SENATE COMMITTEE ON PUBLIC SAFETY

Senator Aisha Wahab, Chair
2023 - 2024 Regular

Bill No:	AB 1027	**Hearing Date:**	July 11, 2023
Author:	Petrie-Norris		
Version:	July 3, 2023		
Urgency:	No	**Fiscal:**	Yes
Consultant:	MK		

Subject: ***Social media platforms: drug safety policies***

HISTORY

Source: The Alexander Neville Foundation

Prior Legislation: SB 178 (Leno), Chapter 651, Stats. 2015

Support: TechNet

Opposition: ACLU California Action; Electronic Frontier Foundation

Assembly Floor Vote: 77 - 0

PURPOSE

The purpose of this bill is to require social media companies post policies regarding the sale of controlled substance on the platform to require information that violates the polices to be stored for 90 days and to provide for when that information can be shared with law enforcement.

Existing law provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (California Constitution, Article I, Section 1.)

Existing law declares that the right to privacy is a personal and fundamental right protected by the California Constitution and that all individuals have a right of privacy in information pertaining to them. (Civil Code§ 1798.1, the Information Practices Act of 1977.)

Existing law requires, pursuant to the California Consumer Protection Act of 2018 (CCPA), businesses, as defined, to include specified information in their privacy policies, such as a description of consumer rights, the categories of personal information the business collects about consumers, and a list of the categories it has sold about consumers in the preceding 12 months. (Civil Code § 1798.130.)

Existing law requires an operator of a commercial website or online service that collects personally identifiable information about consumers to conspicuously post its privacy policy on its website and included specified disclosures. (Business and Professions Code § 22575.)

Existing law defines "social media platform" as a public or semipublic internet-based service or application that has users in California and meets specified criteria. (Business and Professions Code § 22945.)

Existing law provides that, except as otherwise provided, every person who possesses for sale or purchase for purposes of sale any specified controlled substance, as defined, shall be punished by imprisonment in a county jail for two, three, or four years pursuant to existing law pertaining to felony sentencing. (Health and Safety Code § 11351.)

Existing law provides that, except as otherwise provided, every person who transports, imports into this state, sells, furnishes, administers, or gives away, or offers to transport, import into this state, sell, furnish, administer, or give away, or attempts to import into this state or transport, any specified controlled substance shall be punished by imprisonment in a county jail for two, three, or four years pursuant to existing law pertaining to felony sentencing. (Health and Safety Code § 11352.)

Existing law defines "controlled substance," unless otherwise specified, to mean a drug, substance, or immediate precursor which is listed in any schedule pursuant to the Uniform Controlled Substances Act, as specified. (Health and Safety Code Section 11007; §§ 11054-11058.)

Existing law pursuant to the federal Communications Decency Act of 1996, provides, that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider," and affords broad protection from civil liability for the good faith content moderation decisions of interactive computer services. (47 U.S.C. §§ 230(c)(1) and (2).)

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 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. (Penal Code § 1528 (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. (Penal 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 (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. (Penal Code § 1524.3 (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. (Penal Code, § 1524.3 (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. (Penal Code § 1524.3 (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. (Penal Code § 1524.3(e).)

Existing law creates the Electronic Communications Privacy Act. (Penal Code §§ 1546 *et. seq.*)

Existing law provides that except as provided, a government entity shall not do any of the following:

a) Compel the production of or access to electronic communication information from a service provider.
b) Compel the production of or access to electronic device information from any person or entity other than the authorized possessor of the device.
c) Access electronic device information by means of a physical interaction or electronic communication with the electronic device. (Penal Code § 1546.1(a))

Existing law provides that a government entity may compel the production of or access to electronic communication information from a service provider, or compel the production of or access to electronic device information from any person or entity other than the authorized processor of the device only under the following circumstances:

a) Pursuant to a warrant.
b) Pursuant to a wiretap order.
c) Pursuant to an order for electronic reader cards issued under the Civil Code
d) Pursuant to a subpoena issued pursuant to existing law, provided that the information is not sought for the purpose of investigating or prosecuting a criminal offense.
e) Pursuant to an order of a pen register or trap trace device. (Penal Code § 1546.1(b))

