Date of Hearing: July 15, 2025

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
SB 50 (Ashby) – As Amended July 9, 2025

PROPOSED CONSENT

SENATE VOTE: 38-0

SUBJECT: CONNECTED DEVICES: DEVICE PROTECTION REQUESTS

KEY ISSUE: SHOULD THE LEGISLATURE CREATE A PROCESS BY WHICH SURVIVORS OF DOMESTIC VIOLENCE CAN TERMINATE AN ABUSER'S ACCESS TO THEIR INTERNET-CONNECTED DEVICES AND ASSOCIATED USER ACCOUNTS?

SYNOPSIS

As internet-connected devices become embedded in homes, cars, and personal belongings, perpetrators of domestic violence have exploited them to monitor, harass, and exert control over survivors remotely. Yet survivors often lack the power to disable or restrict a perpetrator's access to shared smart devices. They may not be listed on the account, may lack passwords or administrative privileges, or may face retaliation if they try to disconnect from the abuser. At the same time, survivors depend on technology to rebuild their lives—through mobile phones, computers, and internet-enabled services essential to work, housing, schooling, or medical care. But without the ability to revoke the abuser's access to devices in their home, survivors remain tethered to systems that can be turned against them.

This bill creates a new statutory framework to prevent the misuse of internet-connected devices in the context of domestic violence, stalking, and other covered acts. It authorizes a survivor, or a designated representative acting on the survivor's behalf, to submit a device protection request to the company or platform that controls access to a connected device. It requires providers to terminate access to perpetrators or provide survivors with the ability to reset the device, and imposes penalties on providers who fail to comply, which can be brought by injured parties or public prosecutors. Unlike the federal Safe Connections Act that this bill is modeled after, this bill would apply broadly to all connected-devices.

This bill is sponsored by the Alliance for HOPE International and 3Strands. It is supported by a broad coalition of domestic violence organizations such as WEAVE and San Francisco Safehouse, and by organizations such as Oakland Privacy and the California District Attorneys Association. It has no formal opposition and was heard and passed by the Assembly Committee on Privacy and Consumer Protection on Consent.

SUMMARY: Establishes a legal process for survivors of domestic violence and related crimes to terminate an abuser's access to internet-connected devices and associated user accounts, protecting survivors from technological abuse and coercive control. Specifically, **this bill**:

1) Makes findings and declarations regarding domestic violence rates, and the prevalence of technology-enabled violence, specifically.

2) Defines key terms including “connected device,” “device access,” “device protection request,” “perpetrator,” and “survivor.”

3) Authorizes a survivor, or a designated representative of a survivor, to submit a device protection request to an account manager seeking to terminate a perpetrator’s access to a connected device or associated account.

4) Requires the device protection request to include specific documentation verifying the abuse, the survivor’s legal control of the device, and the identity of the perpetrator and affected device.

5) Requires an account manager to respond to a complete device protection request within two business days by either:

   a) Terminating the perpetrator’s access and notifying the survivor, or

   b) If termination is not possible, providing a means for the survivor to reset the device to factory settings without needing a PIN or password, based on physical proximity.

6) Prohibits the account manager from charging a fee, requiring consent from other users, increasing rates, or denying requests due to unpaid balances.

7) Prohibits the account manager from notifying the perpetrator of the disconnection or disclosing any account or device information after access has been removed.

8) Provides that survivors shall not be held financially responsible for any charges incurred by the perpetrator after their access has been terminated.

9) Requires account managers to make the process and required documentation publicly available and to provide secure, accessible remote submission methods.

10) Requires account managers to treat survivor-submitted materials as confidential and to delete them within 90 days, subject to limited compliance recordkeeping.

11) Establishes that failure to comply with the above requirements constitutes a violation of this chapter, enforceable by survivors or public prosecutors through civil actions.

12) Authorizes courts to impose civil penalties of up to $2,500 per violation and to award attorney’s fees and costs to prevailing plaintiffs.

13) Declares that any waiver of these protections is void as against public policy.

14) Clarifies that the duties and remedies in this chapter are cumulative with other laws.

15) Exempts from this chapter entities already subject to the federal Safe Connections Act of 2022 or to specified provisions of the Vehicle Code relating to telematics systems.

16) Includes a severability clause.

17) 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. (Penal Code Section 236 *et seq*.)

2) Criminalizes conduct amounting to rape, duress, and other unlawful sexual conduct, including prostitution and abduction. (Penal Code Section 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. (Vehicle Code Section 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. (Vehicle Code Section 28206.)

5) Beginning January 1, 2028, automobile manufactures, for a 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. (Vehicle Code Section 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. (Family Code Section 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. (Government Code Section 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. (U.S. Public Law 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. (Government Code Section 6205 *et seq*.)

10) Requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and information contained in the device from unauthorized access, destruction, use, modification, or disclosure. (Civil Code Sections 1798.91.04 - 1798.91.06.)

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

COMMENTS: As explained by 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.

