Date of Hearing: April 16, 2024

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 3139 (Weber) – As Amended March 21, 2024

AS PROPOSED TO BE AMENDED

SUBJECT: Data privacy: vehicle manufacturers: remote vehicle technology

SYNOPSIS

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.

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.

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 allowing this type of technology to be used in cars without offering a way for it to discreetly be turned off by the driver. Over the 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.

As currently in print, this bill is substantially similar to the federal Safe Connections Act (SCA) of 2022 (PL 117-223), 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. Like the SCA, the purpose of this bill is to require an automobile manufacturer disconnect a vehicle from any remote vehicle technology within two business days of receiving a request from a survivor.

The Committee is concerned 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. As an alternative, the Committee proposes another, more immediate model for breaking the connection between a vehicle and the devices that have remote access. At the core of the policy is allowing a survivor to immediately disable the remote technology from inside the car in a manner that permanently breaks the connection thus not allowing the abuser to restore

the connection from their remote device. With the suggested amendments, the bill would work as follows:

1. *If/when technologically feasible, an auto manufacturer would need to update the technology in the vehicle to install an option for immediately disabling all remote technology (while preserving all other technology in the vehicle). The method for disabling will be required to be easy to access and disable, without requiring a password or log-in information.*

2. *Once disabled, the survivor will have seven days to submit the information currently required in the bill in order for the connection to remain severed. Similarly, the registered owner of the car will have seven days to contact the auto manufacturer to have the connection restored. Assuming that the technology was disabled for a reason other than to protect a survivor, the connection will be turned back on by the manufacturer.*

3. *If it is not technologically feasible for a manufacturer of a vehicle that offers remote capabilities to update the system to allow it to be disabled, then the original process proposed in this bill will become the default, with the exception that the auto manufacturer would have one-business day after receiving the request to disable the technology.*

This bill is sponsored by the Consumer Federation of California and has a number of supporters. Currently, there is no registered opposition.

If the bill passes this Committee, it will next be heard by the Judiciary Committee.

SUMMARY: Requires a vehicle manufacturer to separate access to remote vehicle technology from a vehicle no later than two days after receiving a separation request from a survivor of intimate partner violence. Specifically, **this bill**:

1) Requires a vehicle manufacturer to do the following:

    a) Separate a domestic abuse perpetrator's access to the remote vehicle technology from a vehicle if technologically possible.

    b) Separate the technology from the vehicle if a) cannot be operationally or technically achieved.

    c) Perform the separation without imposing any fee, penalty, charge, condition, or agreement.

    d) Perform the separation notwithstanding the consent of another individual, including the registered owner of the car.

    e) Offer a secure remote means via the internet for a survivor to submit a vehicle separation request that includes a prominent link entitled "CALIFORNIA SURVIVOR DOMESTIC VIOLENCE ASSISTANCE."

    f) Notify the survivor who submitted the request, no later than two days after receiving the request, of its inability to carry out the separation request.

g) Assist the survivor in modifying the settings of the remote vehicle technology to prevent the perpetrator from obtaining information about the survivor, including their location data.

2) Requires a vehicle separation request to include a vehicle identification number 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 either of the following 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:

i) A signed affidavit from any of the following individuals acting within the scope of their employment:

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

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

(3) A licensed social worker.

(4) A victim services provider.

(5) A licensed military victim services provider.

(6) An employee of a court.

ii) A copy of any of the following documents:

(1) A police report.

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

(3) A charging document.

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

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

3) Defines a "covered act" as including domestic violence, dating violence, sexual assault, stalking, and sex trafficking.

4) Defines "perpetrator" as an individual who has committed or allegedly committed a covered act against a survivor or an individual under the care of a survivor.

5) Defines "remote vehicle technology" 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.

6) Defines "survivor" as an individual who has had a covered act committed or allegedly committed against them or an individual who provides care to an individual who has had a covered act committed or allegedly committed against them.

7) Provides that a vehicle manufacturer that violates the provisions of this chapter shall be liable in a civil action brought by a survivor for the following:

   a) Reasonable attorney's fees and costs.

   b) A civil penalty not to exceed $50,000 per violation, or a civil penalty 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.

   d) These penalties are in addition to any other remedy provided by law and any waiver of the requirements of the chapter are against public policy, void, and unenforceable.

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) 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. (Chapter 3.1 (commencing with Section 6205) of Division 7 of Title 1 of the Government Code.)

FISCAL EFFECT: As currently in print, this bill is keyed 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

[1] California Partnership to End Domestic Violence. *California Domestic Violence Fact Sheet* (2022) https://www.cpedv.org/policy-priorities.

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.

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) **Technological 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

---

[2] The National Domestic Violence Hotline. *Domestic Violence Statistics.* https://www.thehotline.org/stakeholders/domestic-violence-statistics/.
[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/.

