Date of Hearing: June 18, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 1000 (Ashby) – As Amended May 16, 2024

AS PROPOSED TO BE AMENDED

SENATE VOTE: 38-0

SUBJECT: Connected devices: device protection requests

SYNOPSIS

Alongside advances in technology are parallel advances in the dangers for people who are or were in relationships with violent perpetrators. The technological advances have brought new and inventive ways for perpetrators to abuse and torture the people 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. Smart speakers can often be used to listen in on conversations in a home through an online app. Home security cameras and baby monitors can allow an abuser to watch and record their victims. Small tracking devices can easily be hidden in bags, clothing, or vehicles, allowing an abuser to monitor their current or former partner's movements. As new technology seeps into everyday life, abusers have adopted and repurposed it to terrorize and control their current and former partners.

This bill is substantially similar to the federal Safe Connections Act (SCA) of 2022 (PL 117-223). The SCA 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. Like the SCA, within two business days of receiving a device protection request this bill requires the account manager for a connected device to deny access to any person listed in the protection request.

The scope of this bill includes vehicles. As with other bills in the Legislature that propose applying the policy framework of the SCA to connectivity in vehicles, the Committee has taken the

position that allowing two business days to disconnect the technology is too long in the case where a survivor is in immediate danger and needs to use their vehicle to escape an abuser. Therefore, the suggested Committee amendments require that drivers be able to immediately disable remote technology manually from inside the car.

This bill is supported by San Francisco SafeHouse, Oakland Privacy, and Alliance for Hope International, among others. Should it pass this Committee, it will next be heard in the Judiciary Committee.

SUMMARY: Requires account managers of internet 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. Specifically, **this bill**:

1) 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 (IP) or Bluetooth address.

    c) "Device access" means the ability to remotely control a connected device, remotely change the characteristics of a connected device, or remotely view or manipulate data collected by or through a connected device, by accessing a user account or accounts associated with the connected device. Acts that require device access include, but are not limited to, remotely manipulating an audio system, security system, light fixture, or other home appliance or fixture and accessing camera or location data from a motor vehicle.

2) Requires an account manager to do the following:

    a) Deny a person's device access, as identified in a qualifying device protection request, within two business days.

    b) Offer the ability to submit a device protection request through secure remote means that are easily navigable. An account manager shall not require a specific form of documentation to submit a device protection request.

    c) Make information about these options publicly available on their website and mobile application, if applicable.

3) Requires a device protection request to include all of the following:

    a) Verification of the requester'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 requester's exclusive use care, possession, or control of the connected device.

b) Identification of the connected device or devices.

c) Identification of the person that the requester seeks to deny device access.

4) Prohibits an account manager from conditioning a device protection request upon any limitation or requirement, including:

a) Payment of a fee, penalty, or other charge.

b) Approval of the device protection request by any other person who is not a legal owner or in legal possession of the device.

c) A prohibition or limitation on the ability to deny device access as a result of arrears accrued by the account or associated with the connected device.

d) An increase in the rate charged for the account if any subscription fee or other recurring charge for account access applies.

e) Any other limitation or requirement.

5) Provides that an account manager, and other specified agents or employees, shall treat any information submitted as confidential and securely dispose of the information not later than 90 days after receiving the information. This does not prohibit the maintenance, for longer than the period specified, of a record that verifies that a requester fulfilled the conditions of a request.

6) Makes any waiver of these provisions void and unenforceable. The duties and obligations imposed are cumulative with any other duties or obligations imposed under other law, and shall not be construed to relieve any party from any duties or obligations imposed under other law. The remedies or penalties provided by this chapter are cumulative to each other and to the remedies or penalties available under all other laws of the state.

7) Includes a severability clause.

8) Makes these provisions operative on January 1, 2026.

9) Amends the definition of "disturbing the peace of the other party" 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. (Pen. Code § 236 et seq.)

2) Criminalizes conduct amounting to rape, duress, and other unlawful sexual conduct, including prostitution and abduction. (Pen. Code § 261 et seq.)

3) 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.)

