Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

THIRD READING

Bill No: SB 1000
Author: Ashby (D) and Rubio (D)
Amended: 5/16/24
Vote: 21

SENATE JUDICIARY COMMITTEE: 11-0, 4/23/24
AYES: Umberg, Wilk, Allen, Ashby, Caballero, Durazo, Gonzalez, Laird, Min, Niello, Wahab

SENATE APPROPRIATIONS COMMITTEE: 7-0, 5/16/24
AYES: Caballero, Jones, Ashby, Becker, Bradford, Seyarto, Wahab

SUBJECT: Connected devices: device protection requests

SOURCE: Author

DIGEST: This bill requires account managers of connected devices to deny account access to a person in response to a "device protection request" when the requester submits specified documentation, including verification that they are in exclusive legal possession or control of the connected device.

ANALYSIS:

Existing law:

1) Criminalizes conduct amounting to false imprisonment and human trafficking. (Pen. Code § 236 et seq.)

2) Criminalizes conduct amounting to rape, duress, and other unlawful sexual conduct, including prostitution and abduction. (Pen. Code § 261 et seq.)

3) Authorizes a court to issue an ex parte order enjoining a party from molesting, attacking, striking, stalking, threatening, sexually assaulting, battering, credibly impersonating, falsely personating, harassing, telephoning, including, but not limited to, making annoying telephone calls,

destroying personal property, contacting, either directly or indirectly, by mail or otherwise, coming within a specified distance of, or disturbing the peace of the other party. "Disturbing the peace of the other party" refers to conduct that, based on the totality of the circumstances, destroys the mental or emotional calm of the other party. This conduct may be committed directly or indirectly, including through the use of a third party, and by any method or through any means including, but not limited to, telephone, online accounts, text messages, internet-connected devices, or other electronic technologies. (Fam. Code § 6320.)

4) Authorizes an adult person, or a parent or guardian on behalf of a minor or an incapacitated person, to apply to participate in the Safe at Home program by stating that they are a victim of specified conduct, including domestic violence, sexual assault, stalking, human trafficking, child abduction, or elder or dependent adult abuse, or is a household member of a victim, designating the Secretary of State (SOS) as the agent for service of process and receipt of mail, and providing the SOS with any address they wish to be kept confidential. (Gov't Code § 6206(a).)

This bill:

1) Defines the relevant terms, including:
    a) "Account manager" means a person or entity that provides an individual an internet-based or app-based user account, or a third party that manages those user accounts on behalf of that person or entity, that has authority to make decisions regarding user access to those user accounts.
    b) "Connected device" means any device, or other physical object that is capable of connecting to the internet, directly or indirectly, and that is assigned an internet protocol (IP) or Bluetooth address.
    c) "Device access" means the ability to remotely control a connected device, remotely change the characteristics of a connected device, or remotely view or manipulate data collected by or through a connected device, by accessing a user account or accounts associated with the connected device. Acts that require device access include, but are not limited to, remotely manipulating an audio system, security system, light fixture, or other home appliance or fixture and accessing camera or location data from a motor vehicle.

2) Requires an account manager to do the following:

a) Deny a person's device access, as identified in a qualifying device protection request, within two business days.
b) Offer the ability to submit a device protection request through secure remote means that are easily navigable. An account manager shall not require a specific form of documentation to submit a device protection request.
c) Make information about these options publicly available on their website and mobile application, if applicable.

3) Requires a device protection request to include all of the following:
   a) Verification of the requester's exclusive legal possession or control of the connected device, including, but not limited to, a dissolution decree, temporary restraining order, protective order, domestic violence restraining order, or other document indicating the requester's exclusive use care, possession, or control of the connected device.
   b) Identification of the connected device or devices.
   c) Identification of the person that the requester seeks to deny device access.

