Date of Hearing: July 2, 2024

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
SB 1000 (Ashby) – As Amended June 24, 2024

SENATE VOTE: 38-0

SUBJECT: CONNECTED DEVICES: DEVICE PROTECTION REQUESTS

KEY ISSUES:

1) SHOULD THE MANAGER OF AN INTERNET-BASED OR APP-BASED USER ACCOUNT HAVE THE AUTHORITY TO DENY A PERSON ACCESS TO A CONNECTED DEVICE, AS SPECIFIED, IF REQUESTED TO DO SO BY A SURVIVOR OF DOMESTIC VIOLENCE?

2) SHOULD A VEHICLE MANUFACTURER BE REQUIRED TO PROVIDE A SURVIVOR OF DOMESTIC VIOLENCE WITH A MEANS TO DISABLE REMOTE VEHICLE TECHNOLOGY MANUALLY, FROM INSIDE OF THE VEHICLE AND WITHOUT NEEDING A PASSWORD OR LOGIN INFORMATION?

SYNOPSIS

Although domestic violence has apparently always been with us, the tools of the domestic abuser have changed with available technology. Today most of us find ourselves dependent upon our "connected devices," which this bill defines as internet-based devices that enable a person to remotely obtain data from, or send commands to, a connected device or account through a software application. While these devices aim to make our lives easier, they also provide novel means of harassment, stalking, and abuse for those so inclined to use them for those purposes. According to recent media coverage, based on reports of domestic survivors and those who work with them, the perpetrators of domestic violence increasingly use connected devices to inflict further pain and suffering on victims and survivors. An article appearing last year in the New York Times *told of abusive husbands tracking the location of ex-wives, or remotely turning on heat on a hot day in a formerly shared home. Other recent reports stress the dangers of the remote tracking of vehicles, which could prevent a victim from eluding a violent abuser.*

This bill is one of three moving through the Legislature that attempt to protect victims of domestic violence from an abuser's use of remote technology. The two other bills only address remote vehicle *technology, while this bill covers vehicles as well as the panoply of other connected devices. The bill does this by requiring "account managers" of connected devices to deny access to a perpetrator within two days of receiving a request from a survivor. The bill requires manufacturers of vehicles with remote technology to provide a survivor with the ability to deny access immediately, including by permitting a person to disable the technology manually from inside the car without a password or login information.*

While it is critical that the Legislature amend the law as necessary to account for new tools of domestic violence and abuse, the provisions in this bill on remote technology in vehicles raise a number of questions, including possible unintended consequences that could endanger the very people it seeks to protect. The bill is supported by advocates of domestic violence survivors.

While there is no opposition, the Electronic Frontier Foundation and the Alliance for Automotive Innovation have raised significant concerns. The bill recently passed out of the Assembly Privacy Committee on an 11-0 vote.

SUMMARY: Requires an account manager to deny a person access to a connected device no later than two days after the submission of a device protection request by a survivor of domestic violence; requires a vehicle manufacturer to immediately terminate access or disable remote technology and provide the survivor with a way to disable remote vehicle technology manually, as specified. Specifically, **this bill**:

1) Requires an account manager, as defined, to terminate or disable access to a connected device or account by a perpetrator of domestic violence (perpetrator) if a survivor of domestic violence (survivor) has submitted a device protection request to the account manager. Requires termination or disabling of the account no later than two days after the survivor has submitted the request.

2) Requires a vehicle manufacturer to immediately terminate or disable remote vehicle technology upon receipt of a device protection request from a survivor.

3) Requires a survivor who submits a device protection request to an account manager to include in the request all of the following:

    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 specified documentation, including, among other things, police reports, restraining orders, or a signed affidavit from a licensed medical or mental health care provider.

    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 and identification of the perpetrator.

4) Requires the account manager to provide the survivor with a secure means of submitting a device protection request and to keep confidential information submitted by the survivor. Prohibits the account manager from conditioning a device protection request upon payment of a fee or other specified limitations.

5) Defines the following terms for purposes of the above:

    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 a device that is capable of connecting to the internet, directly or indirectly, and that 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.

6) Requires a vehicle manufacturer that offers a vehicle for sale, rent, or lease in California that includes remote vehicle technology to do all of the following:

   a) Ensure that a driver of the vehicle can immediately disable the remote vehicle technology from inside the car and requires, among other things, that this can be done without a password or login information.

   b) Offer secure remote means via the internet for a survivor to submit a vehicle separation notice that includes a prominent link on the vehicle manufacturer's internet website.

   c) Upon request, reset the remote vehicle technology with a new secure account and delete all data from the original account.

   d) Reenable the remote vehicle technology only if the registered owner of the car notifies the manufacturer that the remote vehicle technology was disabled in error, and a survivor has not contacted the vehicle manufacturer to provide the information required by 7) within seven days of the remote vehicle technology being disabled.