> platforms, computers, mobile devices, cameras and imaging programs, apps, location tracking devices, or communication technologies, or any other emerging technologies.[5]

Specifically, as it relates to this bill and 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 allowing this type of technology to be used in cars without offering a way for it to discreetly be turned off by the driver.[6] Over the 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.[7]

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."[8]

3) **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, the purpose of this bill is to require an automobile manufacturer to disconnect a vehicle from any remote vehicle technology within two business days of receiving a request from a survivor.

4) **Author's statement.** 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.

5) **Federal Communications Commission (FCC) Rulemaking.** FCC chair, Jessica Rosenworcel, has called on automakers to help in protecting domestic abuse survivors from the

---

[5] 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.
[6] 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.
[7] 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.
[8] *Ibid.*

misuse of remote vehicle technology by abusers. As modern vehicles make it increasingly easy for passengers and drivers to access hands-free communication tools, find-your car services, and more, these smart car services can and have been used to stalk, harass, and intimidate survivors of intimate partner violence. Chairwoman Rosenworcel importantly notes, "No survivor of domestic violence and abuse should have to choose between giving up their car and allowing themselves to be stalked and harmed by those who can access its data and connectivity."[9]

The FCC is currently examining how the agency can use existing law to ensure car manufacturers are taking steps to assist abuse victims and are seeking comment on additional steps the Commission can take to safeguard domestic violence survivors.[10]

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 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. 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. 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 likely ample time for an abuser to track down their victim and either harm them more or force them to return to their home.

In working closely with the author, the Committee proposes another, more immediate model for breaking the connection between a vehicle and the devices that have remote access. At the core of the policy is allowing a survivor to immediately disable the remote technology from inside the car in a manner that permanently breaks the connection thus not allowing the abuser to restore the connection from their remote device. With the suggested amendments, the bill would work as follows:

1. If/when technologically feasible, an auto manufacturer would need to update the technology in the car to install an option for immediately disabling all remote technology (while preserving all other technology in the vehicle). The method for disabling will be required to be easy to access and disable, without requiring a password or log-in.

2. Once the remote technology is disabled, the survivor will have seven days to submit the information currently required in the bill in order for the connection to remain severed. Similarly, the registered owner of the car will have seven days to contact the auto manufacturer to have the connection restored. Assuming that the technology was disabled

---

[9] FCC Media Release (Jan. 11, 2024) https://docs.fcc.gov/public/attachments/DOC-399700A1.pdf.
[10] Miranda, Shauneen. "FCC chairwoman asks that automakers be subject to a domestic abuse law." *Axios* (Feb. 28, 2024) https://www.axios.com/2024/02/28/fcc-automakers-proposal-domestic-abuse.

for a reason other than to protect a survivor, the connection will be turned back on by the manufacturer.

3. If it is not technologically feasible for a manufacturer of a vehicle that offers remote capabilities to update the system to allow for it to be disabled, then the original process proposed in this bill will become the default, with the exception that the auto manufacturer would have one business day after receiving the request to disable the technology.

Creating a safe harbor. The intent of these amendments is to provide survivors with the immediate protection they need while allowing them time to submit the necessary information to an auto manufacturer establishing that even though the survivor is not the registered owner of the vehicle, they have a right to disconnect the technology because they are using the vehicle to flee an abusive relationship. The amendments will also clarify that the manufacturers are not required to verify the validity of the documentation. These changes are intended to provide stronger protections for the survivor. In addition, the amendments will provide additional protections for the auto manufacturers that will no longer be responsible for determining whether or not it is appropriate to sever the remote vehicle connection.

7) **Proposed Committee amendments.** The suggested Committee amendments will fundamentally restructure this bill in order to strengthen the protections for survivors who are being tracked and/or technologically abused by their perpetrator through remote vehicle technology features. Conceptually, the amendments will reflect the following:

1. An automobile manufacturer that offers a vehicle for sale, rent or lease in California that includes remote vehicle technology (as defined) is required to do the following:

    a. Include the following capability, if it is technologically feasible:

        i. The remote vehicle technology shall be capable of being immediately and manually disabled by a driver of the vehicle while that driver is inside the vehicle.

        ii. The method of manually disabling the remote vehicle technology features shall be prominently located and easy to disable, without requiring access to a remote, online application.

        iii. The method of manually disabling the remote vehicle technology shall not require a password or any log-in information. However, disabling the technology may require the presence of the key or key-fob that is required to operate the vehicle.

        iv. No warning or notification shall be sent to the remote device at any point before, during, or after it is manually disabled. Nor shall the registered owner of the car receive an email, telephone call, or any other notification related to the remote vehicle technology being disabled.

        v. Once the remote vehicle technology is manually disabled from inside the car, it must remain disabled for a minimum of seven days and must be capable of being re-enabled only by the automobile manufacturer.

