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

AB 3139 (Weber)
Version: April 24, 2024
Hearing Date: June 18, 2024
Fiscal: Yes
Urgency: No
CK

SUBJECT

Data privacy: vehicle manufacturers: remote vehicle technology

DIGEST

This bill requires a vehicle manufacturer to ensure that any remote technology in their vehicles can be immediately manually disabled by a driver from inside the vehicle, as provided, or, if technically impossible, to create a mechanism for survivors of specified crimes to submit a request to disable such technology, which shall be done within one business day. The bill requires a survivor of specified crimes to provide a notice with specified documentation to the manufacturer within seven days of using the manual mechanism.

EXECUTIVE SUMMARY

Domestic violence can take many forms, but generally involves 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. Victims of human trafficking face similar patterns of control and violence. Escaping these situations is often harrowing and beset by fear of being caught or found by the perpetrator of the violence or other criminal abuse.

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

This bill requires vehicle manufacturers to ensure the ability to manually disable any remote technology from within their vehicles immediately or, if not possible, to create a user-friendly process for a survivor of domestic violence, human trafficking, or other

crimes, to request the disabling of the technology and to submit supporting documentation. The manufacturer can only reenable the technology upon request of the survivor, or if documentation is not provided by a survivor, after seven days and with the request of the registered owner. A survivor is required to submit documentation within 7 days of disabling the technology or along with the request through the alternative mechanism. However, the manufacturer is not required to verify ownership, the identity of the survivor, or the authenticity of any information submitted.

The bill is sponsored by the Consumer Federation of California. It is supported by several advocacy groups, including the California Low-Income Consumer Coalition. The Electronic Frontier Foundation is in opposition. Should the bill pass out of this Committee, it will next be referred to the Senate Transportation Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) 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).

2) 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.)

3) 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) Requires a vehicle manufacturer that offers a vehicle for sale, rent, or lease in the state that includes remote vehicle technology to do all of the following:
    a) Ensure that the remote vehicle technology can be immediately manually disabled by a driver of the vehicle while that driver is inside the vehicle by a method that meets all of the following criteria:
        i. The method of manually disabling the remote vehicle technology is prominently located and easy to use and does not require access to a remote, online application.
        ii. Upon its use, the method of manually disabling the remote vehicle technology informs the user of the below notice requirements.
        iii. The method of manually disabling the remote vehicle technology does not require a password or any log-in information.
        iv. Upon its use, the method of manually disabling the remote vehicle technology does not result in the remote vehicle technology, vehicle manufacturer, or a third-party service provider sending to the registered owner of the car an email, telephone call, or any other notification related to the remote vehicle technology being disabled.
        v. Upon its use, the method of manually disabling the remote vehicle technology causes the remote vehicle technology to be disabled for a minimum of seven days and capable of being reenabled only by the vehicle manufacturer, as provided.
    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 that meets both of the following requirements:
        i. The link is titled, in bold and capital letters, "CALIFORNIA SURVIVOR DOMESTIC VIOLENCE ASSISTANCE."
        ii. The link provides a designated internet website portal that provides a survivor the ability to submit a vehicle separation notice and includes a form that enables a survivor to submit the information required.
    c) Upon the request of a survivor, 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 within seven days of the remote vehicle technology being disabled.

2) Requires a survivor to submit a vehicle separation notice to a vehicle manufacturer through the means provided by the vehicle manufacturer within 7

days of the date on which the survivor used the required method of manually disabling remote vehicle technology, which shall include the vehicle identification number of the vehicle and either of the following:

a) A statement by the survivor signed under penalty of perjury that a perpetrator who has access to the remote vehicle technology in the vehicle has committed, or allegedly committed, a covered act against the survivor or an individual in the survivor's care.
b) A copy of specified documents that supports that the perpetrator has committed, or allegedly committed, a covered act against the survivor or an individual in the survivor's care, including a signed affidavit from specified individuals acting within the scope of that person's employment, including a health care provider or social worker, a police report, or a restraining order.

3) Provides that, only if, for technological reasons, a vehicle manufacturer is unable to comply with the above requirements regarding a manual method, the vehicle manufacturer shall create a conspicuous mechanism that is easy to use by which a survivor or a designated person can submit a request to disable a vehicle's remote vehicle technology. A manufacturer must disable the technology within one business day after receiving a request from a survivor that includes the information required.

4) Provides that it does not authorize or require a vehicle manufacturer to verify ownership of a vehicle, the identity of a survivor, or the authenticity of information that is submitted by the survivor.