Existing law provides that a government entity may access electronic device information by means of a physical interaction or electronic communication device only: pursuant to a warrant; wiretap; with authorization of the possessor of the device; with consent of the owner of the device; in an emergency; if seized from an inmate. (Penal Code § 1546.1(c))

Existing law describes what a warrant for electronic information shall include. (Penal Code § 1546.1(d))
Existing law provides that if a government entity receives electronic communication voluntarily it shall destroy that information within 90 days except under specified circumstances. (Penal Code § 1546.1(g))

This bill provides that among the items that a social media company shall submit to the Attorney General regarding their terms of service report that they shall include whether their current terms of service defines controlled substance distribution.

This bill adds to the items that a social media platform shall create and publicly post on their websites the following:

- A general description of the social media platform's policy on the retention of electronic communication information as defined in Section 1546 of the Penal Code.
- A general description of the social media platform's policies and procedures governing when a platform proactively shares relevant information pertaining to the illegal distribution of a controlled substance.

This bill provides that a social media platform shall retain data on content it has taken action to take down or remove for a violation of a policy prohibiting the unlawful sale, distribution, amplification, or otherwise proliferation of controlled substances and related paraphernalia.

This bill provides that social medial platform shall retain the content that violated a policy and the user name of the violating account for a period of 90 days.

This bill provides that it does not prohibit a social media platform from disclosing account and user information when request by law enforcement under the California Consumer Privacy Act.

This bill provides that the Attorney General shall identify a clear and designated point of contact within the Department of Justice to direct reports by a social media platform of actioned content or accounts that indicate an "eminent" threat to human life.

This bill provides that it does not authorize a governmental entity to compel production of or access sot content or electronic communication from a service provider, or compel the production of or access to electronic device information except as pursuant to the California Electronic Privacy Act in the Penal Code.

COMMENTS

1. Need for This Bill

According to the author:

> Two disturbing trends have dramatically escalated the dangers of fentanyl: the deceptive use of fentanyl in counterfeit pills and the use of social media to traffic these drugs to young people. Drug dealers have capitalized on the anonymity of social media sites to target their sales to pre-teens, teens and unhoused youth. These sites have chat settings designed to erase chat history after just a few hours, making it incredibly difficult for law enforcement to track and prosecute online fentanyl traffickers.

AB 1027 will strengthen the collaboration between social media companies and law enforcement as they work together to curb the practice of online drug trafficking in California. Specifically, the bill will:

- Require social media companies to post in their policy statement a general description of their platform's policy on the retention of electronic communications information.
- Require social media companies to create and submit to the California Attorney General's office a monthly report of accounts that have been flagged for illicit drug sales.
- Require social media companies to retain the information related to the actioned account, including a record of, and the content of, the communications for 90 days.
- Upon failure to retain information related to the actioned account, a social media company will be subject to fine of not more than $190,000 for the initial violation and no more than $380,000 for subsequent violations.

2. Search warrants and the California Electronic Privacy Act

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.)

In 2015, the Legislature enacted CalECPA (SB 178 (Leno), Chapter 651, Statutes of 2015), a comprehensive digital privacy law which took effect on January 1, 2016 (§ 1546 et seq.).

> [CalECPA] 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.

The act defines "electronic device information" as any information stored on or generated through the operation of an electronic device, including the current and prior locations of the device. "Electronic communication information" means 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. "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.

3. Possible Conflict between CalECPA and the California Consumer Privacy Act

This bill intends to address issues with social media platforms being used for drug sales. It adds to reports they need to start submitting to the Attorney General in 2024 information regarding their terms of service contract information on sales of a controlled substance. It also adds to the things a social media platform must post on their website information on the retention of electronic communication information and a general description of their policies and procedures governing when they will proactively share relevant information pertaining to illegal distribution of a controlled substance.

This bill on the one had provides that it does not prohibit a social media platform from disclosing account and user information when requested *by law enforcement* under the California Consumer Privacy Act (CCPA) but it also provides that it does not authorize a governmental entity to compel the production of or access to content or electronic communications device or electronic device information except under CalECPA. CCPA provides that it shall not restrict a business's ability to comply with a civil, criminal, or regulatory inquiry, subpoena, or summons by federal, state, or local authorities. It also allows law enforcement to request consumer information not be destroyed for 90 days pursuant to an investigation in order to allow an agency to receive a subpoena or warrant. CalECPA requires law enforcement to get a warrant to access electronic communication information. The bill already requires the information to be stored for 90 days so is that provision of CCPA necessary. Should the law be clear that CalECPA needs to be followed to access the information and the reference to CCPA be deleted?