vi. *Offer a secure remote means via the internet for a survivor to submit a vehicle separation notice that includes a prominent link entitled "CALIFORNIA SURVIVOR DOMESTIC VIOLENCE ASSISTANCE."*[11]

vii. *Notify the survivor who submitted the notice, no later than two days after receiving the notice, of whether or not the documents have been accepted and the remote vehicle technology has been permanently severed from the previous account.*

viii. Allow the survivor to request that the remote vehicle technology be reset with a new, secure account and that all data be deleted from the original account.

ix. Re-enable the remote vehicle technology after seven days, only if the registered owner of the car notifies the manufacturer within that time period that it was disabled in error *and* the survivor has not contacted the manufacturer to provide the necessary documentation.

b. If the required modifications in (a) are technologically incapable of being implemented, the automobile manufacturer must disable the remote vehicle technology no more than one business day after receiving a request from a survivor that includes the required documentation.

2. Requires a vehicle separation notice from a survivor to be submitted within one week of manually disabling the remote vehicle technology and requires that it include a vehicle identification number 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 either of the following 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:*

i. *A signed affidavit from any of the following individuals acting within the scope of their employment:*

ii. *A licensed medical or mental health care provider.*

iii. *A licensed military medical or mental health care provider.*

iv. *A licensed social worker.*

v. *A victim services provider.*

---

[11] Italicized text indicates language that remains substantially similar, if not identical, to language currently in the bill in print.

vi. *A licensed military victim services provider.*

vii. *A copy of any of the following documents:*

1. A police report.

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

3. A charging document.

4. A protective or restraining order, including military protective orders.

5. Any other relevant document that is an official record.

3. States that nothing in this section shall be interpreted to authorize or require the auto manufacturer to verify ownership of the vehicle, the identity of the survivor, or the authenticity of the documentation that is submitted by the survivor.

4. *Provides that a vehicle manufacturer that violates the provisions of this chapter shall be liable in a civil action brought by a survivor for the following:*

a. *Reasonable attorney's fees and costs.*

b. *A civil penalty not to exceed $50,000 per violation, or a civil penalty 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.*

d. *These penalties are in addition to any other remedy provided by law and any waiver of the requirements of the chapter are against public policy, void, and unenforceable.*

5. *Defines a "covered act" as including domestic violence, dating violence, sexual assault, stalking, and sex trafficking.*

6. *Defines "perpetrator" as an individual who has committed or allegedly committed a covered act against a survivor or an individual under the care of a survivor.*

7. *Defines "remote vehicle technology" 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.*

8. *Defines "survivor" as an individual who has had a covered act committed or allegedly committed against them or an individual who provides care to an individual who has had a covered act committed or allegedly committed against them.*

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.** SB 1000 (Ashby and Rubio, 2024), commencing January 1, 2026, would require an account manager, as defined, to deny an abuser, as defined, access to a connected device commencing no later than two days after a device protection request is submitted to the account manager by a victim of that abuser, and would set forth the requirements for a victim to submit a device protection request and the requirements that an account manager make the request available. 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 before Senate Transportation Committee.

ARGUMENTS IN SUPPORT: The sponsors of the bill, the California Consumer Federation, writes:

> In a recent story published in The New York Times, Christine Dowdall was being tracked by her husband, a Drug Enforcement Administration Agent, through 'Mbrace'—a part of 'Mercedes Me,' which is a suite of connected services for her Mercedes-Benz C300 sedan. Ms. Dowdall had only used the Mercedes Me app to make her auto loan payments and was unaware that the service could also be used to track her vehicle's location. Despite numerous calls to Mercedes customer service, where she provided evidence of her payment history, a restraining order against her husband, and legal documentation granting her exclusive use of the car during their divorce proceedings, the representatives informed her that her husband, being listed on the loan, was considered the primary customer, allowing him to retain full access to the vehicle's connected services.
>
> The inability of consumers to control the access and use of their own personal data poses a threat to safety, and in the case of survivors, it can mean life or death. These practices have raised concerns for the Federal Communications Commission, prompting them to inquire

> with automakers about their plans to support survivors, the use of geolocation data collected by the services. . . . (Citations removed.)

Also in support of the bill, Secure Justice notes:

> We believe AB 3139 is a commonsense approach to an increasing problem - women being stalked by current or past partners via electronics in their vehicles. By mandating the manufacturer to provide a technical solution to terminating the remote monitoring of such electronics, the burden is shifted from the victim towards the party most qualified to bear the burden of implementing the technical fix.
>
> In addition, by requiring that requests for separating the communications to be submitted under penalty of perjury, the likelihood of false allegations against former partners is greatly lessened.
>
> For these reasons, AB 3139 would further Secure Justice's goals of guarding against erosion of our civil liberties and right to privacy.

REGISTERED SUPPORT / OPPOSITION:

Support

Consumer Federation of California
Elder Law & Advocacy
Oakland Privacy
Public Law Center
Secure Justice

Support if Amended

Electronic Frontier Foundation

Opposition

None on file.

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