Date of Hearing: June 24, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 50 (Ashby) – As Amended May 23, 2025

SENATE VOTE: 38-0

SUBJECT: Connected devices: device protection requests

SYNOPSIS

Alongside advances in technology are parallel advances in the dangers for women[1] who are or were in relationships with violent male perpetrators. The technological advances have brought new and inventive ways for men to abuse and torture the women in their lives. In fact, the federal government now recognizes technology-enabled abuse as a form of domestic abuse. The Office of Violence against Women, housed in the US Department of Justice, defines technological abuse as:

> *An act or pattern of behavior that is intended to harm, threaten, control, stalk, harass, impersonate, exploit, extort, or monitor another person that occurs using any form of technology, including but not limited to: internet enabled devices, online spaces and platforms, computers, mobile devices, cameras and imaging programs, apps, location tracking devices, or communication technologies, or any other emerging technologies.*

As internet connected devices have become even more commonplace, domestic violence shelters have reported growing numbers of calls from women who are convinced they are going crazy. They are reporting that their air-conditioning systems were turning on and off without them touching them, that the code numbers on front door digital locks changed daily and they could not figure out why, or that they kept hearing the doorbell ring, but no one was ever there. Abusers not only use connected devices to terrorize their victims, but also to stalk and surveil their every move. As new technology seeps into everyday life, abusers have adopted and repurposed it to terrorize and control their current and former partners.

This bill is substantially similar to the federal Safe Connections Act (SCA) of 2022 (PL 117-223). The SCA requires mobile service providers to separate the line of a survivor of domestic violence (and other related crimes and abuse) and any individuals in the care of the survivor from a mobile service contract shared with an abuser within two business days after receiving a request from the survivor. Like the SCA, this bill requires that within two business days of receiving a

---

[1] While both women and men report instances of intimate partner violence (IPV), researchers have found that women experience a greater range and severity of IPV at the hands of male partners, while IPV acts against men comprise primarily low severity acts perpetrated by their female partners. As such, when discussing violent, prolonged, and frequent IPV, this analysis uses the most likely gender of the survivor and the perpetrator to clarify that IPV is primarily a gendered issue and men are the most likely perpetrators of violence against their partners or former partners. For a survey of the literature, see *Evidence of Gender Asymmetry in Intimate Partner Violence Experience at the Population-Level* by Janet Fanslow, et al (Apr. 9, 2023) https://pmc.ncbi.nlm.nih.gov/articles/PMC10668541/.

device protection request that the account manager for the device deny access to any person listed in the protection request.

The Committee amendments prohibit account managers from notifying perpetrators about being removed from the account.

The bill is co-sponsored by 3 Strands Global Foundation and Alliance for Hope International. There is no registered opposition. If this bill passes this Committee, it will next be heard by the Judiciary Committee.

THIS BILL:

1) Requires an account manager, commencing no later than two business days after receiving a device protection request from a survivor or an "eligible organization," 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 specified information.

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.

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) "Covered act" means primarily conduct that constitutes any of the following:

i) False imprisonment.
ii) Human Trafficking.
iii) Sexual assault.
iv) Abandonment and neglect of children.
v) Spousal abuse or domestic violence.
vi) Child abduction.
vii) Bigamy
viii) Incest.
ix) Crimes against nature.
x) A sex offense.

d) "Eligible organization" may include a governmental or nongovernmental organization and means a service provider that has experience in using national or local networks to serve victims of domestic violence and experience qualifying, providing, and coordinating services for victims of domestic violence.

e) "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.

f) "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.

g) "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 defined, 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 per violation 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" under existing law for purposes of securing a restraining order to include conduct committed through a connected device.

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) Beginning July 1, 2025, for vehicles with connected vehicle service, automobile manufacturers are required to provide a process for a driver to terminate a person's access to connected vehicle service, if they receive a request from a survivor of intimate partner violence. (Veh. Code § 28200 et seq.)

4) Beginning January 1, 2028, requires a vehicle with connected vehicle service to clearly indicate to a person who is inside the vehicle when a person who is outside the vehicle has accessed either the connected vehicle service or the connected vehicle location access. (Veh. Code § 28206.)

