Date of Hearing: July 2, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 918 (Umberg) – As Amended June 20, 2024

SENATE VOTE: 39-0

SUBJECT: Law enforcement liaisons: search warrants

SYNOPSIS

Shielded by the sweeping immunity provided by Section 230 of the federal Communications Decency Act of 1996, some social media platforms have become useful forums for trafficking in a wide array of illicit activities. Of particular concern are reports that social media platforms are not reliably responding to notifications from users and law enforcement about drug dealers on the platforms, allowing drug dealers to continue to sell illicit drugs, especially fentanyl—the synthetic opioid that is 50 to 100 times stronger than morphine—on the platform for weeks or months after being made aware of the illegal conduct.

This bill seeks to make social media platforms with over a million discrete monthly active users more responsive to California-based law enforcement entities. First, the bill requires platforms to provide a liaison to respond to law enforcement requests for information. Second, the bill requires platforms to comply with search warrants within 72 hours, as specified. The bill grants courts the ability to extend this period for good cause, provided that doing so will not result in an adverse result that jeopardizes the investigation.

The bill is sponsored by the author and is supported by numerous law enforcement organizations. The bill is opposed by ACLU California Action, the Electronic Frontier Foundation, and Internet.Works California. Recent amendments that introduce more flexibility into the process established under the bill appear to have addressed, if not resolved, their principal concerns.

SUMMARY: Requires platforms to provide a liaison to respond to law enforcement requests for information and to comply with search warrants within 72 hours. Specifically, **this bill**:

1) Requires a social media platform with over 1 million discrete monthly active users to:

    a) At all times, make available by telephone to a California law enforcement agency a law enforcement liaison—a natural person who serves as the point of contact with law enforcement agencies—for the purpose of receiving, and responding to, requests for information.

    b) Except as required by any other law, comply with a search warrant within 72 hours if the search warrant is provided to the social media platform by a law enforcement agency and the subject of the search warrant is information associated with an account on the social media platform and that information is controlled by a user of the social media platform.

2) Provides that a court may reasonably extend the time required to comply with a search warrant if the court makes a written finding that the social media platform has shown good cause for the extension and has shown that it would not cause an adverse result.

EXISTING LAW:

1) Provides, pursuant to the U.S. Constitution, 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., Fourth Amend; *see also* Cal. Const. art. 1, § 13.)

2) Defines "social media platform" as a public or semipublic internet-based service or application that has users in California and that meets both of the following criteria:
    a) A substantial function of the service or application is to connect users in order to allow users to interact socially with each other within the service or application.
        i. A service or application that provides email or direct messaging services shall not be considered to meet this criterion on the basis of that function alone.
    b) The service or application allows users to do all of the following:
        i. Construct a public or semipublic profile for purposes of signing into and using the service.
        ii. Populate a list of other users with whom an individual shares a social connection within the system.
        iii. Create or post content viewable by others, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the users with content generated by others. (Bus. & Prof. Code § 22945(a)(3).)

3) Permits a person to seek an order requiring a social media platform to remove content that includes an offer to transport, import into the state, sell, furnish, administer, or give away a controlled substance in violation of specified state law.
    a) If the platform has a reporting mechanism, the person must report the content and request that it be removed before seeking the order, and the court may not act upon the request until 48 hours have passed since the request was made.
    b) If the platform does not have a reporting mechanism, the person may bring, and the court may act on, the action at any time.
    c) The court shall award court costs and reasonable attorney's fees to a prevailing plaintiff. (Bus. & Prof. Code § 22945.5.)

4) Defines a "search warrant" as a written order 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. (Pen. Code § 1523.)

5) 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.)

6) Defines "adverse result" with respect to notification of the existence of a search warrant, as:
    a) Danger to the life or physical safety of an individual.
    b) A flight from prosecution.
    c) The destruction of or tampering with evidence.
    d) The intimidation of potential witnesses.
    e) Serious jeopardy to an investigation or undue delay of a trial. (Pen. Code § 1524.2(a)(2).)

7) Provides that a foreign corporation may be required to produce records in response to a search warrant in five days if there is a showing that the failure to produce the records within that timeframe would cause an adverse result. Enables a court to reasonably extend that time period for good cause shown. (Pen. Code § 1524.2(b)(2).)

8) 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.)

9) 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 § 1529(a).)

10) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. (Pen. Code § 1546 et seq.)

11) Requires a provider of an electronic communication service subject to CalECPA to maintain a law enforcement contact process that must do all of the following, at a minimum:
    a) Provide a specific contact mechanism for law enforcement personnel.
    b) Provide continual availability of the law enforcement contact process.
    c) Provide a method to provide status updates to a requesting law enforcement agency on a request for assistance. (Pen. Code § 1524.4(a), (b).)