4. Notice to the Attorney General

The bill provides that the Attorney General shall identify a clear and designated point of contact with in the Department of Justice to direct reports by a social media platform of actioned content or accounts that indicate an eminent (*sic*) threat to human life. If a threat is imminent, will notifying the Attorney General's office help? Is the AG expected to act on it immediately? Will the contact have to be available 24/7? Would it make more sense to have a social media platform notify a local agency if the locale can be determined? Since this could be seen as an

exception to CalECPA, should what is an imminent threat be more clearly defined such as the potential of death or great bodily injury?

As a technical amendment, staff believes the intent was to refer to an imminent threat, not an eminent threat? If it is intended to mean that it is not urgent but instead that it stands out maybe a different term than eminent should be used?

5. Double-referral

This bill was first heard by the Senate Judiciary Committee.

6. Argument in Support

Technet supports this bill stating:

> AB 1027 takes a significant step toward establishing greater collaboration between law enforcement and social media platforms in combatting the illegal sale of controlled substances online. This bill would require platforms to retain data on specified content related to a violation of its controlled substances policy and retain that data for a period of 90 days. AB 1027 also requires platforms to report to the Attorney General information about content related to controlled substances on the platform on a semiannual basis. We are working with the author to secure an additional amendment that replaces the reference to "controlled substances distribution" with "controlled substances," broadening the category and bringing it into closer alignment with how platforms currently collect such information. Adding these requirements will equip law enforcement and prosecutors with more information about when and how to file preservation requests and warrants, which can mean the difference between successfully building a case against a dealer or not.

7. Argument in Opposition

The Electronic Frontier Foundation opposes this bill stating (letter for 6/20/23 version):

> There are several reasons that a person may wish to delete records of their personal conversations promptly. Many choose to automatically delete messages for convenience's sake. But there are several instances where being able to delete information whenever you want carries greater importance. For example, a student may be speaking to a friend about a potential decision to become public about their sexual orientation in messages, and not wish for their parents to see it.
>
> This is particularly true right now, as many states across the country pass laws criminalizing certain types of healthcare. A person seeking reproductive or genderaffirming care that's criminalized in their state may speak to a support group about receiving that care. Law enforcement officials seeking to prosecute people seeking or supporting this kind of health care will have far more time to request access to that information if this bill requires its retention. Those seeking to expose that information— whether to bring lawsuits under bounty-style state laws around reproductive care, or to simply to embarrass people by exposing their personal conversations—will also have more time to hack into it.

Conditioning retention mandates on whether a social media platform has taken an action on content is also deeply concerning. Social media company content moderation and takedown systems are unreliable and often flag information that is not in violation of any rules. Speech moderation rules are unevenly enforced, with little to no transparency, against a range people for whom the Internet is an irreplaceable forum to express ideas, connect with others, and find support. This includes people on the margins who question authority, criticize the powerful, educate, and call attention to discrimination.

The bill's requirement that providers scan "actioned content" also poses serious threats to end-to-end encryption and, therefore, user privacy. Requiring that platforms scan actioned content may as a practical matter mean that platforms will not let people use end-to-end encryption because it would interfere with scanning.

Private communication is a basic, universal right. In the online world, the best tool we have to defend this right is end-to-end encryption. This ensures that governments, tech companies, social media platforms, and other groups cannot view or access our private messages, the pictures we share with family and friends, or our bank account details. This is a universal right, and one that is a particularly vital protection for the most vulnerable in society—such as children or human rights defenders who rely on private messaging to do their jobs in hostile environments.

Requiring companies to retain this kind of information under a government mandate undermines people's control of their own personal conversations. It also substantially increases risks that their information could be exposed, and effectively removes the option for end-to-end encryption. For these reasons, we must respectfully oppose A.B.1027 and respectfully urge your ″no" vote. Thank you.

-- END –