword demand, to file a petition to void or modify the reverse-location demand or reverse-keyword demand, or to order the destruction of any information obtained in violation of this bill's provisions or the California or United States Constitution.

*This bill* provides that a person whose information was obtained in violation of this bill's provisions shall be immediately notified of the violation and of the legal recourse available to that person as specified in the bill.

*This bill* requires notice to be in writing by the violating government entity and by any entity that responded to the demand.

*This bill* authorizes a person whose information was obtained in violation of this bill's provisions to institute a civil action against the government entity for one or any combination of the following:

- $1,000 per violation or actual damages, whichever is greater;
- Punitive damages;
- Injunctive or declaratory relief; or,
- Any other relief that the court deems proper.

*This bill* specifies that in assessing the amount of punitive damages, the court shall consider all of the following:

- The number of people whose information was disclosed;
- Whether the violation directly or indirectly targeted persons engaged in exercises of activities protected by the California or United States Constitutions; and,
- The persistence of violations by the particular government entity.

*This bill* provides that in any successful action brought under the provisions of this bill, the court shall award reasonable attorney's fees to a prevailing plaintiff.

*This bill* contains various legislative findings and declarations regarding protecting reproductive and LGBTQI rights and the protecting the privacy and free expression rights of Californians.

*This bill* contains a severability clause so that if any provision of this bill or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.

## COMMENTS

### 1. Need for This Bill

According to the author of this bill:

> Current laws also do not prevent law enforcement from using increasingly common and invasive "reverse warrants" to obtain sensitive private information without sufficient legal process. A normal warrant requires police to have probable cause to investigate an individual. Reverse warrants turn this due process on its head: they compel companies to search their records and reveal the identities of all people who were present at a particular location (geofence demands) or all people who looked up a particular keyword online (keyword demands).
>
> Reverse warrants may also violate the Fourth Amendment. Unlike typical warrants for electronic information, reverse warrants are not targeted to specific individuals or accounts. Instead, they provide access to information about all users or devices that searched for certain words or were located near a certain location. These warrants lack individualized suspicion, allow for broad officer discretion, and impact the privacy rights of countless innocent individuals. They are arguably even broader than the general warrants that inspired the Fourth Amendment's drafters. Early test cases, such as *In the Matter of the Search of Information Stored at the Premises Controlled by Google*, Case No. KM-2022-79 (19th J.D. VA, February 8, 2022), have found the use of reverse warrants to be unconstitutional, as applied.
>
> Digital surveillance is a threat to our reproductive freedoms and to vulnerable people. Since the repeal of Roe, we have seen anti-abortion states use digital data including Facebook messages to prosecute people for having abortions or helping others obtain reproductive care. Geofence demands have also been used to track the locations and identities of people protesting police violence, and could be used to track the locations and identities of people visiting reproductive health clinics as well. People in California have a fundamental, constitutional right of privacy. But fishing expeditions from reverse-geofence and reverse-keyword demands undermine that right—especially for people seeking abortions and gender-affirming care. Reverse warrants can also chill the exercise of the freedom of speech, association, religion, assembly, movement, and the press.
>
> California-based companies are receiving more reverse warrants each year, and the demand will only rise as more states seek to criminalize abortions and gender-affirming healthcare. By passing AB 793, lawmakers can put a stop to the use of these highly invasive methods of surveillance.
>
> This bill builds on the protections established by AB 1242 (Chapter 627, Statutes of 2022), authored by Asm. Rebecca Bauer-Kahan; AB 2091 (Chapter 628,

> Statutes of 2022), authored by Asm. Mia Bonta; AB 1666 (Chapter 42, Statutes of 2022), authored by Asm. Rebecca Bauer-Kahan; and SB 107 (Chapter 810, Statutes of 2022) authored by Sen. Scott Wiener. These four bills limited the ways that out-of-state law enforcement can obtain information related to abortion and gender-affirming care from entities within California.
>
> AB 793 also builds on SB 178 (Chapter 651, Statutes of 2015), authored by Sen. Mark Leno, established strong privacy protections for digital information sought by law enforcement.

**2. Background on Geofencing**

Geofencing is the creation of a virtual boundary in real-world geographic area. Geofencing requires communication technologies such as Global Positioning System (GPS), radio frequency identification (RFID), Wi-Fi or cellular data to trigger a virtual geographic boundary and can track when a device enters or exits that boundary. A virtual boundary can be created around a geographical location as small as a building, store or mall, and as large as a ZIP code, city or entire state.

