

## SENATE RULES COMMITTEE

AB 375

Office of Senate Floor Analyses

(916) 651-1520 Fax: (916) 327-4478

---

### THIRD READING

---

Bill No: AB 375  
Author: Chau (D), et al.  
Amended: 9/12/17 in Senate  
Vote: 21

---

SENATE JUDICIARY COMMITTEE: 5-2, 7/18/17

AYES: Jackson, Hertzberg, Monning, Stern, Wieckowski

NOES: Moorlach, Anderson

SENATE ENERGY, U. & C. COMMITTEE: 9-1, 7/18/17

AYES: Hueso, Bradford, Cannella, Hertzberg, Hill, McGuire, Skinner, Stern,  
Wiener

NOES: Vidak

NO VOTE RECORDED: Morrell

ASSEMBLY FLOOR: 77-0, 5/11/17 (Consent) - See last page for vote

---

**SUBJECT:** Broadband Internet access service providers: customer privacy

**SOURCE:** Author

---

**DIGEST:** This bill enacts the California Broadband Internet Privacy Act in an effort to reinstate the consumer privacy protections afforded by rules finalized by the Federal Communications Commission in October 2016, but recently eliminated by the Trump Administration and Congress.

### **ANALYSIS:**

Existing law:

- 1) Provides, through the California Constitution, that all people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy. (Cal. Const., Art. I, Sec. 1.)

- 2) Requires an operator of a commercial Internet Web site or online service (operator) that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit the commercial Internet Web site or online service to conspicuously post, or make available, its privacy policy, as specified. An operator violates this provision if the operator fails to post its policy within 30 days after being notified of noncompliance. (Bus. & Prof. Code Secs. 22575 & 22576.)
- 3) Requires, among other things, that the privacy policy identify the categories of personally identifiable information that the operator collects about individual consumers and the categories of third-party persons or entities with whom the operator may share that information. (Bus. & Prof. Code Secs. 22575 & 22576.)
- 4) Provides that, for purposes of Business and Professions Code Sections 22575 and 22576, the term “personally identifiable information” means individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including, in part, name, social security number, identifiers that permit the physical or online contacting of a specific individual, and information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described therein. (Bus. & Prof. Code Sec. 22577.)
- 5) Requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law further provides that a business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code Sec. 1798.81.5.)
- 6) Requires a business that collects personal information about a California consumer and shares that information with a third party for marketing purposes to disclose, upon a consumer’s written request, the categories of information that were disclosed to a third party for the third party’s direct marketing purposes and the names and addresses of all third parties that received the

information. Alternatively, a business may comply with this requirement by adopting a policy that allows a customer to prevent the disclosure of personal information to a third party for the third party's direct marketing purposes, and the business notifies the customer of his or her right to prevent disclosure under the policy and provides the user with a cost-free means of exercising that right. (Civ. Code Sec. 1798.83.)

- 7) Provides, with regard to the automatic purchase renewals statute, that “clear and conspicuous” or “clearly and conspicuously” means in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks, in a manner that clearly calls attention to the language. In the case of an audio disclosure, “clear and conspicuous” and “clearly and conspicuously” means in a volume and cadence sufficient to be readily audible and understandable. (Bus. & Prof. Code Sec. 17601(c).)
- 8) Specifies that every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications service provided by a telecommunications carrier. (47 U.S.C. Sec. 222(a).)
- 9) Provides that a telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts. (47 U.S.C. Sec. 222(b).)
- 10) Provides that except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of: the telecommunications service from which such information is derived; or services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories. (47 U.S.C. Sec. 222(c)(1).)
- 11) Provides that for purposes of 47 U.S.C. Sec. 222(c)(1), without express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to:

- call location information concerning the user of a commercial mobile service, as defined, or the user of an IP-enabled voice service, as defined, other than in accordance with 47 U.S.C. Sec. 222(d)(4); or
  - automatic crash notification information to any person other than for use in the operation of an automatic crash notification system. (47 U.S.C. Sec. 222(f).)
- 12) Provides that a telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer. (47 U.S.C. Sec. 222(c)(2).)
- 13) Provides for the disclosure by a telecommunications carrier of aggregate customer information, as specified. (47 U.S.C. Sec. 222(c)(3).)
- 14) Provides that nothing in 47 U.S.C. Section 222 prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents to:
- initiate, render, bill, and collect for telecommunications services;
  - protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;
  - provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and
  - provide call location information concerning the user of a commercial mobile service, as defined, or the user of an IP-enabled voice service, as defined: to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency service; to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or to providers of information or database management services solely for purposes of assisting the delivery of emergency services in response to an emergency. (47 U.S.C. Sec. 222(d).)
- 15) Does not define "approval of the customer".
- 16) Defines "customer proprietary network information" as:

- information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
  - information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. (47 U.S.C. Sec. 222(h)(1).)
- 17) Provides that “customer proprietary network information” does not include subscriber list information, as defined. (47 U.S.C. Sec. 222(d).)
- 18) Provides for the sharing of “subscriber list information” for the purpose of publishing directories, as specified, and defines “subscriber list information” as any information:
- identifying the listed names or subscribers of a carrier and such subscribers telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classification; and
  - that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format. (47 U.S.C. Secs. 222(d)(3) & (e).)
- 19) Defines “aggregate customer information” as collective data that relates to a group or category of services or customers from which individual customer identities and characteristics have been removed. (47 U.S.C. Sec. 222(h)(2).)
- 20) Contains provisions regarding subscriber listed and unlisted information for emergency services purposes, as specified. (47 U.S.C. Sec. 222(g).)
- 21) Regulates the information practices of various industries. Examples of such laws include the federal Gramm-Leach-Bliley Act (which regulates financial institutions), Health Insurance Portability and Accountability Act (which regulates the health care industry), the California Confidentiality in Medical Information Act (protects information maintained by the health care industry), the California Financial Information Privacy Act (protects information maintained by financial institutions), the Student Online Personal Information Protection Act (SOPIPA) (protects student information on K-12 Web sites or applications), and the Insurance Information Privacy Act (protects information maintained by the insurance industry).

This bill:

- 1) Enacts the California Broadband Internet Privacy Act (Act). The stated intent of the Act is to incorporate into statute certain provisions of the Federal Communications Commission (FCC) Report and Order, “Protecting the Privacy of Customers of Broadband and Other Telecommunications Services” (FCC 16-148), which were revoked by Senate Joint Resolution 34 (Public Law 115-22).
- 2) Provides that it is the intent of the Legislature in enacting this Act to give consumers greater control over their personal information when accessing the Internet through an Internet service provider and thereby better protect their own privacy and autonomy. The stated intent is that the consumer protections set forth in this Act be interpreted broadly and any exceptions interpreted narrowly, using the FCC Report and Order as persuasive guidance, in order to maximize individual privacy and autonomy.
- 3) Defines “broadband Internet access service” (BIAS) to mean a mass-market retail service by wire or radio in California that provides the capability to transmit data and to receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to, and enable the operation of, the service, but excluding dial-up Internet access service. The term also encompasses any service that provides a functional equivalent of the service described, or that is used to evade the Act’s protections. A “broadband Internet access service provider” is a person engaged in the provision of BIAS to a customer account located in California. It does not include a premises operator, including a coffee shop, bookstore, airline, private end-user network, or other business that acquires BIAS from a BIAS provider to enable patrons to access the Internet from its respective establishment.
- 4) Defines the following terms for purposes of this Act:
  - “aggregate customer information”;
  - “customer”;
  - “customer proprietary information” (CPI);
  - “customer proprietary network information”;
  - “material change”;
  - “nonsensitive customer proprietary information”;
  - “opt-in approval”;
  - “opt-out approval”;
  - “person”;
  - “personally identifiable information”;

- “sensitive customer proprietary information”; and,
  - “Internet Web site browsing history and application usage history.”
- 5) Provides that a BIAS provider shall not use, disclose, or permit access to CPI except with the opt-out or opt-in approval of a customer, as specified, with certain, specified purposes excepted from this requirement. The approval necessary, if any, will depend on the type of information involved and the relevant purpose.
  - 6) Outlines the requirements for soliciting customer approval, including mandatory notifications and appropriate mechanisms for providing consent.
  - 7) Prohibits a BIAS provider from engaging in certain actions based on a customer’s exercise or waiver of the customer’s privacy rights.
  - 8) Clarifies that it does not limit the other statutory rights of a customer or the statutory obligations of a BIAS provider. It further provides that its requirements apply to BIAS providers operating within California when providing BIAS to their customers who are residents of and physically located in California. Any waiver by the customer of the provisions of this chapter shall be deemed contrary to public policy and shall be void and unenforceable.
  - 9) Becomes operative on January 1, 2019.