7) Requires a survivor to submit a vehicle separation notice to a vehicle manufacturer, as specified, within seven days of the date on which the survivor used the method of manually disabling remote vehicle technology. Requires the notice to include information about the vehicle, the perpetrator, the act, and other information with supporting documentation.

8) Defines "remote vehicle technology," for purposes of the above, to mean any technology that allows a person who is outside of a vehicle to access the activity, track the location, or control any operation of the vehicle or its parts, including, but not limited to, a global positions system (GPS), and app-based technology, or any other remote wireless connectivity technology.

9) Makes an account manager or vehicle manufacturer who violates the provisions above liable for a civil penalty not to exceed $2,500 for each violation, in an action brought by a person injured by a violation or by the Attorney General or other public prosecutor in the name of the people of California. Provides for the distribution of a civil penalty brought by a public prosecutor. If the action is brought by a person injured by the violation, the penalty shall be awarded to that person.

EXISTING LAW:

1) 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.)

2) 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.)

3) Authorizes a court to issue an ex parte order enjoining a party from molesting, attacking, striking, stalking, threatening, sexually assaulting, battering, 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. Defines "disturbing the peace of the other party" for this purpose to mean conduct that, based on the totality of the circumstances, destroys the mental or emotional calm of the other party. Specifies that this conduct may be committed through, among other things, online accounts, text messages, internet-connected devices, or other electronic technologies. (Family Code Section 6320.)

4) Authorizes a person to participate in the Safe at Home program if they, or a household member, are a victim of domestic violence, sexual assault, stalking, human trafficking, child abduction, or elder or dependent adult abuse. Designates the Secretary of State (SOS) as the agent for service of process and receipt of mail, and providing the SOS with any address they want kept confidential. (Government Code Section 6206 (a).)

5) 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*.)

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

COMMENTS: According to the author, this bill "addresses the increasingly prevalent problem of digital abuse and control in domestic violence cases." The author notes that domestic violence organizations are concerned with the increased number of abuse cases related to internet-connected devices and shared accounts. "While modern technology offers convenience and connectivity," the author writes, "it has unfortunately become a tool for perpetrators to exert control over their victims remotely." The author believes that "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."

Technological Abuse and the "Internet of Things." The Office on Violence against Women (OVW), within the U.S. Department of Justice, breaks down domestic violence into several categories of abuse. Not surprisingly, it includes the more familiar categories of "physical abuse," "sexual abuse," "emotional abuse," and "psychological abuse." However, the OVW list now includes a newer category of "technological abuse." OVW defines "technological abuse" as follows:

> 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. (https://www.justice.gov/ovw/domestic-violence.)

In 2021, an article in the *California Law Review* aptly noted, "tactics of domestic violence are nothing new. However, as with various other aspects of modern life, technology threatens disruption." The article detailed how the "Internet of Things" has given abusers "a powerful new tool to expand and magnify the traditional harms of domestic violence, threatening the progress advocates have made in the past thirty years and creating novel dangers for survivors." The article noted that those who work in the domestic violence sphere have developed creative responses and educational resources to warn people about the potential dangers of connected devices and ways to mitigate risks. However, the article then turned to how advocates might supplement these important efforts with legal remedies. Most the article's recommendations focused on updating definitions of domestic violence, harassment, and stalking to account for the rising use of smart technology; recognizing that efforts to "control" another person were a key element of violence and abuse; and ensuring that the terms of domestic violence restraining orders (DVROs) consider forms of technological harassment and stalking. For the most part, as even the article noted, California has already adopted many of these changes. (Madison Lo, "A Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies under Current Law," 109 *California Law Review* 277 (2021).) Yet it appears that most legal responses to the problem of technological abuse have focused on the conduct and methods of the abuser.

This bill focuses not on the abusers, but on the managers, operators, and manufacturers of the devices. The bill contains two parts. The first part applies to "connected devices," defined as internet-based devices that enable a person to remotely obtain data from, or send commands to, a connected device or account through a software application. The second part deals more specifically with "remote vehicle technology," defined as any technology that allows a person who is outside of a vehicle to access the activity, track the location, or control any operation of the vehicle or its parts.