4) 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, Code § 6206(a).)

5) 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).

6) 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. (Gov. Code § 6205 *et seq*.)

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

COMMENTS:

1) **Intimate Partner Violence.** Nationally more than one-third of women will experience rape, physical violence, and/or stalking by an intimate partner in their lifetime. Nearly 8 million women experience one or more of these abuses by a current or former partner each year. There are nearly 90 domestic violence related killings in California each year. There were 87 deaths in 2020, 70 were women and 17 were men.[1] The National Domestic Violence Hotline reports that an average of 24 people per minute are victims of rape, physical violence or stalking by an intimate partner in the United States — more than 12 million women and men over the course of a single year. Almost half of all women and men in the US have experienced psychological aggression by an intimate partner in their lifetime (48.4% and 48.8%, respectively).[2]

Statistically speaking, the most dangerous place for a woman is not out in public, it is in her home. In addition, the most dangerous people for a woman are not strangers, they are the men she knows and has relationships with (e.g. current and former partners, fathers, brothers, and friends). Given where the danger generally lies, for those situations where the danger is also a current partner or someone else who lives in their home, survivors need a safe, quick means of escape.

---

[1] California Partnership to End Domestic Violence. *California Domestic Violence Fact Sheet* (2022) https://www.cpedv.org/policy-priorities.
[2] The National Domestic Violence Hotline. *Domestic Violence Statistics.* https://www.thehotline.org/stakeholders/domestic-violence-statistics/.

Adding to the risk, the most dangerous time for someone who is in a relationship with a violent abuser is when they decide to leave. According to organizations working with survivors of abuse, when someone being abused in a relationship leaves or attempts to leave, abusers often lash out in an attempt to regain control over their partner or, in some cases, resort to extreme violence, even homicide, because they feel they have nothing left to lose.[3] According to Canada's Battered Women Support Services:

> Separation is a common theme found within spousal murder-suicide where half of the cases occur after the couple have either separated (26%), were in the process of separating (9%), or had expressed a desire to separate (15%). . . . The statistics outline the reality that the most dangerous time for a survivor/victim is when she leaves the abusive partner; 77 percent of domestic violence-related homicides occur upon separation and there is a 75 percent increase of violence upon separation for at least two years.[4]

With the omnipresent nature of technology that contains remote geo-location capabilities, especially vehicles, leaving an abuser becomes significantly more difficult, if the abuser has online access to the survivor's location that allows them to track the survivor's every movement.

2) **The internet of things (IoT).** The "internet of things" (IoT) refers to a network of devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data. Some examples are kitchen appliances, thermostats, door locks, home surveillance systems, or automated sprinklers.

According to IBM's website:

> IoT enables these smart devices to communicate with each other and with other internet-enabled devices. Like smartphones and gateways, creating a vast network of interconnected devices that can exchange data and perform various tasks autonomously. This can include:
>
> - monitoring environmental conditions in farms
> - managing traffic patterns with smart cars and other smart automotive devices
> - controlling machines and processes in factories
> - tracking inventory and shipments in warehouses
>
> The potential applications of IoT are vast and varied, and its impact is already being felt across a wide range of industries, including manufacturing, transportation, healthcare, and agriculture. As the number of internet-connected devices continues to grow, IoT is likely to play an increasingly important role in shaping our world. Transforming the way that we live, work, and interact with each other.[5]

---

[3] *Will My Partner Be Violent After I Leave? How to predict violence after leaving an abuser.* DomesticShelters.org. (Mar. 24, 2017) https://www.domesticshelters.org/articles/safety-planning/will-my-partner-be-violent-after-i-leave.
[4] *Eighteen Months After Leaving Domestic Violence is Still the Most Dangerous Time*, Battered Women's Support Services (Jun. 11, 2020) https://www.bwss.org/eighteen-months-after-leaving-domestic-violence-is-still-the-most-dangerous-time/.
[5] IBM, *What is the IoT?* https://www.ibm.com/topics/internet-of-things.