5) Provides that, in addition to any other remedy provided by law, a vehicle manufacturer that violates the bill shall be liable in a civil action brought by a survivor for all of the following:
   a) Reasonable attorney's fees and costs of the prevailing survivor.
   b) Statutory damages in an amount not to exceed $50,000 per violation, or statutory damages in an amount not to exceed $100,000 per violation for knowing violations.
   c) Actual damages or three times the amount at which the actual damages are assessed for knowing or reckless violations.

6) Provides that any waiver of the requirements of this chapter shall be against public policy, void, and unenforceable.

7) Defines the relevant terms. "Covered act" is defined as conduct that is any of the following:
   a) A crime described in subsection (a) of Section 40002 of the federal Violence Against Women Act (34 U.S.C. Sec. 12291), including domestic violence, dating violence, sexual assault, stalking, and sex trafficking.

b) An act or practice described in paragraph (11) or (12) of Section 103 of the federal Trafficking Victims Protection Act of 2000 (22 U.S.C. Sec. 7102) relating to severe forms of trafficking in persons and sex trafficking, respectively.
c) An act under state law, tribal law, or the Uniform Code of Military Justice (Chapter 47 (commencing with Section 801) of Title 10 of the United States Code) that is similar to an offense described in subparagraph (A) or (B).

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]

[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 June 4, 2024.

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]

One particularly problematic area where constant surveillance victimizes survivors is through their vehicles:

> 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.

[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.

> Weeks later, Sergeant Radford asked Tesla 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.
>
> 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.

---

[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/.

> 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 are desperately needed:

> 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.
>
> 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. <u>Allowing survivors of violence to regain control</u>

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 ensure that any remote vehicle technology can be *immediately* manually disabled by a driver of the vehicle while that driver is inside the vehicle by a method that meets specified criteria, including that the method be easy, not require a password, and must notify the driver, upon use, of the requirement for survivors to submit a "vehicle separation notice" to the manufacturer within seven days. The notice must identify the vehicle and must be accompanied by either (1) one of a host of documents, including a police report,

---

[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.
[5] *Ibid*.

affidavit of a counselor, or other relevant, official record, or, (2) a statement signed under penalty of perjury by the survivor that states a perpetrator has committed a specified crime against the individual and the perpetrator has access to the remote technology. The manufacturer must provide a secure, remote means to submit such notice.

The technology must be disabled for at least seven days. The manufacturer is the *only* one that can enable it again. That can *only* be done after seven days if the required notice from the survivor has not been received *and* the manufacturer has received a notice from the registered owner that the technology was disabled by error. The survivor can also request the technology be reset, with old data being deleted and a new secure account being established.

The bill provides an alternative for manufacturers only if it is unable due to technological reasons to ensure immediate, manual disabling. In that case, the manufacturer must create a conspicuous mechanism for a survivor to submit the required documentation and request disabling. Upon receiving such a documented request, the manufacturer is required to disable access within one business day.

The manufacturer is not required nor authorized to verify ownership of the vehicle, the identity of the survivor, or the authenticity of the information submitted by the survivor. The manufacturer is also prohibited from notifying the registered owner that the technology is being disabled.

A survivor is authorized to bring a civil action against a vehicle manufacturer in violation of these provisions and to seek all of the following in addition to any other remedy provided by law:

- Reasonable attorney's fees and costs of the prevailing survivor.
- Statutory damages in an amount not to exceed $50,000 per violation, or statutory damages in an amount not to exceed $100,000 per knowing violation.
- Actual damages or three times the amount at which the actual damages are assessed for knowing or reckless violations.

At the federal level, the Safe Connections Act (117 P.L. 223, 2022) takes the first step by providing a process for survivors of various crimes, including domestic violence and human trafficking, to separate their mobile phone plan from a documented perpetrator. More specifically to the issue at hand, the FCC Chair Jessica Rosenworcel has publicly urged auto manufacturers to address the issues of remote vehicle technology in the hands of perpetrators of violence: "The Chairwoman sent letters to nine of the largest automakers serving the American marketplace. These letters ask the companies for details about the connected car systems they offer, any existing plans to support

survivors in their efforts to disconnect from abusers, and how these companies handle consumers' geolocation data."[6]

According to the author:

> AB 3139 will bolster DV survivor protections by enacting state laws that expand upon the Federal Safe Connections Act to cover vehicle manufacturers, enabling survivors to eliminate abusers' access to their vehicles and personal information.
>
> AB 3139 enables DV survivors to request, with proper documentation such as a copy of a signed affidavit from a licensed medical or mental health care provider, that auto manufacturers separate the information of the survivor from the information of the abuser. This request is required to be completed by auto manufacturers no later than two business days after receiving the request.

