**SENATE JUDICIARY COMMITTEE**
**Senator Thomas Umberg, Chair**
**2023-2024 Regular Session**

SB 1394 (Min)
Version: April 11, 2024
Hearing Date: April 23, 2024
Fiscal: Yes
Urgency: No
CK

## SUBJECT

Access to remote vehicle technology

## DIGEST

This bill requires a vehicle manufacturer to create a process for terminating a person's access to remote vehicle technology, as defined, upon a completed request from a driver who establishes proof of legal possession of the vehicle. Upon a successful submission, access shall be terminated within two business days. The bill requires manufacturers to provide a notification inside a vehicle of whether remote vehicle technology is in use.

## 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. 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 vehicles to harass and terrify their victims even after they have managed to escape.

This bill requires vehicle manufacturers to create a user-friendly online process for terminating a person's remote access to location tracking technology in a vehicle. A driver is required to provide proof of legal possession of the vehicle, such as a vehicle title or a court order awarding exclusive access. Access must then be terminated within two days. Manufacturers are also required to provide a notification in vehicles with this technology, indicating whether it is in use.

The bill is co-sponsored by the Domestic Violence Clinic at the University of California, Irvine School of Law and Ending Tech-Enabled Abuse (EndTab). It is supported by several advocacy groups, including Streets for All. No timely opposition was received by the Committee. The bill passed out of the Senate Transportation Committee on a 15 to 0 vote.

## PROPOSED CHANGES TO THE LAW

Existing law:

1) 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.)

2) 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) Defines "remote vehicle technology" as any technology that allows a person who is outside of a vehicle to track the location of, or control any operation of, the vehicle, and includes, but is not limited to, a Global Positioning System (GPS) that tracks the location of the vehicle or an app-based technology that controls any operation of the vehicle.

2) Requires a vehicle manufacturer to terminate a person's access to remote vehicle technology within two business days after the date of receiving a completed request from a driver, as provided.

3) Requires a driver submitting such a request to provide proof of legal possession of the vehicle, such as a dissolution decree, temporary order, or domestic violence restraining order that awards possession or exclusive use of the vehicle. Legal possession of a vehicle may be established by providing a vehicle title. A court order awarding sole possession or ownership of a vehicle shall take priority over a vehicle title showing joint ownership. Nothing further shall be required of the driver and no fee may be charged.

4) Requires the manufacturer to notify the driver that they may contact the driver to confirm a person's access to the remote vehicle technology has been terminated.

5) Requires a vehicle manufacturer to provide a notification inside of a vehicle that is installed with remote vehicle technology that shows if it is being used.

6) Requires a vehicle manufacturer to detail the above process on its website and remote technology application. An efficient, secure, and user-friendly online submission process for requests must be established including the following:
    a) A confirmation email acknowledging receipt.
    b) Disclosure of the action taken or of additional information needed.
    c) If approved, a clear explanation and guidance on how to create their own app account, if necessary, to ensure that the driver can maintain control over the vehicle's remote technology once the person's access to remote vehicle technology has been terminated.

7) Requires the vehicle manufacturer to adhere to relevant data protection laws and regulations.

## 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, it also has increasingly been used 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 as 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.
>
> . . .
>
> 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 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]

---

[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 April 11, 2024.

[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.

The problem of constant surveillance follows victims through their vehicles, too:

> San Francisco police Sergeant David Radford contacted Tesla in May 2020 with a request on a case: Could the automaker provide data on an alleged stalker's remote access to a vehicle?
>
> A woman had come into the station visibly shaken, according to a police report. She told police that her abusive husband, in violation of a restraining order, was stalking and harassing her using the technology in their 2016 Tesla Model X.
>
> The SUV allows owners to remotely access its location and control other features through a smartphone app. She told police she had discovered a metal baseball bat in the back seat — the same bat the husband had previously used to threaten her, the police report stated.
>
> Weeks later, Sergeant Radford asked Tesla (TSLA.O), opens new tab for data that might help the investigation. A Tesla service manager replied that remote-access logs were only available within seven days of the events recorded, according to records in a lawsuit the woman later filed. Radford's investigation stalled.
>
> Cases of technology-enabled stalking involving cars are emerging as automakers add ever-more-sophisticated features, such as location tracking and remote control of functions such as locking doors or honking the horn, according to interviews with divorce lawyers, private investigators and anti-domestic-violence advocates. Such abusive behavior using other devices, such as phone spyware or tracking devices, has long been a concern, prompting technology companies including Google and Apple to design safeguards into their products.[3]

A similar story was reported by the New York Times:

> After almost 10 years of marriage, Christine Dowdall wanted out. Her husband was no longer the charming man she had fallen in love with. He had become narcissistic, abusive and unfaithful, she said. After one of their fights turned violent in September 2022, Ms. Dowdall, a real estate agent, fled their home in Covington, La., driving her Mercedes-Benz C300 sedan to her daughter's house near Shreveport, five hours away. She filed a domestic abuse report with the police two days later.

---

[3] Kristina Cooke & Dan Levine, *An abused wife took on Tesla over tracking tech. She lost.* (December 19, 2023) Reuters, https://www.reuters.com/technology/an-abused-wife-took-tesla-over-tracking-tech-she-lost-2023-12-19/.