3) **Technology-enabled abuse.** Alongside advances in technology are parallel advances in the dangers for people who are or were in relationships with violent perpetrators. The advances have brought new and inventive ways for perpetrators to abuse and torture the people in their lives. In fact, the federal government now recognizes technological 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.[6]

A *New York Times* article in 2018 explored the relatively new phenomenon of abuse cases that were tied to the rise of smart home technology. According to that article, domestic violence shelters were reporting calls from women who were convinced they were going crazy. They were 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. At the time, the *Times* reported:

> In more than 30 interviews with The New York Times, domestic abuse victims, their lawyers, shelter workers and emergency responders described how the technology was becoming an alarming new tool. Abusers — using apps on their smartphones, which are connected to the internet-enabled devices — would remotely control everyday objects in the home, sometimes to watch and listen, other times to scare or show power. Even after a partner had left the home, the devices often stayed and continued to be used to intimidate and confuse.[7]

In the intervening years, internet connected devices have become even more commonplace. Abusers not only use connected devices to terrorize their victims, but also to stalk and surveil their every move. Smart speakers can often be used to listen in on conversations in a home through an online app. Home security cameras and baby monitors can allow an abuser to watch and record their victims. Small tracking devices can be easily hidden in bags, clothing, or vehicles, allowing an abuser to monitor their victim's movements. As each new technology seeps into everyday life, abusers have adopted and repurposed them to terrorize and control their current and former partners.

Specifically as it relates to automobile technology, since 2012 when General Motors' OnStar debuted Family Link, a service that allowed remote users to track their family members and receive alerts about where the car goes, advocates and experts working with survivors of stalking and domestic abuse have warned about the dangers related to allowing this type of technology to be used in cars without offering a way for it to discreetly be turned off by the driver.[8] Over the

---

[6] Information on the types of domestic violence and the Office of Violence against Women can be found at https://www.justice.gov/ovw/domestic-violence.
[7] 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.
[8] Lineman, Tracey. "Connected Car Technology Can Enable Abusers to Track Their Victims," *Motherboard, Tech by Vice* (Aug. 14, 2018) *available at* https://www.vice.com/en/article/gy3kw7/internet-connected-car-technology-can-enable-abusers-to-track-victims.

last 12 years this technology has become more sophisticated and common with most new cars offering remote vehicle technology that allows someone with a smart phone app to check a car's location, including following the movement of the car in real time; track the history of where the car has been driven to; lock and unlock the vehicle remotely; turn it on or off; set the car's climate controls; make the horn honk; and turn on its lights.[9]

According to a recent article in *The New York Times*, "Domestic violence experts say that these convenience features are being weaponized in abusive relationships, and that car makers have not been willing to assist victims. This is particularly complicated when the victim is a co-owner of the car, or not named on the title."[10] The goal of this bill is to require manufacturers and account holders for all connected devices to be responsive to women who are reporting that their abuser has used the company's device as a weapon and that the abuser needs to be removed from the account.

4) **Purpose of this bill.** This bill is substantially similar to the federal Safe Connections Act (SCA) of 2022 (PL 117-223). The SCA 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. Like the SCA, within two business days of receiving a device protection request this bill requires the account manager for a connected device to deny access to any person listed in the protection request.

5) **Author's statement.** According to the author:

> SB 1000 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, cameras, and even vehicles. While modern technology offers convenience and connectivity, it has unfortunately become a tool for perpetrators to exert control over their victims remotely.
>
> 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.

6) **Analysis.** As noted previously, this bill is modeled after federal legislation that allows survivors to have their mobile phones separated from family plans or contracts that are connected to their abuser. This allows survivors to keep their phones and phone numbers. Under that law

---

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

and this legislation, businesses have two business days to break the connection between devices once the business receives a request accompanied by documentation from a survivor.

