SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

SB 50 (Ashby)
Version: December 16, 2024
Hearing Date: April 1, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

Connected devices: device protection requests

DIGEST

This bill requires account managers of connected devices to terminate or disable perpetrators' access to such devices upon receiving a "device protection request" with specified documentation from survivors of "covered acts," as defined.

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. Upon receipt of specified documentation, including verification that a covered act has allegedly been committed against the survivor and verification of the survivor's exclusive possession or control of the device, account managers, those in control of device access, must grant a device protection request, essentially denying the perpetrator access to the connected device. This bill is author-sponsored and supported by several groups, including Oakland Privacy. No timely opposition has been 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) Requires an account manager, commencing no later than two business days after receiving a device protection request from a survivor, to terminate or disable a connected device or account access to a perpetrator, as identified in the request.

2) Provides that in the case of a survivor seeking to deny a perpetrator device or account access, the survivor shall submit to the account manager a device protection request that includes all of the following:
    a) A verification that the perpetrator has committed or allegedly committed a covered act against the survivor or an individual in the survivor'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, a temporary restraining order, or one of specified protective orders.
ii. A copy of a police report, statements provided by 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) Verification of the survivor'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 survivor's exclusive use care, possession, or control of the connected device.
c) Identification of the connected device or devices.
d) Identification of the person that the requester seeks to deny device or account access.

3) Requires an account manager to offer a survivor the ability to submit a device protection request through secure remote means that are easily navigable. Except as specified, an account manager shall not require a specific form of documentation to submit a device protection request.

4) Requires an account manager to make information about the options and process publicly available on the internet website and mobile application, if applicable, of the account manager.

5) Requires an account manager to notify the survivor of both of the following:
a) The date on which the account manager intends to give any formal notice to the perpetrator that has had their device or account access denied.
b) That the account manager may contact the survivor, or designated representative of the survivor, to confirm that the perpetrator's device or account access is denied, or to notify the survivor that the device protection request is incomplete.

6) Prohibits an account manager from conditioning a device protection request upon specified conditions, including payment or any other limitations or requirements not specifically listed.

7) Requires an account manager, as specified, to treat any information submitted by a survivor as confidential and to securely dispose of the information not later than 90 days after receiving it. This shall not be construed to prohibit an account manager from maintaining, for longer than the period specified, a record that verifies that a survivor fulfilled the conditions of a device protection request.

8) 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 address or Bluetooth address or enables a person to remotely obtain data from or send commands to a connected device or account, which may be accomplished through a software application that is designed to be operated on a mobile device, computer, or other technology.
    c) "Perpetrator" means an individual who has committed or allegedly committed a covered act against a survivor or an individual under the care of a survivor.
    d) "Survivor" means an individual who has had a covered act committed, or allegedly committed, against the individual, 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.
    e) "User account or account" means an account or other means by which a person enrolls in or obtains access to a connected device or online service.

9) Deems a perpetrator that maintains or exercises device or account access, including by disturbing the peace of the other party, as described in subdivision (c) of Section 6320 of the Family Code, despite having their device or account access denied in violation hereof.

10) Authorizes actions to be brought by any person injured by a violation or in the name of the people of the State of California by the Attorney General, a district attorney, county counsel, a city attorney, or a city prosecutor.

11) Authorizes a court to enjoin a person or entity who engages, has engaged, or proposes to engage in a violation hereof. The court may make any orders or judgments as may be necessary to prevent a violation of this chapter.

12) Provides that a person or entity who engages, has engaged, or proposes to engage in a violation shall be liable for a civil penalty not to exceed $2,500 for each connected device in violation, to be distributed as specified.

13) Prohibits any waiver of these provisions and clarifies that 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 are

cumulative to each other and to the remedies or penalties available under all other laws of the state.

14) Exempts any entity that is subject to the federal Safe Connections Act of 2022 or regulations of the Federal Communications Commission.

15) Includes a severability clause.

16) 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, such connectivity has also increasingly been used as 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; 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.
> . . .
>
> 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

[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 March 14, 2025.

> 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 that 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. Allowing survivors of violence to reclaim control

Last year, SB 1394 (Min, Ch. 655, Stats. 2024) addressed these issues with respect to connected vehicles. It required connected vehicles to clearly indicate when connected service and location access has been accessed and required providers to establish mechanisms for disabling remote vehicle access. SB 1000 (Ashby, 2024) also sought to address these issues with connected devices. This bill largely mirrors that effort.

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

---

[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*.

perpetrators of specified crimes within two business days of receiving a "device protection request."

To initiate such requests, a survivor must provide specified documentation. This includes verification that the perpetrator has committed or allegedly committed a "covered act" against the survivor or an individual in the survivor's care. Covered acts include specified crimes, or equivalent offenses, including false imprisonment, human trafficking, or sexual crimes. 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.

The survivor must also provide identification of the person the survivor seeks to deny access to and identification of the relevant connected device. The request must also include verification of the survivor'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 survivor's exclusive use care, possession, or control of the connected device

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, must deny device access to a perpetrator 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 50 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, and cameras. While modern technology offers convenience and connectivity, it has unfortunately become a tool for perpetrators to exert control over their victims remotely.
>
> SB 50 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 violate the law can be subject to civil actions brought by those injured or by specified public prosecutors. Courts can grant injunctive relief and civil penalties not to exceed $2,500 per device. Such relief can also be awarded against a perpetrator that maintains or exercises device access despite having their access denied pursuant to a device protection request.

Writing in support, Oakland Privacy states:

> IoT devices' come into people's homes with the benign appeal of improving lives but these devices can easily and covertly be weaponized to surveil without an individual's consent or knowledge. Moreover, an abuser may even coerce a victim into being surveilled and to voluntarily give up their personal privacy in an abusive relationship. Protections should shift the burden from victims that require them to be technologically savvy, or to avoid using technology – in which there are probably instances that victims are unaware of connected devices - to general privacy protection measures by design such as data minimization, storage and sharing to increase the overall safety of IOT devices. In addition to regulation like SB 50, technology developers should take into account the privacy of all users - active and passive - of their devices and recognize the fluid relationships and even enmeshment of various people interacting with their devices. Enacting proactive measures will help curb victim-blaming perspectives, and will shift some of the burden from survivors to those building and deploying these technologies - by fostering tech that is designed with safety protections from the outset. An easily implementable requirement would be to have companies add information and warnings about potential misuse in owners manuals, as is done for Apple Air Tags.
>
> This bill will help with reducing public safety interventions in domestic violence situations and potentially de-escalate potential acts of conflict, confrontation and violence.

SUPPORT

3Strands Global Foundation
Alliance for HOPE International
Oakland Privacy
Sacramento Regional Family Justice Center
San Francisco Safehouse

OPPOSITION

None received

RELATED LEGISLATION

Pending Legislation: None known.

Prior Legislation:

SB 1000 (Ashby, 2024) *See* Comment 2. SB 1000 died in the Assembly Appropriations Committee.

SB 1394 (Min, Ch. 655, Stats. 2024) *See* Comment 2.

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.

****