Originally, geofencing was used by companies to provide targeted ads to their users when they are near certain businesses or services. For example, Google uses the location-based data that it collects "to target ads and measure how effective they are - checking, for instance, when people go into an advertiser's store." (*Article: The Best Offense is a Good Defense: Fourth Amendment Implications of Geofence Warrants* (2022) 50 Hofstra L.Rev. 829, 832.)

Law enforcement agencies started seeking data from companies that store location-based data to develop suspects after the commission of a crime. A geofence warrant seeks cell phone location information that is stored by third-party companies and identifies everyone at a location (provided that they have a cell phone and it is turned on) during a particular time. Law enforcement officials use a geofence warrant to target a crime scene instead of a specific suspect, working backwards in the hopes of developing a suspect, which is why the warrants are often referred to as "reverse-location" warrants. The third party company can establish that the suspect was at the location searched during the time period in question and provide subscriber information. (*Id*. at pp. 833-834.)

Typically, a geofence warrant involves a three-step process to ascertain identifying information about a user:

> First, the warrant targets a specific geographic area defined by GPS coordinates, as well as a specific time frame at that location for some type of criminal offense. Based on this warrant, "Google searches its entire database of user location information - tens of millions of accounts - to extract the subset of data responsive to the warrant, giving police de-identified information on all devices within the area." This first step could lead to hundreds and even thousands of potential devices held by individuals who happened to have been within the geographical zone at the targeted time. Based on this collection, Google then provides anonymized information to the law enforcement officials.
>
> In the second step, law enforcement officials review the initial responses from Google and resubmit requests narrowing down the devices, but receiving more

> information about the devices. Moreover, the information requested about these devices will include information outside of the original designated geographical area.
>
> In the third step, law enforcement officials analyze the devices' data received in the second step. If they believe the information is related to the criminal investigation, they then request that Google provide identification related to these devices. Pursuant to such a request, Google can provide phone numbers, email addresses, and subscribers' names, as well as other information. (*Id*. at pp. 835-836.)

Geofence warrants are on the rise. The first geofence warrant was filed in 2016 and by the end of 2019, Google was receiving about 180 search warrant requests per week from law enforcement officials across the country. Between 2018 and 2020, Google received about 20,000 geofence warrant requests for data. During that two-year time period, over 95% of these requests came from state law enforcement officers. (*Id*. at p. 834.) Google's location history database contains information about hundreds of millions of devices around the world, going back almost a decade. (*Id*. at p. 835.)

The proponents of this bill argue that the use of geofence warrants raises privacy concerns and questions about whether the practice violates constitutional protections against unreasonable searches and seizures. The reverse-keyword demand search works in a similar manner. Those searches operate when law enforcement requests information regarding all internet users who searched for a specific topic or keyword in a specific time period. From there, law enforcement can ascertain who was searching for information related to potentially unlawful conduct.

In the context of reproductive and gender-affirming health care, states that criminalize such health care may use geofence warrants and reverse-keyword searches to track down the locations and identities of people who come to California to access or help others access such care.

**3. Search Warrant Requirements**

Both the United States and the California constitutions guarantee the right of all persons to be secure from unreasonable searches and seizures. (U.S. Const., amend. IV; Cal. Const., art. 1, sec. 13.) Generally, a "search" is a governmental intrusion upon, or invasion of a person's security in an area in which they have a reasonable expectation of privacy. These constitutional provisions generally require the police to secure a warrant before conducting a search, and specify that the warrant must be issued "upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched." (*Ibid*.)

Penal Code section 1523 defines a "search warrant" as an order, in writing, signed by a magistrate, commanding a peace officer to search for personal property and bring it before a magistrate. Section 1524 outlines the statutory grounds for issuance of search warrants and mandates that they be supported by probable cause. The standard for probable cause to issue a search warrant is "whether, given all the circumstances set forth in the affidavit, there is a fair probability that contraband or evidence of a crime will be found in a particular place." (*Illinois v. Gates* (1983) 462 U.S. 213, 238.)

The California Electronic Privacy Act (CalECPA), enacted by SB 178 (Leno), Chapter 651, Statutes of 2015, is a comprehensive digital privacy law which took effect on January 1, 2016 (§ 1546 et seq.):

> [I]t requires all California state and local law enforcement agencies to obtain a search warrant or wiretap order before they can access any electronic communication information. The law defines 'electronic communication information' in the broadest terms possible so that it includes emails, digital documents, text messages, location information, and any digital information stored in the cloud. The law protects all aspects of electronic communication information, not just its contents, but also metadata information relating to the sender, recipient, format, time, date, and location of the communications, including IP addresses.
>
> CalECPA also limits the ability of California law enforcement to obtain information directly from a smartphone or similar device, or to track them. Law enforcement must either obtain a warrant or get the consent of the person possessing the electronic device.