Writing in support, Oakland Privacy asserts:

> AB 3139 helps legal protections for victims of domestic violence (DV) to catch up with technology used to harass, intimidate, monitor or control them. Modern technology has enabled perpetrators to facilitate abuse in a myriad of ways, from a distance and with little effort or cost.
>
> Moreover, modern cars are essentially computers on wheels - and a class of Internet of Things (IoT) devices. As cars are often a necessity in today's society, it is important that vehicle technology is not weaponized to exert abuse or control over another individual.
>
> AB 3139 affords victims with an important tool to break from the grip of an abuser, however it also reveals gaps in legal protections against abuse through IoT devices generally. More protections should shift the burden from victims to tech developers, and general privacy protection measures such as data minimization, storage and sharing increase the overall safety of IOT devices.

The Electronic Frontier Foundation writes in an oppose-unless-amended position:

> We believe AB 3139 falls short in capturing strong privacy protections for victims of techenabled abuse. First, we are concerned that proposed

[6] Press release, *FCC Chairwoman Calls on Carmakers and Wireless Companies to Help Ensure the Independence and Safety of Domestic Violence Survivors* (January 11, 2024) FCC, https://docs.fcc.gov/public/attachments/DOC-399700A1.pdf.

Section 22948.671's requirement that a car manufacturer "ensure that the remote vehicle technology can be immediately manually disabled by a driver of the vehicle while that driver is inside the vehicle" will not make survivors of abuse safer. Instead, it will have the unintended consequence of creating entirely new avenues of abuse. An immediately-effective manual method of disabling remote vehicle technology that is available to any driver is also available to any passenger who can reach across the car. Car thieves, kidnappers, and carjackers will benefit from the ability to turn off tracking of vehicles that they have stolen. The kidnapping of children shared by the abuser and the survivor and theft of shared property, such as motor vehicles, are common elements of domestic abuse. Creating a scenario in which an abuser can make off with a car, its driver, and possibly a child passenger without the ability to track their location for an extended period of time will put survivors in significant danger.

Secondly, a vehicle separation notice website that is clearly labeled under A.B. 3139 to state "CALIFORNIA SURVIVOR DOMESTIC VIOLENCE ASSISTANCE" poses significant privacy implications for a survivor's browser history. Current practice is to have a quick "escape" button on domestic violence survivor services website. The "escape" button's purpose is to conceal that the survivor has been looking for resources and serves as a simple and quick to use to ensure the utmost safety. We recommend that A.B. 3139 bill require a more innocuous title that will not be so easily found in a victim's browser search history.

Lastly, A.B. 3139 seems to relieve car manufacturers of any responsibility to exercise due diligence when reviewing and ultimately granting a request, including verification of the requester's identity. We recommend that an amendment like that contained in S.B. 1000 (Ashby) that delineates the request process and specifies what documents or supporting materials are required to complete the request is considered and amended into A.B. 3139. This will ensure a victim completes the request procedure thoroughly the first time. Time is of the essence, and making sure all steps are thoroughly described will ensure expediency.

SUPPORT

Consumer Federation of California (sponsor)
California Low-income Consumer Coalition
Consumers for Auto Reliability & Safety
Elder Law & Advocacy
Oakland Privacy
Public Law Center
Rise Economy

OPPOSITION

Electronic Frontier Foundation

RELATED LEGISLATION

Pending Legislation:

SB 1000 (Ashby, 2024) requires account managers of connected devices to deny account access to a person in response to a "device protection request" when the requester submits specified documentation, including verification that they are in exclusive legal possession or control of the connected device. SB 1000 is currently in the Assembly Privacy and Consumer Protection Committee.

SB 1394 (Min, 2024) requires a vehicle manufacturer to terminate 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 or a domestic violence restraining order naming the person whose access is sought to be terminated. SB 1394 prohibits a vehicle manufacturer from charging a fee to a driver for completing their request requires a vehicle manufacturer, among other things, to establish an efficient, secure, and user-friendly online submission process for requests related to terminating a person's access to remote vehicle technology, as specified, and to ensure that all personal information provided during this process is handled with the utmost security and privacy, adhering to relevant data protection laws and regulations. A vehicle manufacturer is required 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. SB 1394 is currently in the Assembly Privacy and Consumer Protection 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:

Assembly Floor (Ayes 71, Noes 0)
Assembly Appropriations Committee (Ayes 15, Noes 0)
Assembly Judiciary Committee (Ayes 11, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 0)

****