5) Beginning January 1, 2028, automobile manufactures, for vehicle with connect services, are required to provide a mechanism within the car that can be used by a driver who is inside a vehicle to immediately disable connected vehicle location access. Prohibits the mechanism from requiring a password or account information. (Veh. Code § 28202.)

6) 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.)

7) 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. Code § 6206(a).)

8) Establishes the federal Safe Connections Act (SCA) of 2022, which requires mobile service providers to separate the line of a survivor of domestic violence (and other related crimes and abuse), and any individuals in the care of the survivor, from a mobile service contract shared with an abuser within two business days after receiving a request from the survivor. (PL 117-223.)

9) Establishes the Safe at Home (SAH) address confidentiality program in order to enable state and local agencies to both accept and respond to requests for public records without disclosing the changed name or address of a victim of domestic violence, sexual assault, or stalking. (Gov. Code § 6205 et seq.)

COMMENTS:

1) **Author's statement**. 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.

2) **Intimate Partner Violence.** Nationally, more than one-third of women will experience rape, physical violence, and/or stalking by a male intimate partner in their lifetime. Nearly 8 million women experience one or more of these abuses by a current or former male partner each year. There are nearly 90 domestic violence related killings in California each year. Of the 87 IPV

related deaths in 2020, 70 were women and 17 were men.[2] The National Domestic Violence Hotline reports that an average of 24 people per minute are victims of rape, physical violence or stalking by an intimate partner in the United States — more than 12 million women and men over the course of a single year. Almost half of all women and men in the US have experienced psychological aggression by an intimate partner in their lifetime (48.4% and 48.8%, respectively).[3]

Statistically speaking, the most dangerous place for a woman is not out in public; it is in her home. In addition, the most dangerous people for a woman are not strangers; they are the men she knows and has relationships with (e.g. current and former partners, fathers, brothers, and friends).

Adding to the risk, the most dangerous time for someone who is in a relationship with a violent abuser is when they decide to leave. According to organizations working with survivors of abuse, when someone being abused in a relationship leaves or attempts to leave, abusers often lash out in an attempt to regain control over their partner or, in some cases, resort to extreme violence, even homicide, because they feel they have nothing left to lose.[4] According to Canada's Battered Women Support Services:

> Separation is a common theme found within spousal murder-suicide where half of the cases occur after the couple have either separated (26%), were in the process of separating (9%), or had expressed a desire to separate (15%). . . . The statistics outline the reality that the most dangerous time for a survivor/victim is when she leaves the abusive partner; 77 percent of domestic violence-related homicides occur upon separation and there is a 75 percent increase of violence upon separation for at least two years.[5]

With the omnipresent nature of technology that contains remote geo-location capabilities, including location trackers, leaving an abuser becomes significantly more difficult, if the abuser has online access to the survivor's location that allows them to track the survivor's every movement.

3) **The internet of things.** The "internet of things" (IoT) refers to a network of devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data. Some examples are kitchen appliances, thermostats, door locks, smart speakers, home surveillance systems, or automated sprinklers.

Amazon describes the IoT in this way:

> The term IoT, or Internet of Things, refers to the collective network of connected devices and the technology that facilitates communication between devices and the cloud, as well as

---

[2] California Partnership to End Domestic Violence. *California Domestic Violence Fact Sheet* (2022) https://www.cpedv.org/policy-priorities.
[3] The National Domestic Violence Hotline. *Domestic Violence Statistics.* https://www.thehotline.org/stakeholders/domestic-violence-statistics/.
[4] *Will My Partner Be Violent After I Leave? How to predict violence after leaving an abuser.* DomesticShelters.org. (Mar. 24, 2017) https://www.domesticshelters.org/articles/safety-planning/will-my-partner-be-violent-after-i-leave.
[5] *Eighteen Months After Leaving Domestic Violence is Still the Most Dangerous Time*, Battered Women's Support Services (Jun. 11, 2020) https://www.bwss.org/eighteen-months-after-leaving-domestic-violence-is-still-the-most-dangerous-time/.