(Daniels, *California Updates Privacy Rights with the Electronic Communications Privacy Act* (Nov. 17, 2015) JDSupra.)

Recently, a California Court of Appeal found that a geofence warrant used by law enforcement in finding two murder suspects violated the Fourth Amendment but did not violate CalECPA. (*People v. Meza* (2023) 90 Cal.App.5th 520.) *Meza* involved two defendants who were identified as suspects in a murder after a geofence warrant directed to a technology company revealed that their cell phone data was connected to several of the same locations as the victim on the day of the victim's murder. The defendants moved to suppress the evidence but were denied and ultimately convicted of murder. The court of Appeal found that the geofence warrant violated the Fourth Amendment but upheld the murder convictions under the good faith exception to the exclusionary rule.

In determining the validity of a warrant courts examine three main factors: probable cause, particularity and overbreadth. (*Meza*, *supra*, 90 Cal.App.5th at 535.) Probable cause will be found to support the issuance of a warrant if "'the magistrate had a substantial basis for concluding a fair probability existed that a search would uncover wrongdoing.'" . . . . "Particularity is the requirement that the warrant must clearly state what is sought." . . . .To satisfy this requirement, "[c]omplete precision in describing the place to be searched is not required. . . . . "Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based." (*Ibid*.)

The *Meza* court found that while the geofence warrant was supported by probable cause because it was reasonable for the magistrate to conclude that the perpetrators of the murder were carrying cell phones the day of the murder and may have used them in coordinating their movements. (*Id*. at p. 536.) However, the court found that the geofence warrant lacked particularity and was overbroad in violation of the Fourth Amendment. Specifically, the geofence warrant "failed to meet the particularity requirement because it provided law enforcement with unbridled discretion regarding whether or how to narrow the initial list of users identified by Google. Once the step one search had been conducted, law enforcement officials were able to enlarge the geographic parameters of the search and request additional information on any of the potentially thousands

of users identified without any objective criteria limiting their discretion. Again, at step three law enforcement could seek identifying information of any of the users found within the search parameters without restriction on how many users could be identified or any further showing that information concerning each individual user would be relevant to the case." (*Id*. at pg. 538.)

The court found that the warrant was overbroad because law enforcement failed to draw the search boundaries as narrowly as they could have given the information that was available to them which potentially allowed a location-specific search of thousands of individuals. The court recognized that it may be impossible to exclude any uninvolved third parties, but stated that the proper inquiry is the reasonableness of the search. The court concluded that "The warrant here, authorizing the search of more than 20 acres total over a cumulative period of more than five hours in residential and commercial areas did not meet this fundamental threshold requirement." (*Meza*, *supra*, 90 Cal.App.5th at pp. 539-541.)

This bill would ban geofence warrants and reverse-keyword searches. Specifically, this bill would prohibit any government entity from seeking, or any court from enforcing, assisting, or supporting, a reverse-keyword or reverse-location demand, as defined, issued by a government entity or court in this state or any other state. Any person or California entity would be prohibited from complying with a reverse-keyword or reverse-location demand. The bill would require a court to suppress any information obtained or retained in violation of these provisions, the United States Constitution, or California Constitution.

Proponents of this bill argue that such digital surveillance undermines the public's fundamental, constitutional right of privacy which is especially dangerous for people seeking abortions and gender-affirming care. Additionally, they argue that the reverse-keyword search can chill the exercise of the freedom of speech, association, religion, assembly, movement, and the press.

Opponents of the bill argue that a blanket prohibition on the use of these types of warrants which have been effective in identifying suspects that commit serious crimes is overbroad and will lead to such crimes going unsolved.

**4. Full Faith and Credit Clause**

Generally, the laws of the state regulate conduct that occurs within that state. However, situations may arise where more than one state's laws may apply such as collection of previously-owed income taxes or child support obligations from another state. Or one state has jurisdiction to criminally prosecute an offense because someone has fled the state or committed part of the crime in the prosecuting state. Under the United States Constitution, states are required to provide full faith and credit to "to the public acts, records, and judicial proceedings of every other state. (U.S. Const. art. IV, sec. 1.)"

