SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2023-2024 Regular Session

SB 1000 (Ashby)
Version: March 13, 2024
Hearing Date: April 23, 2024
Fiscal: Yes
Urgency: No
CK

SUBJECT

Connected devices: access: abusers

DIGEST

This bill authorizes victims of "covered acts," as defined, to submit a "device protection request," to with specified documentation, to deny abusers access to connected devices.

EXECUTIVE SUMMARY

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 survivors of "covered acts" to regain control of these devices. These acts include false imprisonment, human trafficking, and other sexual crimes. With verification that a covered act has been committed against the victim and verification of the device as the victim's or in the victim's exclusive control or fixed within their home or vehicle, account managers, those in control of device access, must grant a device protection request, essentially denying the abuser access to the connected device. This bill is author-sponsored. The bill is supported by Oakland Privacy and Alliance for Hope International. No timely opposition was received.

PROPOSED CHANGES TO THE LAW

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) "Abuser" means an individual who has committed or allegedly committed a covered act against a victim or an individual in the victim's care.
    b) "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.

c) "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.
d) "Covered act" means conduct that constitutes any of the following, but does not require a conviction or any other court determination:
    i. A crime described in Penal Code Section 236 et seq. or Section 261 et seq.
    ii. An act under federal law, tribal law, or the Uniform Code of Military Justice that is similar to an offense described above.
e) "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.
f) "Victim" means an individual against whom a covered act has been committed or allegedly committed or who cares for another individual against whom a covered act has been committed or allegedly committed, provided that the individual providing care did not commit or allegedly commit the covered act.

2) Authorizes a victim seeking to deny an abuser "device access" to submit to the account manager a device protection request that includes both of the following:
    a) A verification that the abuser has committed or allegedly committed a covered act against the victim or an individual in the victim's care, by providing either of the following:
        i. A copy of a signed affidavit from a licensed medical or mental health care provider, licensed military medical or mental health care provider, licensed social worker, victim services provider, or licensed military victim services provider, or an employee of a court, acting within the scope of that person's employment.
        ii. A copy of a police report, statements provided by police, including military police, to magistrates or judges, charging documents, protective or restraining orders, military protective orders, or any other official record that documents the covered act.
    b) Identification of the connected device or devices that the victim seeks to deny the abuser access to, and a statement that the connected device or devices are at least one of the following:
        i. Solely owned by the victim or an individual in the victim's care.
        ii. Legally under the sole possession or control of the victim or an individual in the victim's care.

iii. A fixture or feature within a dwelling or motor vehicle that the abuser may not legally enter or use.

3) Requires an account manager to do the following:
   a) Deny device access to an abuser, as identified in the request, within two business days.
   b) Offer a victim 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.
   d) Notify the victim of both of the following:
      i. The date on which they intend to give any formal notice to the abuser that has had their device access denied.
      ii. That the account manager may contact the victim, or designated representative, to confirm that the abuser's device access is denied, or to notify the victim that the device protection request is incomplete.

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 person who has device access that is not the victim.
   c) A prohibition or limitation on the ability to deny device access to an abuser 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 by a victim 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 victim fulfilled the conditions of a request.

6) Subjects account managers in knowing violation of these provisions, and abusers that knowingly maintain device access despite access denial, to civil actions brought by any person injured by the violation or in the name of the people of the State of California by the Attorney General or by any district attorney. The court may award injunctive relief, and any other relief necessary to prevent a violation. Those in knowing violation are also liable for civil penalties not to

exceed $2,500 for each connected device. If the action is brought by the Attorney General, the penalty shall be deposited into the General Fund. If the action is brought by a district attorney, the penalty shall be paid to the treasurer of the county in which the judgment was entered.

7) 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.

8) Includes a severability clause.

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

10) 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.

