

SENATE THIRD READING
SB 50 (Ashby)
As Amended September 03, 2025
Majority vote

SUMMARY

This bill requires that within two business days of receiving a device protection request that the account manager for the device deny access to any person listed in the protection request.

Major Provisions

- 1) Requires an account manager, commencing no later than two business days after receiving a device protection request from a survivor do one of the following:
 - a) Terminate or disable a connected device or account access to a perpetrator, as identified in the request.
 - b) *Inform the survivor, in a clear and conspicuous manner, of any methods* to reset the device to factory settings or to a similar state that removes all account access, as specified.
- 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) Prohibits an account manager from notifying the perpetrator of the access termination and from disclosing any data, credential, or account changes related to the survivor.
- 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) "Connected device" does not include *either of the following*:
 - i) Peripheral or component devices that are dependent on a primary connected device for internet connectivity.
 - ii) *A connected device that is more than 10 years old or is no longer supported by the account manager.*
- d) "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.
- 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.

COMMENTS

Alongside advances in technology are parallel advances in the dangers for women¹ 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.

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.

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/>.

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.

Arguments in Opposition

None on file.

FISCAL COMMENTS

- 1) Possible costs (General Fund, special funds) to the Department of Justice (DOJ) of an unknown amount. Actual costs will depend on whether the Attorney General pursues enforcement actions, and, if so, the level of additional staffing DOJ needs to handle the related workload. If DOJ hires staff to handle enforcement actions authorized by this bill, it would incur significant costs, likely in the low hundreds of thousands of dollars annually at a minimum. Additionally, DOJ anticipates costs of \$88,000 in fiscal year (FY) 2025-26 and \$167,000 in FY 2026-27 and ongoing for one new permanent analyst in its Victim Services Unit. DOJ reports the analyst will provide subject matter expertise, help survivors navigate the request process established in the bill, and act as a liaison for survivors and their families, local level victim services agencies, law enforcement agencies.

- 2) Cost pressures (Trial Court Trust Fund, General Fund) of an unknown but potentially significant amount to the courts to adjudicate civil enforcement cases. Actual costs will depend on the number of cases filed and the amount of court time needed to resolve each case. It generally costs approximately \$1,000 to operate a courtroom for one hour. Although courts are not funded on the basis of workload, increased pressure on the Trial Court Trust Fund may create a demand for increased funding for courts from the General Fund. The fiscal year 2025-26 state budget provides \$82 million ongoing General Fund to the Trial Court Trust Fund for court operations.

VOTES

SENATE FLOOR: 38-0-2

YES: Allen, Alvarado-Gil, Archuleta, Arreguín, Ashby, Becker, Blakespear, Cabaldon, Caballero, Cervantes, Choi, Cortese, Dahle, Durazo, Gonzalez, Grayson, Grove, Hurtado, Jones, Laird, Limón, McGuire, McNERney, Menjivar, Niello, Ochoa Bogh, Padilla, Pérez, Richardson, Rubio, Seyarto, Smallwood-Cuevas, Stern, Umberg, Valladares, Wahab, Weber Pierson, Wiener
ABS, ABST OR NV: Reyes, Strickland

ASM PRIVACY AND CONSUMER PROTECTION: 15-0-0

YES: Dixon, Bennett, Bryan, DeMaio, Irwin, Lowenthal, Hoover, McKinnor, Ortega, Patterson, Pellerin, Petrie-Norris, Ward, Wicks, Wilson

ASM JUDICIARY: 12-0-0

YES: Kalra, Dixon, Bauer-Kahan, Bryan, Connolly, Harabedian, Macedo, Pacheco, Papan, Sanchez, Stefani, Zbur

ASM APPROPRIATIONS: 11-0-4

YES: Wicks, Arambula, Calderon, Caloza, Elhawary, Fong, Mark González, Ahrens, Pacheco, Pellerin, Solache
ABS, ABST OR NV: Sanchez, Dixon, Ta, Tangipa

UPDATED

VERSION: September 03, 2025

CONSULTANT: Julie Salley / P. & C.P. / (916) 319-2200

FN: 0001632