## **Background**

Since President Trump was elected, the California Legislature has been shepherding a number of measures designed to codify federal policy ahead of inevitable rollbacks by the Trump administration. For example, in order to ensure college students are protected from campus sexual violence, SB 169 (Jackson, 2017) was introduced to codify the U.S. Department of Education’s Office of Civil Rights Enforcement “Dear Colleague Letter,” which made it clear that the department considers sexual violence on campus a form of gender discrimination unlawful under Title IX. In the same vein, SB 49 (De León, 2017) establishes certain minimum federal environmental, public health, and labor standards as baselines and prohibits the corresponding California standards from falling below those baselines. Similarly, this bill seeks to reinstate privacy rules finalized by the FCC last year, but repealed recently by President Trump and the United States Congress.

## Comments

The author writes:

California Broadband Internet Privacy Act (CalBIPA) was drafted to ensure that consumers enjoy choice, transparency and security in the treatment of their personal information when accessing the internet through an Internet Service Provider (ISP). Earlier this year, Congress and the Trump Administration approved Senate Joint Resolution 34 that repealed the privacy rules adopted by the Federal Communications Commission (FCC) under President Obama to give broadband internet consumers greater control over their personal information.

These privacy rules, which were developed over the course of several years and reflected extensive public comment, were described by the FCC at the time as built on widely accepted privacy principles that would have required ISPs to provide their customers with meaningful choice, while keeping customer data secure and giving ISPs the flexibility to continue to innovate. In April, those rules were eliminated on a largely party line vote. However, the public does not see privacy as a partisan issue. One poll conducted in March of this year found that 80% of Democrats and 75% of Republicans wanted the President to veto the repeal bill and allow the FCC privacy rules to take effect. With AB 375, California is going to restore what Washington stripped away.

### *Reinstating the protections afforded by the FCC Rules and the Report and Order*

Federal law requires broadband providers to protect customer information. (47 U.S.C. Sec. 222.) The FCC sought to outline, through the rulemaking process, privacy protections that apply to sensitive data that broadband providers collect. In October 2016, after years of development,<sup>1</sup> the FCC finalized rules (FCC Rules) and published them with an attendant FCC Report and Order.<sup>2</sup> The FCC Rules provide clarity regarding telecommunications carriers' treatment of consumer information and provide consumers a measure of control over their personal information. However, before the FCC Rules could take effect, President Trump

---

<sup>1</sup> See July 5, 2017 letter of support by Congressman John Garamendi describing how the "FCC rule that Congress eliminated was developed over several years with careful consideration of extensive public comment and input from industry experts."

<sup>2</sup> See FCC Rules In the Matter of Protecting the Privacy of Customers of Broadband and other Telecommunications Services, WC Docket No. 16-106, FCC-16-148 (Oct. 27, 2016) <[https://apps.fcc.gov/edocs\\_public/attachmatch/FCC-16-148A1.pdf](https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf)> [as of Sept. 13, 2017].



and Congress killed the rules through Senate Joint Resolution 34 (Public Law 115-22).<sup>3</sup>

This bill seeks to reinstate the FCC Rules to ensure these critical consumer protections are preserved, at least for consumers who are residents of and are physically located in California. Based on the FCC Rules, and guided by the FCC Report and Order, this bill restricts Broadband Internet access service (BIAS) providers from violating the privacy rights of consumers and provides clarity regarding BIAS providers' treatment of consumer information by, for example, requiring the providers to seek consent if they intend to use the information for certain purposes.

Based on the FCC Rules, the bill prohibits a BIAS provider from refusing to provide BIAS, or in any way limiting it, to a customer who does not waive the customer's privacy rights. It also restricts BIAS providers from penalizing or incentivizing customers as a direct or indirect consequence of their decision to, or refusal to, waive privacy rights guaranteed them by law or regulation.