4) Prohibits an account manager from conditioning a device protection request upon any limitation or requirement, including:
   a) Payment of a fee, penalty, or other charge.
   b) Approval of the device protection request by any other person who is not a legal owner or in legal possession of the device.
   c) A prohibition or limitation on the ability to deny device access as a result of arrears accrued by the account or associated with the connected device.
   d) An increase in the rate charged for the account if any subscription fee or other recurring charge for account access applies.
   e) Any other limitation or requirement.

5) Provides that an account manager, and other specified agents or employees, shall treat any information submitted as confidential and securely dispose of the information not later than 90 days after receiving the information. This does not prohibit the maintenance, for longer than the period specified, of a record that verifies that a requester fulfilled the conditions of a request.

6) Makes any waiver of these provisions void and unenforceable. The duties and obligations imposed are cumulative with any other duties or obligations

imposed under other law, and shall not be construed to relieve any party from any duties or obligations imposed under other law. The remedies or penalties provided by this chapter are cumulative to each other and to the remedies or penalties available under all other laws of the state.

7) Includes a severability clause.

8) Makes these provisions operative on January 1, 2026.

9) Amends the definition of "disturbing the peace of the other party" for purposes of securing a restraining order to include conduct committed through a connected device.

Background

Domestic violence can take many forms, but generally involve a pattern of behaviors by an abuser to gain and maintain power and control over a victim. This can involve emotional abuse, intimidation, economic abuse, coercion and threats, and physical or sexual violence. Abusers can assert control over economic resources, children, and modes of transportation. Escaping domestic violence is often harrowing and beset by fear of being caught or found by the abuser.

With the near ubiquitous nature of connected devices and attendant tracking mechanisms, a new tool for abusers to maintain power and control has caused alarm among survivors and advocates. Research and reporting finds that abusers are increasingly using connected devices in homes and other consumer products to harass and terrify their victims even after they have managed to escape.

This bill provides a mechanism for submitting a "device protection request" to deny device access to connected devices to other persons. However, a person needs to verify that they have exclusive legal possession or control of the device. The bill also does not require the account manager to notify the requester when the account manager intends to notify the person being denied access. There is no mechanism for enforcement identified in the bill. This bill is author-sponsored. The bill is supported by Oakland Privacy and Alliance for Hope International. No timely opposition was received.

Comment

According to the author:

SB 1000 requires companies to swiftly cut off access to shared accounts, applications, and devices, offering immediate protections for domestic violence victims when proper documentation is provided. This is a necessary measure that addresses the increasingly prevalent problem of digital abuse and control in domestic violence cases.

Domestic violence organizations continue to raise concerns about the increasing number of abuse cases related to internet-connected devices and shared accounts. Victims report escalating issues of virtual abuse, including loss of autonomy over everyday household items such as doors, speakers, thermostats, lights, cameras, and even vehicles. While modern technology offers convenience and connectivity, it has unfortunately become a tool for perpetrators to exert control over their victims remotely.

SB 1000 addresses the urgent need to stop this alarming new trend. This bill empowers victims and provides a crucial layer of protection. It ensures that California law evolves alongside technological advancements, empowering and safeguarding victims of domestic violence.

FISCAL EFFECT: Appropriation: No Fiscal Com.: No Local: No

According to the Senate Appropriations Committee:

Unknown, potentially significant workload cost pressures (General Fund, Trial Court Trust Fund) to the courts.

SUPPORT: (Verified 5/17/24)

Alliance for Hope International
Oakland Privacy

OPPOSITION: (Verified 5/17/24)

None received

ARGUMENTS IN SUPPORT: Oakland Privacy states:

Modern technology has enabled perpetrators to facilitate abuse in a myriad of ways, from a distance and with little effort or cost. SB 1000 affords victims of domestic violence with legal protections to break from the grips of an abuser who utilizes connected devices (IoT

devices) - an insidious exploitation of privacy - to harass, intimidate, monitor or control their victims, and endanger their physical safety.

Prepared by: Christian Kurpiewski / JUD. / (916) 651-4113
5/18/24 16:20:46

****** END ******