COMMENTS

1. Technology as a means of abusive control

Smart technology has revolutionized everything in our lives, from our phones, to our cars, and even our thermostats. However, while remote access to many of these connected devices provides unparalleled convenience, it also has increasingly been used a weapon by abusers to maintain control over their victims. One study of the use of device tracking states the scope of the issue:

> Intimate partner violence, abuse, and harassment is routinely linked with efforts to monitor and control a targeted person. As new technologies have seeped into everyday life, aggressors have adopted and repurposed them to terrorize, control, and manipulate their current and former partners. When National Public Radio conducted a survey of 72 domestic violence shelters in the United States, they found that 85% of domestic violence workers assisted victims whose abuser tracked them using GPS. The US-based National Network to End Domestic Violence found that 71% of domestic abusers monitor survivors' computer activities, while 54% tracked survivors' cell phones with stalkerware. In Australia, the Domestic Violence Resources Centre Victoria conducted a survey in 2013 that found that 82% of victims reported abuse via smartphones and 74% of practitioners reported tracking via applications as often occurring amongst their client base. In Canada, a national survey of anti-violence

> support workers from 2012 found that 98% of perpetrators used technology to intimidate or threaten their victims, that 72% of perpetrators had hacked the email and social media accounts of the women and girls that they targeted, and that a further 61% had hacked into computers to monitor online activities and extract information. An additional 31% installed computer monitoring software or hardware on their target's computer.[1]

Given the explosion of connected devices in our homes, the problem has only gotten worse as even when survivors are able to physically escape domestic violence, the abuse continues:

> Connected home devices have increasingly cropped up in domestic abuse cases over the past year, according to those working with victims of domestic violence. Those at help lines said more people were calling in the last 12 months about losing control of Wi-Fi-enabled doors, speakers, thermostats, lights and cameras. Lawyers also said they were wrangling with how to add language to restraining orders to cover smart home technology.
>
> Muneerah Budhwani, who takes calls at the National Domestic Violence Hotline, said she started hearing stories about smart homes in abuse situations last winter. "Callers have said the abusers were monitoring and controlling them remotely through the smart home appliances and the smart home system," she said.
>
> Graciela Rodriguez, who runs a 30-bed emergency shelter at the Center for Domestic Peace in San Rafael, Calif., said some people had recently come in with tales of "the crazy-making things" like thermostats suddenly kicking up to 100 degrees or smart speakers turning on blasting music.
>
> "They feel like they're losing control of their home," she said. "After they spend a few days here, they realize they were being abused."
>
> Smart home technology can be easily harnessed for misuse for several reasons. Tools like connected in-home security cameras are relatively inexpensive — some retail for $40 — and are straightforward to install. Usually, one person in a relationship takes charge of putting in the technology, knows how it works and has all the passwords. This gives that person the power to turn the technology against the other person.

---

[1] Christopher Parsons, et al., *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* (June 12, 2019) Citizen Lab, https://citizenlab.ca/docs/stalkerware-holistic.pdf. All internet citations are current as of April 9, 2024.

> . . .
>
> Each said the use of internet-connected devices by their abusers was invasive — one called it a form of "jungle warfare" because it was hard to know where the attacks were coming from. They also described it as an asymmetry of power because their partners had control over the technology — and by extension, over them.
>
> One of the women, a doctor in Silicon Valley, said her husband, an engineer, "controls the thermostat. He controls the lights. He controls the music." She said, "Abusive relationships are about power and control, and he uses technology."[2]

The concern is that often the abuser is the named account holder and likely installed and has continued access to the device even after the survivor has escaped the situation or even secured a restraining order. Advocates argue updates to the applicable laws need to be updated:

> Legal recourse may be limited. Abusers have learned to use smart home technology to further their power and control in ways that often fall outside existing criminal laws, Ms. Becker said. In some cases, she said, if an abuser circulates video taken by a connected indoor security camera, it could violate some states' revenge porn laws, which aim to stop a former partner from sharing intimate photographs and videos online.
>
> Advocates are beginning to educate emergency responders that when people get restraining orders, they need to ask the judge to include all smart home device accounts known and unknown to victims. Many people do not know to ask about this yet, Ms. Becker said. But even if people get restraining orders, remotely changing the temperature in a house or suddenly turning on the TV or lights may not contravene a no-contact order, she said.[3]