*Providing clear guidance on how a customer's information can be used*

Tracking the language from the FCC Rules, this bill defines "customer proprietary information" to include the following information that a BIAS provider acquires in connection with its provision of BIAS: individually identifiable customer proprietary network information; personally identifiable information; and content of communications. It further differentiates "nonsensitive" CPI from "sensitive" CPI, the latter of which includes geolocation, financial and health information; information regarding children; social security numbers; the content of communications; and Internet Web site browsing history, application usage history, and the functional equivalents of either.

Mirroring the FCC Rules, this bill prohibits a BIAS provider from using, disclosing, or permitting access to CPI except with the opt-out or opt-in approval of a customer, with limited exceptions.

A BIAS provider shall obtain *opt-out* approval from a customer to use, disclose, or permit access to any of the customer's *nonsensitive* CPI. Such approval is assumed if a customer fails to object after being provided appropriate notification. However, if a BIAS provider wishes to use, disclose, or permit access to *sensitive* CPI or to make certain material changes, it must obtain *opt-in* approval from the customer. Such approval requires the BIAS provider to obtain affirmative, express

---

<sup>3</sup> Senate Joint Resolution 34 invoked the Congressional Review Act to repeal the FCC internet service provider broadband privacy rules.

consent allowing the requested usage, disclosure, or access to the information after the customer is provided appropriate notification.

Similar to the FCC Rules, this bill requires a BIAS provider to solicit the above customer approval, as applicable, at the point of sale and when making one or more material changes to privacy policies. A BIAS provider's solicitation of customer approval shall be completely translated into a language other than English where appropriate. It shall also be clear and conspicuous, and in language that is comprehensible and not misleading. The solicitation shall disclose the types of CPI involved; the purposes for which the CPI will be used; and the categories of entities to which the BIAS provider intends to disclose or permit access to the CPI. Furthermore, a BIAS provider must make available, at no additional cost, a simple, easy-to-use mechanism for customer approval. The customer's grant, denial, or withdrawal of approval shall be given effect promptly and remain in effect until the customer revokes or limits the grant, denial, or withdrawal of approval.

Despite these requirements, BIAS providers are permitted to use, disclose, or permit access to CPI without customer approval for a number of purposes. These permissible purposes largely track what telecommunications carriers are currently permitted to do with customer data without consent as provided in 47 U.S.C. Sec. 222(d). These purposes include use of information to initiate, render, bill, and collect for BIAS; to provide inbound marketing, referral or administrative services to the customer, as specified; and to generate an aggregate customer information dataset using customer personal information.

This bill balances the important constitutional interests at stake with the practical and operational needs of BIAS providers. In addition, any operational difficulties in meeting the requirements of this bill are mitigated to a certain extent by the fact that many BIAS providers should have already begun preparing in earnest to comply with the FCC Rules, which these new requirements largely track.

**FISCAL EFFECT:** Appropriation: No Fiscal Com.: No Local: No

**SUPPORT:** (Verified 9/15/17)

Access Humboldt

American Civil Liberties Union of California

Asian Americans Advancing Justice, Los Angeles

Asian Food Trade Association

Asian Pacific Policy & Planning Council

Calegislation

California Association of Competitive Telecommunications Companies

California Alliance for Retired Americans  
California Center for Rural Policy  
California Low-Income Consumer Coalition  
California Public Interest Research Group  
Campaign for a Commercial-Free Childhood  
Center for Democracy & Technology  
Center for Digital Democracy  
Center for Media Justice  
Chinese American Community Affairs Council  
Chinese Consolidated Benevolent Association  
City and County of San Francisco  
Color of Change  
Common Sense Kids Action  
Consumer Action  
Consumer Assistance Council  
Consumer Federation of America  
Consumer Federation of California  
Consumers Union  
Consumer Watchdog  
Credo Mobile  
Cruzio Internet  
Digital Privacy Alliance  
Edwin Lee, Mayor of the City and County of San Francisco  
Electronic Frontier Foundation  
Friends of the Chinese American Museum  
John Garamendi, Member of Congress  
Giant Union Co. Inc.  
Golden Pacific Foods Inc.  
Hocean, Inc.  
Media Alliance  
New America's Open Technology Institute  
New Japan International, Inc.  
Oakland Privacy  
Online Trust Alliance  
Open Technology Institute  
Pacific Internet  
Privacy Rights Clearinghouse  
Public Law  
Roxy Trading Inc.  
Sonic