The first part of the bill would require "account managers" to block a perpetrator's access to a connected device or account within two days of receiving a request from a survivor. The bill defines the "account manager" to mean a person or entity that provides the internet-based or app-based account, or a third party that manages the account on their behalf, and that has the authority to make decisions regarding access to the device or account. The bill sets forth the process and the documentation that must accompany a request.

The bill also requires manufacturers who sell or lease vehicles with remote technology within the state to provide the survivor with a means of disabling the perpetrator's access to the technology. Most new cars offer some form of remote vehicle technology that allows someone with a smart phone app to check the vehicle's location and even track the history of where the car has been. Some technology even allows a person to remotely lock and unlock the vehicle, turn it on or off, honk the horn, or even set the car's climate controls. (Kashmir Hill, "Your Car Is Tracking You. Abusive Partners May Be, Too." *New York Times*, Dec. 31, 2023.) However, rather than allowing this to be done within two days of the request, the bill requires the vehicle manufacturer to provide a means by which the survivor can deny access immediately, including by permitting the survivor – or any other person, for that matter – to disable the technology manually from inside the car without a password or login information.

Unintended consequences of immediate and manual disabling in vehicles. The ability to disable the tracking system, immediately and manually, without prior documentation could be a vital tool for a survivor who needs immediate protection from a perpetrator who is stalking, abusing, or harassing them by means of the vehicle tracking system. However, it also is possible

that this capability could be misused. For example, if any person inside the vehicle could manually disable the technology, someone other than the survivor could misuse this method of deactivation. For example, a car thief could disable the tracking system in order to escape detection by law enforcement. A perpetrator might block access to a survivor, who might want to know the abuser's location. Indeed, an abusive ex-husband could turn off the technology while kidnapping the survivor or the survivor's children.

The remote vehicle technology provisions in this bill track the language of AB 3139 (Weber), which is now in the Senate Appropriations Committee, and which this Committee heard and passed in April. However, this Committee's analysis pointed out potentially dangerous unintended consequences of manual disabling, and suggested that the author of that bill consider this possibility as the bill moved forward. Not only were the provisions of AB 3139 not amended, the prior Committee inserted the language from AB 3139 into the bill now before the Committee. *The Committee believes that the author of this bill should also seriously consider these potential unintended consequences, albeit with the understanding that this bill is much later in the legislative process than was AB 3139 when heard by this Committee.*

Technical feasibility and application to existing vehicles. As noted above, the bill requires any vehicle manufacturer that offers to sell, rent, or lease a vehicle with remote vehicle technology to ensure that a driver can immediately and manually disable the technology from inside the vehicle. Moreover, the driver must be able to do this without needing to use a password or enter any other login information. In addition to the unintended consequences discussed above, the Alliance for Automotive Innovation (Alliance) points out that, at present, few if any vehicles offer such a method of manual disabling this technology. In light of this, the Committee has asked the author's office if it expects that the bill will only apply to vehicles manufactured after the operative date of this bill. That is, the bill imposes its restrictions on the "manufacturer." Thus going forward, if manufacturers want to sell or lease their vehicles in California, they will need to install a manual mechanism that does not require access to the internet or a software application on all future vehicles that they manufacture. It is unclear, however, what obligation the manufacturer will owe to the driver of an existing vehicle within this state that has remote technology. The other requirements under the bill seem less problematic. For example, the manufacturer should be able to offer a secure means by which a survivor could ask the manufacturer to disable the technology remotely, by resetting or otherwise amending the existing account. However, the Alliance has raised questions about the ability of a manufacturer to do this *legally* where the abuser, as opposed to the survivor, is the owner of the vehicle and the account. Having said that, it is notable that the Alliance does not *oppose* this bill, but has only registered its concerns about a manufacturer's ability to comply with the bill, both technologically and legally. The Alliance supports the intent of the bill, but simply wants to ensure – especially given that three different bills address the same issue – that compliance will be possible and requirements uniform.

Related legislation: do we need three bills on remote vehicle technology? As noted above, this bill is one of three pending pieces of legislation that seek to protect survivors of domestic violence from modern technology. The two other bills apply exclusively to remote vehicle technology. SB 1394 (Min) – which was not referred to this Committee – requires a vehicle manufacturer to terminate a person's access to remote vehicle technology upon request from a driver who establishes proof that they have exclusive use and legal possession of the vehicle, are a survivor of domestic violence, and seek to block access to the perpetrator of that violence. AB 3139 (Weber), like this bill, requires a manufacturer that sells, rents, or leases vehicles with