Arguably, someone escaping violence could turn off their phone while leaving an abuser and wait for the time it takes for the mobile phone career to separate the phone from the connected account before turning it back on. Similarly, someone experiencing technology enabled abuse in their home through the use of internet connected appliances and other devices, may be able to temporarily cover the security cameras, unplug an appliance or reset a Wi-Fi password while the connected devices account manager removes the abuser's access. However, as discussed in detail in previous sections of this analysis, the most dangerous time in an abusive relationship is when the survivor is attempting to leave their abusive partner. Having access to a vehicle is critical during that time for most survivors. Unfortunately, as currently drafted, this bill allows auto manufacturers the same two business-day period to disconnect the remote vehicle technology. Imagine being a survivor in an increasingly dangerous relationship who needs to flee the Friday before Memorial Day. Under this bill, an abuser would have five days to track the person fleeing before the connection is broken. This is ample time for an abuser to track down their victim and either harm them more or coerce them into returning to their home.

Three bills modeled after the Safe Connection Act were introduced in the Legislature this year. AB 3139 (Weber) and AB 1394 (Min) both initially focused solely on applying the policy framework established in the Act to allowing survivors of domestic abuse to request that an auto manufacturer disconnect their vehicles from any remote capabilities. As noted above, the manufacturers would be provided with two business days to fulfill the request. This bill, however, takes the policy framework in the Safe Connection Act and applies it broadly to all connected devices including home appliances, thermostats, locks, doorbells, vehicles, and any other devices that is connected remotely to an application.

When it comes to connectivity in vehicles, the Committee has taken the position that the delayed time frame in all three bills is too long and has proposed amendments to all of the bills that are designed to accomplish three key things:

1. The driver must be able to manually disable the connectivity from inside the car without needing to log into an account or provide a password.

2. Disabling the technology cannot result in account-holders or registered owner being notified that it has been disconnected by the driver.

3. The survivor must be provided with a grace period that allows her time to get to safety and then gather and submit the documents required to permanently remove the abuser from remote access.

Creating a safe harbor. The intent of these amendments is to provide survivors with the immediate protection they need when using their vehicle to escape escalating violence, while allowing them time to submit the necessary information to an auto manufacturer establishing that even though the survivor may not be the registered owner of the vehicle, they have a right to disconnect the technology. The amendments still require that survivors provide the necessary documentation needed to establish their right to the car. This is intended to ensure that abusers cannot further weaponize the vehicle by manually disabling the technology in the car and simply claiming that they are the person being abused in the relationship.

7) **Suggested Committee amendments.** In order to effectuate the goals discussed in the previous section, the Committee suggests adopting the following amendments.

Amendment #1 adds the following definition to 22948.30:

(d) "Remote vehicle technology" means 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, that includes, but is not limited to, any of the following:

(1) A Global Positioning System (GPS).

(2) An app-based technology.

(3) Any other remote wireless connectivity technology.

Amendment #2 inserts the following section:

22948.33.1 (a) A vehicle manufacturer that offers a vehicle for sale, rent, or lease in the state that includes remote vehicle technology shall do all of the following:

(1) 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:

(A) The method of manually disabling the remote vehicle technology shall be prominently located and easy to use and does not require access to a remote, online application.

(B) Upon its use, the method of manually disabling the remote vehicle technology shall inform the user of the requirements of subdivision (b).

(C) The method of manually disabling the remote vehicle technology shall not require a password or any log-in information.

(D) Upon its use, the method of manually disabling the remote vehicle technology shall 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.

(E) Upon its use, the method of manually disabling the remote vehicle technology shall cause the remote vehicle technology to be disabled for a minimum of seven days and capable of being reenabled only by the vehicle manufacturer pursuant to paragraph (4).

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

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

(4) 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 requester has not contacted the vehicle manufacturer to provide the information required by subdivision (b) within seven days of the remote vehicle technology being disabled.

(b) A requester shall submit a vehicle separation notice to a vehicle manufacturer through the means provided by the vehicle manufacturer pursuant to paragraph (2) of subdivision (a) within 7 days of the date on which the requester used the method of manually disabling remote vehicle technology required by subdivision (a), which shall include the vehicle identification number of the vehicle and a copy of either of the following documents that supports that the perpetrator has committed, or allegedly committed, a covered act against the requester or an individual in the requester's care:

(1) A signed affidavit from any of the following individuals acting within the scope of that person's employment:

(A) A licensed medical or mental health care provider.