The Full Faith and Credit Clause may be implicated when there is a conflict between the laws of the different states. At least one court has held that any effort by a state to apply its criminal laws beyond its state borders to criminalize activity that is otherwise lawful in the other state. (*Bigelow v. Virginia* (1975) 421 U.S. 809.) However, the Supreme Court has also held that even when criminal conduct takes place outside of the state, extraterritorial jurisdiction may be proper when the conduct was intended to produce or did produce harmful effects within the state. (*Strassheim v. Daily* (1911) 221 U.S. 280.)

The Supreme Court has also made a distinction between the strength of the Full Faith and Credit Clause's applications to judgements versus state law. "The Full Faith and Credit Clause does not compel 'a state to substitute the statutes of other states for its own statutes dealing with a subject matter concerning which it is competent to legislate. Regarding judgments, however, the full faith and credit obligation is exacting. A final judgment in one State, if rendered by a court with adjudicatory authority over the subject matter and persons governed by the judgment, qualifies for recognition throughout the land.'" (*Baker v. General Motors Co*., *supra*, 522 U.S. at 232-233.) This concept is often referred to as the "public policy exception" meaning statutes in one state is given effect only if they do not contravene the public policy of the other state.

By rejecting out-of-state law enforcement's attempts to seek reverse-location and reverse-keyword data in California, this bill implicates the Full Faith and Credit Clause. If this bill were challenged based on the Full Faith and Credit Clause, California would argue that assisting in the enforcement of laws in other states that restrict reproductive and gender-affirming health care is contrary to the public policy of this State, which is supported by case law. However, it is unclear whether the court would view this bill as ignoring another state's statutory laws versus ignoring a judgement from that state.

**5. Proposition 8: Truth in Evidence**

In 1982, the California voters passed Proposition 8. Proposition 8 enacted article I, section 28 of the California Constitution, which provides in relevant part: "Right to Truth-in-Evidence. Except as provided by statute hereafter enacted by a two-thirds vote of the membership in each house of the Legislature, relevant evidence shall not be excluded in any criminal proceeding, including pretrial and post-conviction motions and hearings." (Cal. Const., art. I, § 28, subd. (f); *People v. Lazlo* (2012) 206 Cal.App.4th 1063, 1069.) The "Truth-in-Evidence" provision of Section 28 "was intended to permit exclusion of relevant, but unlawfully obtained evidence, only if exclusion is required by the United States Constitution." (*In re Lance W*. (1985) 37 Cal.3d 873, 890 (*Lance W*.).) Thus, Section 28 federalized California's search and seizure law. A trial court may exclude evidence under Penal Code section 1538.5 only if exclusion is mandated by the federal Constitution. (*Lance W*., *supra*, 37 Cal.3d at p. 896.)

This bill would require suppression of evidence obtained through a reverse location demand or a reverse keyword demand, even if the violation did not require exclusion under the federal Constitution. Accordingly, this bill may implicate Proposition 8 and thus requires a 2/3 vote.

**6. Committee Amendments**

The author intends to narrow the bill to apply to reverse-location demand or reverse-keyword demand related to seeking, obtaining, providing or supporting another in seeking or obtaining sexual and reproductive health care and gender affirming health care.

**7. Double-Referral with Judiciary Committee**

This bill would authorize the AG to commence a civil action to compel a government entity to comply with the provisions of this bill. An individual whose information is disclosed would be authorized to file a petition to void or modify the reverse-location demand or reverse-keyword demand, or to order the destruction of any information obtained in violation of this bill's provisions or the California or United States Constitution. A person whose information was

obtained in violation of this bill's provisions would be required to be notified in writing of the violation and of any legal recourse available to that person.

Additionally, a person whose information was obtained in violation of this bill's provisions would be authorized to institute a civil action against the government entity.

Because these provisions are within the Judiciary Committee's jurisdiction, this bill has been double-referred and these issues will be fully analyzed by that committee.

**8. Argument in Support**

This bill is supported by a broad coalition of advocacy organizations, which focus on reproductive justice, LGBTQI+ rights, equity, criminal justice, free expression. According to Electronic Frontier Foundation, a co-sponsor of this bill:

> The bill specifically addresses the problem of "reverse demands" and would put a stop to their use in relation to reproductive care, gender-affirming care, and supportive services for that care. These demands have been used to target people exercising their rights and poses an immediate threat after the Supreme Court overturned Roe v. Wade and as more states across the country criminalize gender-affirming care nationwide.
>
> Normal warrants seek information about a particular person police have probable cause to believe merits investigation. A reverse warrant seeks the opposite: the identity of all the people who were present at a particular location (geofence demands) or who looked up a particular term in a search engine (keyword demands) simply because of where they were or what they searched for. Thousands or even millions of people can be included in a single, overbroad request without any probable cause at all. Rather than help law enforcement find a needle in a haystack, reverse warrants give law enforcement a haystack to search through without any guarantee the needle they want is anywhere inside.
>
> These demands can be used to conduct broad fishing expeditions for those who are seeking needed healthcare. They allow local law enforcement in states across the country to request the names and identities of people whose digital data trail shows they've visited California abortion or gender-affirming care providers. They could indicate if people searched for revealing particular keywords online such as "mifepristone," "abortion drugs," "top surgery," or for care options in California. Or a police investigator could ask for everyone who was outside an unrelated business across the street from a reproductive health clinic–skirting around the reproductive privacy protections enacted last year. A.B. 793 also extends greater protections to those seeking gender-affirming care.
>
> Reverse demands have the same practical effect as unconstitutional general warrant. Since our Nation's founding, general warrants have been deemed a significant threat to personal freedom, privacy, and liberty, and the Supreme Court has repeatedly held that the Fourth Amendment to the United States Constitution prohibits the use of these general warrants. These 'hated writs' spurred colonists toward revolution and directly motivated James Madison's

crafting of the Fourth Amendment." It is not surprising then that courts have found reverse-location demands unconstitutional.

This bill originally sought to take these demands off the table completely; however, in response to pushback from legislators, the author has committed to focus the scope of A.B. 793 to give the strongest possible protection to those most immediately vulnerable in the present, post-Dobbs climate. The use of reverse demands poses a threat to those who are seeking reproductive or gender-affirming care, particularly if they are coming to California from other states. Taking reverse warrants off the table in this focused context would solidify California's place as a protector of those who are merely seeking healthcare. It would also provide needed clarity for companies that receive these warrants, which also support the bill because it addresses the lack of scrutiny applied to these demands before they are issued.

**9. Argument in Opposition**

This bill is opposed by police officer associations, police chiefs, sheriffs and district attorneys. According to California District Attorneys Association, who are opposed unless amended:

[T]he proposed amendments (and in print version) of AB 793 would preclude law enforcement's use of reverse demands not just in cases targeting legal reproductive or gender affirming care in California, but in virtually all other instances as well. This result would deprive investigators of critical information routinely used to help solve cases involving mass shootings, bombings, rapes, child sexual assault materials, and a host of other crimes victimizing the most vulnerable in our society.

First, the proposed language would ban law enforcement's reverse search demands for locations for locations "within two miles of any airport, rail terminal, railway station, terminal for interstate bus, or border checkpoint or crossing." It would also ban law enforcement's reverse demands for locations within one mile of a site offering sensitive services. Further, because of the bill's overly expansive definition of "sexual and reproductive health care," such sites would include not only traditional care providing clinics and hospitals, but also all sites that provide mental health care, including jails and prisons, medical offices, including those in schools, pharmacies, sites providing infectious disease services (such as a COVID testing site), and places offering services for victims of sexual assault or hate crimes – regardless of whether those locations actually offer reproductive or gender affirming care.

This geographical ban likely encompasses the vast majority of inhabited California. Its inclusion in the bill means not only law enforcement, but judges and internet service providers as well will need to research and locate all possible service locations and transit sites before approving or responding to any reverse demand – a substantial demand on our judicial officers' time and resources. Even with diligence the definitions are so broad is seems nearly impossible to identify all possible service or transit locations. This is especially important in combination with the bill's other broad language that would require service and transit sites be taken into consideration for virtually all reverse demands. If, for

example, law enforcement officers were investigating a kidnapping, the bill would require diligent law enforcement officers and judges eliminate all protected sites before determining whether a warrant could issue.

Next, the proponent's proposed language (and the bill in print) would ban any reverse demand by a government entity "from which sensitive services information can be inferred." It can always be inferred that someone traveling near or entering into a location providing sensitive service relates to someone seeking, obtaining, providing, or supporting sensitive services. It is unreasonable to expect an officer seeking a warrant or a judicial officer reviewing a warrant (or other request) in any case involving any type of crime to determine whether their request would inadvertently capture information from which sensitive services information could be inferred.

Sadly, providers and patients of reproductive and gender affirming care are among the people most likely to be negatively impacted by the negative impacts of AB 793. Protests and violence at clinic sites are frequent and escalating. For example, just last week, charges were brought against two masked men who bombed a Costa Mesa Planned Parenthood clinic at 1 a.m. in the morning. Reverse keyword searches can be used to find criminal actors who searched for information about bomb making or clinic locations. Under the proposed language however, such techniques would be off limits.

**-- END –**