remote vehicle technology to ensure that a driver of the vehicle can immediately disable the remote vehicle technology from inside the car and without need of a password or login information. The key difference between SB 1394, on the one hand, and AB 3139 and this bill, on the other hand, has to do with both the immediacy and method of deactivation, as well as with the need for the survivor to provide *prior* documentation. While AB 3139 has the advantage of an easy and immediate means of activation, SB 1394 has the advantage of avoiding the potentially dangerous unintended consequences of allowing any person inside the vehicle to disable the technology manually. Ideally, the authors of SB 1394 and AB 3139 could find a way to incorporate the best aspects of both bills and find a solution that protects survivors in a workable fashion. Given that there are already two competing bills on remote vehicle technology, and because this bill covers "connected devices" not covered by the other two bills, the Committee suggested that the author remove the vehicle provisions from this bill. The author rejected that recommendation.

Enforcement. Of particular relevance to this Committee, the bill provides legal remedies if an account manager or vehicle manufacturer violates the provisions of the bill. An account manager or vehicle manufacturer 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. The account manager or vehicle manufacturer that violates the bill would be liable for a civil penalty of $2,500 for each violation. If the Attorney General brings the action, the fine will go to the General Fund. If a local city or county prosecutor brings the action, the fine will go to the city or county treasury. If a person injured by the violation brings an action, the penalty will go to that person.

The Alliance for Automotive Innovation has asked that the enforcement provision include protection from a possible lawsuit by an owner (an alleged perpetrator) denied access to the vehicle. The Alliance points out that under Civil Code Section 1491.6 (d), a property owner who changes locks to protect a victim of domestic violence is not liable to a person excluded. The Alliance seeks a similar provision that would protect them from a person, especially an owner, denied access, so long as the manufacturer acted in good faith compliance with the provisions of this bill. However, the bill only creates a civil action brought against a party or entity that *fails* to deny access, so that the person bringing a civil action under this bill would be the survivor, not the alleged perpetrator denied access. Thus, the Alliance is apparently concerned that a perpetrator denied access could bring a lawsuit on some other grounds, such as an unlawful taking or a common law conversion. *If the bill passes out of this Committee, the author may wish to consider such an amendment.*

***ARGUMENTS IN SUPPORT**:* San Francisco Safehouse supports this bill because it "addresses digital harassment by requiring companies to swiftly cut off access for abusers at the request of a victim, ensuring immediate protection for one of our most vulnerable populations. . . While technology can serve as a valuable resource for victims," Safehouse notes, "it is unfortunately frequently abused by perpetrators of domestic violence. Abusers can use modern technology to monitor, harass, threaten, and violate their victims." Safehouse believes that "SB 1000 is a crucial measure to protect domestic violence victims from digital abuse and control [and] 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."

ARGUMENTS IN SUPPORT IF AMENDED: While the Electronic Frontier Foundation (EFF) supports the general intent of this bill, it can only support the bill if significantly amended. First, for many connected devices found in a home, EFF notes that a person with physical access to the device can simply reset it to the original factory settings. This effectively cuts off the abuser's access. Second, EFF contends that the "broad scope of S.B. 1000 creates a tremendous burden for device manufacturers, who will need to build an infrastructure that receives and verifies device disconnection requests with little additional benefit to survivors of abuse, who already have these other, simpler options for the majority of connected devices." Third, EFF raises concerns about the privacy implications raised by the some of the information that the survivor must submit.

***ARGUMENTS OF CONCERN*:** The Alliance for Automotive Innovation (Alliance) does not oppose this bill, but it believes that this bill, along with SB 1394 or AB 3139, will "create unique challenges that must be addressed." First, the Alliance asks for a single bill or careful coordination of the three bills, noting that manufacturers cannot comply with three different sets of requirements. Second, the Alliance argues that the requirements must be operationally and technologically feasible. Third, the Alliance believes that this bill, like the others, must better clarify the "appropriate level of legal documentation" needed to trigger the requirement to remove an abuser's access to a vehicle. Of the three pending bills, the Alliance believes that SB 1394 establishes the appropriate standard of documentation. Finally, the Alliance argues that vehicle manufacturers should have protection from liability, just as property owners who change locks to protect tenants are not liable to abusers who are denied access to a dwelling.

REGISTERED SUPPORT / OPPOSITION:

Support

Alliance for Hope International
Oakland Privacy
Sacramento Regional Family Justice Center (SRFJS)
San Francisco Safehouse
Voices Survivor Advocacy Network

Support If Amended

Electronic Frontier Foundation

Concerns

Alliance for Automotive Innovation

Opposition

None on file

Analysis Prepared by: Tom Clark / JUD. / (916) 319-2334