2. <u>Allowing survivors of violence to reclaim control</u>

This bill seeks to provide a tool for survivors to reclaim control of their lives by regaining control of the connected devices in their homes and lives. This bill requires "account managers," those that control user access to internet-based or app-based accounts in connection with connected devices, to deny access to such devices to an abuser within two business days of receiving a "device protection request."

---

[2] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse* (June 23, 2018) The New York Times, https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.
[3] *Ibid*.

To initiate such requests, a victim must provide two pieces of documentation. The first is a verification that the abuser has committed or allegedly committed a "covered act" against the victim or an individual in the victim's care. Covered acts include specified crimes, or equivalent offenses, including false imprisonment, human trafficking, or sexual crimes.[4]

This verification can take the form of a signed affidavit from a specified provider, such as a licensed social worker, or a court employee, or a police report, or other court documentation, including charging documents, restraining orders, or other official records documenting the covered act.

Second, the victim must provide identification of the relevant connected device and a statement that the connected device is one of the following:

- Solely owned by the victim or an individual in the victim's care.
- Legally under the sole possession or control of the victim or an individual in the victim's care.
- A fixture or feature within a dwelling or motor vehicle that the abuser may not legally enter or use.

Once documentation is provided, the "account manager," the person or entity that provides an individual an internet-based or app-based user account, or a third party that manages them, that has authority to make decisions regarding user access to those user accounts, must deny device access to an abuser within two business days of receiving the request.

No specific piece of documentation can be required and no limitations or additional requirements can condition granting the request. There is also no requirement that the conduct result in a criminal conviction.

The bill also amends the definition of "disturbing the peace of the other party" for purposes of being issued a restraining order to explicitly include conduct committed through connected devices.

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.

---

[4] The reference in this definition to Title 9 (commencing with Section 261) of Part 1 of the Penal Code is broader than was contemplated by the author. For clarity, the author has agreed to amendments to specify the offenses within that Title that will amount to a "covered act."

> 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.

Account managers that knowingly violate the law can be subject to civil actions brought by those injured or the Attorney General or a district attorney. Courts can grant injunctive relief and civil penalties not to exceed $2,500 per device for knowing violations. Such relief can also be awarded against an abuser that maintain or exercises device access despite having their access denied pursuant to a device protection request.

Writing 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.

SUPPORT

Alliance for Hope International
Oakland Privacy

OPPOSITION

None received

RELATED LEGISLATION

Pending Legislation: SB 1394 (Min, 2024) requires a vehicle manufacturer to terminate a person's access to remote vehicle technology, as defined, upon a completed request from a driver who establishes proof of legal possession of the vehicle or a domestic

violence restraining order naming the person whose access is sought to be terminated. SB 1394 prohibits a vehicle manufacturer from charging a fee to a driver for completing their request requires a vehicle manufacturer, among other things, to establish an efficient, secure, and user-friendly online submission process for requests related to terminating a person's access to remote vehicle technology, as specified, and to ensure that all personal information provided during this process is handled with the utmost security and privacy, adhering to relevant data protection laws and regulations. A vehicle manufacturer is required to provide a notification inside of a vehicle that is installed with remote vehicle technology that shows if the remote vehicle technology is being used. SB 1394 is currently in this Committee.

Prior Legislation: SB 975 (Min, Ch. 989, Stats. 2022) created a non-judicial process for addressing a debt incurred in the name of a debtor through duress, intimidation, threat, force, or fraud of the debtor's resources or personal information for personal gain. This bill also creates a cause of action through which a debtor can enjoin a creditor from holding the debtor personally liable for such "coerced debts" and a cause of action against the perpetrator in favor of the claimant.

****