12) Provides that a court may order the destruction of information gathered pursuant to a warrant under CalECPA and requires that information voluntarily provided under same must, within 90 days, be destroyed. (Pen. Code § 1546.1(e)(2), (g).)

FISCAL EFFECT: As currently in print, this bill is keyed nonfiscal.

COMMENTS:

1) **Crime and social media.** Whereas the European Union requires platforms to take down certain illegal content, Section 230 of the federal Communications Decency Act of 1996

provides civil immunity for online platforms based on third-party content and for the removal of content in certain circumstances.[1] As the United States Department of Justice has stated, "[t]he combination of significant technological changes since 1996 and the expansive interpretation that courts have given Section 230. . . has left online platforms both immune for a wide array of illicit activity on their services and free to moderate content with little transparency or accountability."[2] Social media platforms in the United States thus have virtually no duty to remove deplorable, tortious, or even criminal content.[3]

The accountability vacuum created by Section 230, along with the anonymity and widespread reach of social platforms, some of which have encrypted or disappearing messages, make them a useful medium for criminal activity. Although comprehensive statistics are not available, it is well documented that platforms are commonly used to recruit gang members and terrorists; groom victims of sexual abuse and sex trafficking; circulate child pornography and revenge pornography; cyberstalk, harass, and intimidate victims; gain access to personal information for identify theft; and facilitate the sale and distribution of illegal drugs, particularly to younger social media users.[4]

2) **Search warrants.** The Fourth Amendment of the United States Constitution protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and provides, "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."[5] "The 'basic purpose of this Amendment …' … 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.'"[6] "When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' … official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[7] The Fourth Amendment is enforced in part through motions to exclude evidence from an unlawful search.

"Most federal courts to rule on the issue have agreed that Facebook and other social media users have a reasonable expectation of privacy in content that they exclude from public access, such as private messages."[8] "[W]hether someone can assert a subjective expectation of privacy in their social media accounts depends on the privacy settings they had in place at the time the intrusion occurred."[9] "When a social media user disseminates his postings and information to the public, [these postings] are not protected by the Fourth Amendment" because anyone can view them; thus, a search warrant is not necessary to seize those messages.[10] On the other hand, when

---

[1] 47 U.S.C. § 230.
[2] "Section 230—Nurturing Innovation or Fostering Unaccountability" (June, 2020), https://www.justice.gov/ag/file/1072971/dl?inline=.
[3] See Rustad and Koenig, "The Case for a CDA Section 230 Notice-and-Takedown Duty" (Spring, 2023) 23 Nev.L.J. 533.
[4] *Ibid*.; Hoffman, "Fentanyl Tainted Pills Bought on Social Media Cause Youth Drug Deaths to Soar" (May 19, 2022) *N.Y. Times*, https://www.nytimes.com/2022/05/19/health/pills-fentanyl-social-media.html.
[5] U.S. Const., 4th Amend.
[6] *Carpenter v. United States* (2018) 585 U.S. 296, 303, citation omitted.
[7] *Id*. at p. 304.
[8] *United States v. Zelaya-Veliz* (4th Cir. 2024) 94 F.4th 321, 333.
[9] *United States v. Weber* (D.Mont. 2022) 599 F.Supp.3d 1025, 1033.
[10] *United States v. Meregildo* (S.D.N.Y. 2012) 883 F.Supp.2d 523, 525.

someone posts using a more secure privacy setting on social media, this reflects an intent to keep information private, and so that information may be constitutionally protected.[11]

Because social media accounts may contain a vast history of an individual's private, sensitive communications, law enforcement searches in this space present unique challenges under the Fourth Amendment. To illustrate, the Fourth Circuit Court of Appeals, raising concern over the lack of temporal restrictions in search warrants for the accounts of six men affiliated with a transnational criminal organization who were convicted of sex trafficking a 13-year-old girl, recently wrote:

> […] The reasonableness standard that is so central to the Fourth Amendment necessitates that we permit the government to thwart these emerging criminal tactics with novel investigatory tools of its own. Warrants for social media data are one such tool, as they empower law enforcement officers to reveal the activities of criminal conspirators, disrupt their illicit plots, and bring them to justice. But while social media warrants can support invaluable police work, . . . they also provide significant potential for abuse. We cannot read the Fourth Amendment to allow the indiscriminate search of many years of intimate communications. And because of the inherent interconnectedness of social media, permitting unbridled rummaging through any one user's account can reveal an extraordinary amount of personal information about individuals uninvolved in any criminal activity.
>
> It is not only courts that are struggling to strike a balance between privacy and security in the rapidly changing digital domain, but society as a whole. When criminal offenders use social media to organize their enterprises and evade detection, it would seem unreasonable to disable law enforcement from using those same media to apprehend and prosecute them. To hold otherwise would arbitrarily tip the scales away from law and justice for the benefit of increasingly sophisticated criminal schemes. But at the same time, there comes a point when the Fourth Amendment must emphatically yell STOP, lest we render obsolete the hallowed notion of a secure enclave for personal affairs.[12]