> Her husband, a Drug Enforcement Administration agent, didn't want to let her go. He called her repeatedly, she said, first pleading with her to return, and then threatening her. She stopped responding to him, she said, even though he texted and called her hundreds of times.
>
> Ms. Dowdall, 59, started occasionally seeing a strange new message on the display in her Mercedes, about a location-based service called "mbrace." The second time it happened, she took a photograph and searched for the name online.
>
> "I realized, oh my God, that's him tracking me," Ms. Dowdall said.
>
> . . .
>
> A car, to its driver, can feel like a sanctuary. A place to sing favorite songs off key, to cry, to vent or to drive somewhere no one knows you're going.
>
> But in truth, there are few places in our lives less private.
>
> Modern cars have been called "smartphones with wheels" because they are internet-connected and have myriad methods of data collection, from cameras and seat weight sensors to records of how hard you brake and corner. Most drivers don't realize how much information their cars are collecting and who has access to it, said Jen Caltrider, a privacy researcher at Mozilla who reviewed the privacy policies of more than 25 car brands and found surprising disclosures, such as Nissan saying it might collect information about "sexual activity."[4]

The concern is that often the abuser is the named account holder and likely set up and has continued access to the remote location tracking even after the survivor has escaped the situation or even secured a restraining order. Advocates argue updates to 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.

[4] Kashmir Hill, *Your Car Is Tracking You. Abusive Partners May Be, Too.* (December 31, 2023) The New York Times, https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html.

> 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.[5]

2. Allowing survivors of violence to regain control

This bill seeks to provide a tool for survivors to regain control of their lives by regaining control of their vehicles. This bill requires vehicle manufacturers to establish and make clear a process for drivers to terminate a person's access to the remote vehicle technology installed in the vehicle. To enhance transparency and communication, the manufacturer has to establish an efficient, secure, and user-friendly online submission process for such requests and include specified features that ensure a driver is made aware of the status of the process.

The driver is required to provide proof of legal possession of the vehicle. This can take the form of a dissolution decree, temporary order, or domestic violence restraining order that awards possession or exclusive use of the vehicle. It specifically states that a court order awarding sole possession takes priority over a vehicle title showing joint ownership. The manufacturer cannot ask for additional documentation beyond this or charge the driver a fee.

Upon receiving the request with the required documentation, the manufacturer is required to terminate access within two business days.

To ensure these drivers are on notice of the technology and when it is being used, the bill requires a vehicle manufacturer to provide a notification inside of a vehicle that is installed with remote vehicle technology that shows if the remote vehicle technology is being used. Concerns have been raised about the technical feasibility of this without some phase-in period. The author has committed to further engagement with stakeholders on this particular issue.

According to the author:

> We have known for some time that GPS-tracking technology in cars is being exploited by domestic violence abusers, but unfortunately, some car manufacturers are refusing to act to address this potentially fatal problem. Survivors of abuse should not have to fear technology as a tool for further victimization by abusers who can track and harass them. SB 1394 creates a

[5] *Ibid*.

> process for survivors of domestic abuse to rapidly terminate remote access to a vehicle and ensure their safety and privacy.

Writing in support, the Electronic Frontier Foundation states the need for the bill:

> In addition to internet-connected services and app-controlled access, physical location tracking technology allows stalkers and abusers unprecedented access to a person's location without their knowledge. At EFF, we have been sounding the alarm about this threat to people, especially survivors of domestic abuse. This realm of technology remains an ongoing concern and we steadfastly champion the elevation of the right to privacy and the safeguarding of individuals, valuing these principles over mere property loss.
>
> In situations of domestic violence or abusive environments, an abuser and victim may share car titles, car loans, and car insurance. Once a victim makes the decision to leave a violent relationship or abusive household, they are not thinking their car is yet another tool that their abuser can use against them. Many victims, let alone consumers are not aware that most modern cars are filled with internet-connected services that can track them and also have app controlled capabilities. This enables abusers to continue to surveil and harass their partners. . . .
>
> S.B. 1394 will create a simple and user-friendly online process for a consumer to request termination of another person's remote access to a car. Additionally, car manufacturers will be required to provide a clear notification on the dashboard of a vehicle that discloses to a driver when someone has continued remote access or is using a connected-app to control their car.

**SUPPORT**

EndTab (sponsor)
University of California Irvine, Domestic Violence Clinic (sponsor)
California Women's Law Center
Electronic Frontier Foundation
Family Violence Appellate Project
Junior Leagues of California State Public Affairs Committee
Laura's House
Radiant Futures
Streets for All

## OPPOSITION

None received

## RELATED LEGISLATION

Pending Legislation: SB 1000 (Ashby, 2024) provides a mechanism for survivors of "covered acts" to regain control of connected devices. These acts include false imprisonment, human trafficking, and other sexual crimes. With verification that a covered act has been committed against the victim and verification of the device as the victim's or in the victim's exclusive control or fixed within their home or vehicle, account managers, those in control of device access, must grant a device protection request, essentially denying the abuser access to the connected device. SB 1000 is currently in this Committee.

Prior Legislation: 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 created 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.

## PRIOR VOTES:

Senate Transportation Committee (Ayes 15, Noes 0)

**********