The Internet of things & tech-based abuse. The "Internet of Things" (IoT) refers to the growing ecosystem of internet-connected devices—thermostats, smart locks, lights, speakers, cameras, and appliances—that collect and exchange data with users and each other. These technologies offer convenience, but also create new avenues for abuse. As internet-connected devices become embedded in homes, cars, and personal belongings, perpetrators of domestic violence have exploited them to monitor, harass, and exert control over survivors remotely.

This form of abuse, known as technological abuse, is now formally recognized by the U.S. Department of Justice. (U.S. Dept. of Justice, Office on Violence Against Women, Domestic Violence (2024) [as of July 1, 2025], https://www.justice.gov/ovw/domestic-violence.) It includes any act intended to harm, threaten, control, stalk, impersonate, or monitor another person through digital means, including smart home systems, apps, GPS trackers, online platforms, and other connected technologies. (*Ibid.*)

A 2021 article in the California Law Review warned that the IoT gives abusers "a powerful new tool" to amplify traditional harms, creating "novel dangers for survivors." (Madison Lo, *A*

Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies under Current Law, 109 California Law Review 277 (2021).) This article and others have documented a growing number of cases in which abusers use apps to remotely adjust lighting or temperature, alter door lock codes, activate alarms, or eavesdrop through smart speakers. A 2018 New York Times investigation described survivors reporting that they were being watched or tormented by devices they couldn't control—sometimes long after their abusers had left the home. (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.)

California courts have increasingly acknowledged the psychological toll of this form of abuse. As one court explained: "The impact can be even worse where electronic surveillance is involved because that allows the abuser to create a 'sense of omnipresence,' eliminating the victim's ability to feel safe in any environment." (*G.G. v. G.S.* (2024) 102 Cal.App.5th 413, 425.)

Yet survivors often lack the power to disable or restrict a perpetrator's access to shared smart devices. They may not be listed on the account, may lack passwords or administrative privileges, or may face retaliation if they try to disconnect the abuser. At the same time, survivors depend on technology to rebuild their lives—through mobile phones, computers, and internet-enabled services essential to work, housing, schooling, or medical care. But without the ability to revoke the abuser's access to devices in their home, survivors remain tethered to systems that can be turned against them.

This bill creates a new statutory framework to prevent the misuse of internet-connected devices in the context of domestic violence, stalking, and other covered acts. It authorizes a survivor, or a designated representative acting on the survivor's behalf, to submit a device protection request to the company or platform that controls access to a connected device ("account manager"). The request must include specific documentation verifying the abuse, the survivor's legal control of the device, and identifying the perpetrator and the device. Within two business days of receiving a complete request, the account manager must either (1) terminate the perpetrator's access to the device or account and confirm that action to the survivor, or (2) if technical limitations prevent termination, provide the survivor a way to reset the device to factory settings or a similar state that removes the perpetrator's access—without requiring a password, PIN, or other credential, and based solely on the survivor's physical proximity to the device. The bill prohibits the account manager from charging fees, requiring consent from other users, or denying the request based on unpaid balances. It also prohibits notifying the perpetrator of the disconnection or sharing any subsequent account or device information. In addition, the bill establishes confidentiality requirements for submitted documentation, financial liability protections for survivors, and clear procedural standards for account managers. The bill exempts entities subject to the federal Safe Connections Act or California's Vehicle Code provisions governing connected vehicle systems.

Enforcement. Of particular relevance to this Committee, the bill provides legal remedies if an account manager violates the provisions of the bill. An account manager that fails to deny access to a perpetrator, as required, would be subject to a civil action brought by any person injured by a violation, or by the Attorney General or a city or county public prosecutor acting in the name of the people of California. Courts may issue injunctive relief and impose civil penalties of up to $2,500 per violation, calculated per connected device. If multiple violations are alleged, the court must make specific findings for each. Civil penalties are allocated to the enforcing entity or to

the prevailing plaintiff if brought privately. In addition, prevailing plaintiffs are entitled to recover reasonable attorney's fees and court costs. Though not formally in opposition, some media and technology companies have reached out to the Committee to express the belief that the penalty should be assessed per request—not per connected device. They claim that a connected device may have multiple parts (such as a home security system that utilizes multiple cameras) and therefore a per-request penalty would be a more appropriate proxy for the harm. The author, on the other hand, believes the abuse happens at the device level, and that the violation should reflect that reality.

***ARGUMENTS IN SUPPORT**:* 3Strands Foundation, a nonprofit dedicated to combating human trafficking and exploitation, is co-sponsoring this measure:

> This critical piece of legislation will provide necessary protections to survivors of human trafficking, domestic violence, and related forms of abuse by addressing the increasing misuse of internet-connected devices to stalk, harass, and control victims.
>
> 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.

The California District Attorneys Association also supports this measure:

> SB 50, as amended, which acknowledges that a perpetrator of domestic violence, family violence, or sex abuse, could harass victims using the perpetrator's access over these devices in a victim's home or otherwise.
>
> SB 50 also provides extra protection to victims. This bill requires those companies or entities who provide the apps that control these internet-connected devices to disable the perpetrator's access when a victim submits a "device protection request" to the company or entity that controls the app. Additionally, providing for a $2,500 penalty for each violation insures additional needed protection. All in all this bill will help protect victims of family violence.

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: Shiran Zohar / JUD. / (916) 319-2334