California provides additional protections in this space. The California Electronic Communications Privacy Act ("CalECPA") prohibits government entities from accessing electronic device information from service providers, unless it does so pursuant to a judicial order for, e.g. a warrant, wiretap order, or tracking device search warrant.[13] "Service providers" under CalECPA are entities that "provide[] to its subscribers or users" the ability to send, receive, or store electronic communication information.[14] That includes social media platforms under this bill.[15] Under CalECPA, people who are the target of a search warrant may seek relief in court to void or modify the warrant.[16] CalECPA additionally provides, in certain circumstances, for the destruction of information gathered pursuant to its provisions after the purpose for which the information was collected has been served.[17]

---

[11] *Ibid.*
[12] *United States v. Zelaya-Veliz* (4th Cir. 2024) 94 F.4th 321, 342-343.
[13] Pen. Code § 1546.1(a), (c).
[14] Pen. Code § 1546(e), (j).
[15] *See* Bus. & Prof. Code § 22945(a)(3).
[16] Pen. Code § 1546.1(c).
[17] *See* Pen. Code § 1546.1(e)(2), (g).

3) **Author's statement.** According to the author:

> As a society, we bear a collective responsibility to care for the health and safety of our citizens. That responsibility extends to private companies. Social media companies find themselves in a unique position in terms of their monopolization of communication between people of all ages. With this in mind, companies and sites should be more proactive and aggressive in their enforcement of their terms of service, especially when it comes to prohibitions on drug sales.
>
> SB 918 will help stop drug traffickers from using social media to distribute drugs and prevent unintentional overdoses. SB 918 will achieve this by requiring social media platforms to have a telephone hotline available at all times for law enforcement agencies to be able to timely request information. Social media sites must be more proactive and communicative in their enforcement of their terms of service, which should include being responsive to law enforcement agencies investigating crimes on their platforms. SB 918 also compels social media platforms to immediately comply with a search warrant provided by a law enforcement agency if the subject of the search warrant has an account on the social media platform.

4) **What this bill does.** This bill seeks to make social media platforms with over 1 million discrete monthly active users more responsive to law enforcement. The bill does so in two ways.

First, the bill requires platforms, at all times, to make available by telephone to a California law enforcement agency a law enforcement liaison—a natural person who serves as the point of contact with law enforcement agencies—for the purpose of receiving, and responding to, requests for information. This provision is similar to the existing provision in CalECPA to maintain a law enforcement contact process that must do all of the following, at a minimum:

- Provide a specific contact mechanism for law enforcement personnel.
- Provide continual availability of the law enforcement contact process.
- Provide a method to provide status updates to a requesting law enforcement agency on a request for assistance.[18]

Second, unless another law requires otherwise, the bill requires platforms to comply with a search warrant within 72 hours if the search warrant is provided to the social media platform by a law enforcement agency and the subject of the search warrant is information associated with an account on the social media platform and that information is controlled by a user of the social media platform.

In light of opposition and stakeholder concerns, the author recently amended the bill to grant more flexibility in a platform's response to a warrant. A primary concern for opposition was the requirement in the prior version of the bill that platforms "immediately comply" with a search warrant. In response, the author changed this to give the platform 72 hours to comply. Additionally, the author amended the bill to provide that a court may reasonably extend the time required to comply with a search warrant if the court makes a written finding that the social media platform has shown good cause for the extension and has shown that it would not cause an adverse result. "Adverse result" for these purposes is defined as: danger to the life or physical

---

[18] Pen. Code § 1524.4(a), (b).

safety of an individual; a flight from prosecution; the destruction of or tampering with evidence; the intimidation of potential witnesses; or serious jeopardy to an investigation or undue delay of a trial.[19] In line with other provisions relating to warrants, this expressly clarifies that platforms may seek judicial oversight in responding to warrants that may be infeasible, vague, or unduly broad in scope.

5) **Amendments.** Section 1524.4 of the Penal Code requires a provider of an electronic communication service subject to CalECPA to maintain a law enforcement contact process similar to the liaison process required under this bill. Consistent with suggestions from stakeholders, the author has agreed to amendments that would incorporate these provisions. The amendments are as follows:

[. . .]

22946.1. (a) A social media platform shall ***maintain a law enforcement contact process that does all of the following:***

(A) Makes available a staffed hotline for law enforcement personnel for purposes of receiving, and responding to, requests for information.

(B) Provides continual availability of the law enforcement contact process.

(C) Includes a method to provide status updates to a requesting law enforcement agency on a request for information or a warrant provided pursuant to subdivision (b). ~~, at all times, make available by telephone to a law enforcement agency a law enforcement liaison for the purpose of receiving, and responding to, requests for information.~~

[. . .]