> between the devices themselves. Thanks to the advent of inexpensive computer chips and high bandwidth telecommunication, we now have billions of devices connected to the internet. This means everyday devices like toothbrushes, vacuums, cars, and machines can use sensors to collect data and respond intelligently to users.[6]

4) **Technology-enabled abuse.** Alongside advances in technology are parallel advances in the dangers for people who are or were in relationships with violent perpetrators. The advances have brought new and inventive ways for perpetrators to abuse and torture the people in their lives. In fact, the federal government now recognizes technological abuse as a form of domestic abuse. The Office of Violence against Women housed in the US Department of Justice defines technological abuse as:

> An act or pattern of behavior that is intended to harm, threaten, control, stalk, harass, impersonate, exploit, extort, or monitor another person that occurs using any form of technology, including but not limited to: internet enabled devices, online spaces and platforms, computers, mobile devices, cameras and imaging programs, apps, location tracking devices, or communication technologies, or any other emerging technologies.[7]

A *New York Times* article in 2018 explored the relatively new phenomenon of abuse cases that were tied to the rise of smart home technology. According to that article, domestic violence shelters were reporting calls from women who were convinced they were going crazy. They were reporting that their air-conditioning systems were turning on and off without them touching them, that the code numbers on front door digital locks changed daily and they could not figure out why, or that they kept hearing the doorbell ring, but no one was ever there. At the time, the *Times* reported:

> In more than 30 interviews with The New York Times, domestic abuse victims, their lawyers, shelter workers and emergency responders described how the technology was becoming an alarming new tool. Abusers — using apps on their smartphones, which are connected to the internet-enabled devices — would remotely control everyday objects in the home, sometimes to watch and listen, other times to scare or show power. Even after a partner had left the home, the devices often stayed and continued to be used to intimidate and confuse.[8]

In the intervening years, internet connected devices have become even more commonplace. Perpetrators not only use connected devices to terrorize their victims, but also to stalk and surveil their every move. Smart speakers can often be used to listen in on conversations in a home through an online app. Home security cameras and baby monitors can allow an abuser to watch and record their victims. Small tracking devices can be easily hidden in bags, clothing, or vehicles, allowing an abuser to monitor their victim's movements. As each new technology seeps into everyday life, abusers have adopted and repurposed them to terrorize and control their current and former partners.

---

[6] *What is IoT (Internet of Things)?* https://aws.amazon.com/what-is/iot/.
[7] Information on the types of domestic violence and the Office of Violence against Women can be found at https://www.justice.gov/ovw/domestic-violence.
[8] Bowles, Nellie. "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," *The New York Times* (Jun. 23, 2018) https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

5) **What this bill would do.** This bill is substantially similar to the federal Safe Connections Act (SCA) of 2022 (PL 117-223). The SCA requires mobile service providers to separate the line of a survivor of domestic violence (and other related crimes and abuse), and any individuals in the care of the survivor, from a mobile service contract shared with an abuser within two business days after receiving a request from the survivor. Like the SCA, within two business days of receiving a device protection request this bill requires the account manager for a connected device to deny access to any person listed in the protection request.

Specifically, this bill would require the account managers of internet connected devices to do the following:

1. Sever the perpetrator's remote access to a connected device within two business days of receiving a request from a survivor.

2. Establish an easily navigable, secure, and remote method for a survivor to submit a device protection request.

3. Provide information about the options and process for severing access to the public through their internet website and mobile application.

4. Notify the requestor of the date that the manager intends to notify the perpetrator that their access has been denied and confirmation that the perpetrator has been removed from the account.

In order to remove a perpetrator from a connected device, the survivor or their designated agent must supply the following:

1. Proof that the perpetrator has committed or allegedly committed the abuse.

2. Proof that the survivor has exclusive legal protection and control of the connected device.

3. Identification of the devices.

4. Identification of the person that the survivor wants removed from accessing the device.

6) **Prior legislation.** In 2024, three authors introduced bill that dealt with technology-enabled abuse. Two of those bills, SB 1394 (Min, Ashby, and Weber, Stats. 2024, Ch. 655) and AB 3139 (Weber, 2024) dealt exclusively with automobiles with remote vehicle technology. SB 1000 (Ashby), however, took a broader approach and included the entirety of the IoT, including automobiles. The bill passed this Committee on an 11-0 vote. In the end, the three authors joined together as authors on SB 1394. This bill is a reintroduction of SB 1000. This bill is substantially similar to that bill, with the exception of automobiles, which are no longer included.