(B) A licensed military medical or mental health care provider.

(C) A licensed social worker.

(D) A victim services provider.

(E) A licensed military victim services provider.

(2) A copy of any of the following documents:

(A) A police report.

(B) A statement provided by the police, including military police, to a magistrate judge or other judge.

(C) A charging document.

(D) A protective or restraining order, including military protective orders.

(E) Any other relevant document that is an official record.

(c) (1) Only if, for technological reasons, a vehicle manufacturer is unable to comply with paragraph (1) of subdivision (a), the vehicle manufacturer shall disable remote vehicle technology within one business day after receiving a request that includes the information required by subdivision (b) and is submitted pursuant to the mechanism required by paragraph (1).

8) **Larger policy questions.** While this bill has the potential to make a significant difference in the lives of those fleeing abusive partners, it raises larger policy considerations related to the invasive nature of technology that would benefit from additional attention. With the proliferation of surveillance and tracking technology, including built in vehicle location technology, tracking devices that can easily be concealed in a car or in someone's belongings, in home and public surveillance cameras, automated license plate recognition tools, not to mention the ability to track

someone using the smartphones that are virtually universal, at what point has surveillance gone too far? Should Californians simply accept the complete loss of privacy as people move through their lives in public and private spaces?

Much like the focus that is being placed on the impact of social media, advancement in artificial technology, and the collection and sale of personal information for profit, constant surveillance by private individuals, businesses, and government has a profound impact on Californians' lives. Rather than considering the risks of one device or technological advancement at a time, at some point, it might behoove the Legislature, and this Committee in particular, to explore the larger surveillance policy questions, including the dangers associated with the unchecked proliferation of surveillance tools and their impact on Californians' privacy rights, especially for those who are at risk of abuse.

9) **Related legislation.** AB 3139 (Weber, 2024) requires the manufacturer of a vehicle with remote vehicle technology allowing the vehicle to be tracked to equip the vehicle with a feature that allows the driver to immediately sever the connection between the vehicle and the remote application. In addition, it prohibits manufacturers from restoring the connection for one week, while allowing a survivor of domestic abuse the opportunity to provide a vehicle separation request accompanied by the required documentation. This bill is currently pending in the Senate Judiciary Committee.

SB 1394 (Min, 2024) requires a vehicle manufacturer to terminate a person's access to remote vehicle technology upon a completed request from a driver who establishes legal possession of the vehicle or a domestic violence restraining order naming the person whose access is sought to be terminated. The bill would prohibit a vehicle manufacturer from charging a fee to a driver for completing their request to terminate a person's access to remote vehicle technology. That bill is pending in this Committee.

ARGUMENTS IN SUPPORT:

Writing in support of the bill, Oakland Privacy notes:

> Unfortunately, the advancement of technology has brought with it novel ways for abusers to perpetrate acts of domestic violence and coercive control. And the potential for abuse will grow if not curbed by law. In 2022 The National Domestic Violence Hotline received 35,145 calls (with 18% of the calls featuring some level of digital abuse).
>
> An IoT device is any standalone internet-connected device that can be monitored and/or controlled remotely and a recent study found that U.S. households have an average of connected devices. It is readily apparent that IoT devices will proliferate exponentially, and with that will also come more abuse through those technologies. Abuse of IoT devices can not only intimidate, harass or attempt to control, but can also negatively affect a victim's life in other kinds of ways. For example, an abuser remotely unlocked a victim's home and car, and then weaponized the malicious acts claiming they were an indication that the victim was an unfit parent in a child custody battle.

Also writing in support, San Francisco SafeHouse further argues:

> The National Domestic Violence Hotline reports that one in four women and one in seven men are survivors of severe domestic violence in their lifetime. An average of 24 people per

minute are victims of rape, physical violence, or stalking by an intimate partner in the United States — more than 12 million women and men over the course of a single year. Almost half of all women and men in the US have experienced psychological aggression by an intimate partner in their lifetime.

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 1000 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.

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

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200