6) **Related legislation.** SB 60 (Umberg; Ch. 698, Stats. 2023) authorizes a person to seek an order requiring a social media platform to remove content that includes an offer to transport, sell, furnish, administer, or give away a controlled substance in violation of specified law.

AB 1027 (Petrie-Norris; Ch. 824, Stats. 2023) required social media platforms to include in their already-required policy statements a general description of the platform's policy on the retention of electronic communication information and sharing of specified information; and added to existing terms of service reporting requirements an obligation to disclose policies on addressing the distribution of controlled substances on the platform and data on the number of times such content was flagged and actioned.

AB 1628 (Ramos; Ch. 432, Stats. 2022) requires, until January 1, 2028, a social media company to create and publicly post a policy statement that includes, among other things, the platform's policy on the use of the platform to illegally distribute a controlled substance.

SB 1056 (Umberg; Ch. 881, Stats. 2022) required social media platforms, as defined, to clearly and conspicuously state whether they have mechanisms for reporting violent posts, as defined;

---

[19] Pen. Code § 1524.2(a)(2).

and allows a person who is the target, or who believes they are the target, of a violent post to seek an injunction to have the violent post removed.

SB 1121 (Leno; Ch. 541, Stats. 2016) modified CalECPA to authorize a government entity to access, without a warrant, the location or phone number of an electronic device used to call 911; allowed a government entity to retain voluntarily received electronic communication information beyond 90 days if the service provider or subscriber is or discloses information to, a correctional or detention facility; and excluded driver's licenses and other identification cards from its provisions.

AB 1993 (Irwin; Ch. 514, Stats. 2016) required certain technology companies covered under CalECPA to maintain a law enforcement contact process to coordinate with law enforcement agency investigations, as specified.

SB 178 (Leno; Ch. 651, Stats. 2015) enacted CalECPA, which establishes the procedures for obtaining information from an electronic communication service provider about a user of the service.

ARGUMENTS IN SUPPORT: A coalition of law enforcement agencies writes:

> . . . [F]entanyl is now the number one cause of death for people ages 18-45. The drug overdose epidemic has continued to worsen in the United States over the last several years as synthetic opioids, particularly illicit fentanyl, enter the market. Of specific concern is the primary method through which many individuals, especially teenagers, unlawfully purchase illicit fentanyl and other controlled substances—social media.
>
> Drug traffickers solicit customers via social media platforms such as Snapchat, Facebook, Instagram, Twitter, TikTok, and YouTube. In many cases, traffickers and buyers alike use social media features such as temporary or disappearing posts that help conceal their activities.
>
> News outlets have reported that there are known drug dealers using social media to sell drugs. However, even after law enforcement and concerned users make the platform aware, platforms are slow to respond in removing accounts.
>
> SB 918 will require social media to cooperate with law enforcement and work together to prevent harms like unintentional overdoses.

ARGUMENTS IN OPPOSITION: ACLU California Action, writing about a prior version of the bill that would have required platforms to "immediately" comply with a warrant, stated:

> People of all ages rely on social-media platforms for everything from accessing information and connecting with others, to paying for goods, using transportation, getting work done, and speaking out about issues of the day. Without adequate privacy protections, those platforms can be co-opted to surveil us online and intrude into our private lives. The vast stores of information social-media platforms hold about people—from their posts to their networks of associations and relationships to their private messages—are subject to some of the strongest privacy protections under the law, and for good reason.

We are concerned that SB 918 would undermine these protections, and potentially violate foundational constitutional privacy safeguards. Most concerning is SB 918's requirement that social media platforms "immediately comply" when they receive a search warrant relating to an account held by a user of the platform. Section 22946.1(b). While SB 918 does not define "immediately," its dictionary definition is "without delay."

Put simply, ensuring that people's rights are protected takes time. When a platform receives a search warrant, they must carefully review the warrant, perform a reasonable search for responsive material, and understand the scope of those records in order to determine whether the warrant is tailored as the law requires. The platform should also notify the target of the search, to allow the person to take action to protect their rights. The platform might also communicate with law enforcement about the scope and breadth of the warrant and seek and obtain legal advice from counsel regarding the breadth of the search warrant. It might also be necessary for the platform or the target of the warrant to seek relief in court to void or modify the warrant. There is no way for platforms to comply with a search warrant "immediately" without undermining people's statutory and constitutional rights.

REGISTERED SUPPORT / OPPOSITION:

Support

Peace Officers Research Association of California (PORAC)

Support If Amended

California District Attorneys Association

Opposition

ACLU California Action
Electronic Frontier Foundation
Technet-technology Network

Analysis Prepared by: Josh Tosney / P. & C.P. / (916) 319-2200