7) **Larger policy questions.** While this bill has the potential to make a significant difference in the lives of those fleeing abusive partners, it raises larger policy considerations related to the invasive nature of technology that would benefit from additional attention. With the proliferation of surveillance and tracking technology, including built in vehicle location technology, tracking devices that can easily be concealed in a car or in someone's belongings, in home and public surveillance cameras, automated license plate recognition tools, not to mention the ability to track someone using the smartphones that are virtually universal, at what point has surveillance

gone too far? Should Californians simply accept the complete loss of privacy as people move through their lives in public and private spaces?

Much like the focus that is being placed on the impact of social media, advancement in artificial technology, and the collection and sale of personal information for profit, constant surveillance by private individuals, businesses, and government has a profound impact on Californians' lives. Rather than considering the risks of one device or technological advancement at a time, at some point, it might behoove the Legislature, and this Committee in particular, to explore the larger surveillance policy questions, including the dangers associated with the unchecked proliferation of surveillance tools and their impact on Californians' privacy rights, especially for those who are at risk of abuse.

If this bill passes this Committee, it will next be heard by the Judiciary Committee.

8) **Amendments.** Rather than notifying the survivor of the timeline for notifying the perpetrator, the Committee may wish to prohibit the device manager from notifying the perpetrator that their access has been denied. The only notification that would be required is to let the survivor know that the connection has been severed. The amendment is as follows:

> (e) An account manager shall notify the survivor or the eligible organization ~~**of both of the following:**~~
>
> ~~**(1) 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.**~~
>
> ~~**(2) That the account manager may contact the survivor or the eligible organization**~~ to confirm that the perpetrator's device or account access is denied, or to notify the survivor that the device protection request is incomplete.
>
> ***(f) If an account manager terminated a person's access to a connected device, the account manager shall not provide either of the following:***
>
> ***(1) Notice to the person whose access was terminated.***
>
> ***(2) Any data or information to the person terminated regarding the requestor, the device, or any new connected account that was generated after that person's access to the connected device was terminated.***

ARGUMENTS IN SUPPORT: Alliance for Hope International, co-sponsors of the bill, write in support:

> While technology can serve as a valuable resource for victims, it is unfortunately frequently abused by perpetrators of domestic violence. Abusers can use modern technology to monitor, harass, threaten, and violate their victims. Technology advancements and an increase in the use of technology have become troubling tools in cases of domestic violence and harassment. Perpetrators leverage apps and accounts to control everyday objects within the victims' possession. Even after the abuser has left, the connected devices and accounts often remain with a victim, continuing to be used as a means of intimidating victims.

> SB 50 is a crucial measure to protect domestic violence victims from digital abuse and control. This bill will prevent abusers from using, controlling, or remotely harassing their victims when instances of abuse are reported by a victim – ensuring California law continues to empower and protect victims even as technology advances.

Also writing in support, co-sponsor 3 Strands Global Foundation notes the importance of this bill for people who are survivors of human trafficking:

> We understand the dangers of how traffickers use technology to maintain control over their victims, restricting their movements, monitoring their communications, and instilling fear. The ability to remotely control smart home devices, track locations via connected accounts, and interfere with access to essential services has created a dangerous digital landscape for survivors seeking freedom and safety. Senate Bill 50 acknowledges these threats and takes concrete steps to empower survivors by allowing them to cut off their abusers' access to connected devices within a reasonable timeframe.
>
> This legislation is particularly crucial for survivors of human trafficking, who often experience coercive control that extends beyond physical abuse and into the digital sphere. By ensuring that survivors can swiftly disable their traffickers' access to smart devices and accounts, SB 50 provides an essential safeguard that will help them regain their independence and rebuild their lives. Furthermore, by holding account managers accountable for implementing these protections, the bill ensures that survivors are not left navigating this complex process alone.
>
> We commend the bill's inclusion of clear guidelines for account managers, its confidentiality protections, and its enforcement provisions. These elements will provide survivors with the security and support they need to escape their abusers and prevent further victimization.

REGISTERED SUPPORT / OPPOSITION:

Support

3strands Global Foundation (Co-Sponsor)
Alliance for Hope International (Co-Sponsor)
California District Attorneys Association
Oakland Privacy
Sacramento Regional Family Justice Center (SRFJS)
San Francisco Safehouse
Secure Justice
Weave

Opposition

None on file.

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200