Jackie Speier, Member of Congress  
Spiral Internet  
Tekify  
Telnexus  
The Utilities Reform Network  
Mike Thompson, Member of Congress  
Unwired Ltd.  
Maxine Waters, Member of Congress  
Wilson Creek Communications  
YHS Trading, Inc.  
One individual

**OPPOSITION:** (Verified 9/15/17)

Acxiom Corporation  
Advancing the Seed, Inc.  
Altice Group  
American Advertising Federation  
American Association of Advertising Agencies  
Asian Journal Publications, Inc.  
Association of National Advertisers  
AT&T  
Auto Alliance  
Bay Area Council  
Brea Chamber of Commerce  
CalCom  
California Bankers Association  
California Black Chamber of Commerce  
California Broadcasters Association  
California Business Properties Association  
California Cable & Telecommunications Association  
California Chamber of Commerce  
California Communications Association  
California Justice Association of California  
California Latino Leadership Institute  
California Manufacturers and Technology Association  
California Restaurant Association  
California Retailers Association  
California State Association of Electrical Workers  
Camarillo Chamber of Commerce  
Cambodian-American Chamber of Commerce

Charter Communications  
Children's Resource Network of the Central Coast  
Comcast  
CompTIA  
Computing Technology Industry Association  
Consolidated Communications Inc.  
Consumer Data Industry Association  
COR Community Development Corporation  
Cox Enterprises  
CTIA  
Data & Marketing Association  
EBW Foundation  
Entertainment Software Association  
Every Community Matters Corporation  
Facebook  
Fountain Valley Chamber of Commerce  
Frontier Communications  
Google  
Greater Irvine Chamber of Commerce  
Inland Empire Economic Partnership  
Instituto de Avance Latino CDC  
Interactive Advertising Bureau  
International Franchise Association  
Internet Association  
Internet Coalition  
Latino Coalition for Community Leadership  
Liberty Mutual  
Macedonia Community Development Corporation  
Mediacom  
Motion Picture Association of America  
National Asian American Coalition  
Network Advertising Initiative  
OASIS Center International  
Oath:  
Orange County Business Council  
Oxnard Chamber of Commerce  
Rancho Cordova Chamber of Commerce  
Redondo Beach Chamber of Commerce  
Retail Industry Leaders Association  
San Gabriel Valley Economic Partnership

Santa Maria Valley Chamber of Commerce  
Satellite and Broadcast Communications Association  
Silicon Valley Leadership Group  
Southwest California Legislative Council  
South Bay Association of Chambers of Commerce  
Sprint  
State Privacy and Security Coalition  
TechNet  
T-Mobile USA  
Tracfone  
Verizon

**ARGUMENTS IN SUPPORT:** In support, a coalition of privacy rights, consumer rights, and civil liberty organizations writes:

Providers of broadband internet service have a unique and powerful role in today's online ecosystem. Their position as internet gatekeepers gives them a comprehensive view of individual consumer behavior, one that consumers cannot readily avoid or shield themselves from when they use necessary internet services. The power of the internet service provider is further enhanced by the lack of competition that presently exists for high-speed access. According to the latest FCC data, 41 percent of Americans have only one company offering high-speed broadband access in their community.

As the role of the internet in the daily lives of consumers increases, this means an increased potential for data collection of personal information and sensitive facts about one's daily life. The shadow of surveillance can create a chilling effect on speech, association, and online commerce, and even increase the potential for data-driven discrimination, governmental overreach, and the theft of highly personal information. By contrast, strong protections that enhance Californians' confidence would encourage greater adoption and use of the internet, as individual comfort and trust leads individuals to conduct even more of their everyday business online.

...

In the face of retreat by the federal government and the robust demands of voters, California must respond to the will of the public and restore the protections created by the FCC in 2016 that Congress and the President so thoughtlessly stripped away.

The California Low-Income Consumer Coalition writes in support of the so-called "pay-for-privacy" provisions: "Privacy is a constitutional right in our state –

guaranteed in the very first section of our Constitution – and fundamental rights are not things to be charged for or bartered away. Low-income Californians and people of color are particularly vulnerable to such false ‘bargains.’”

**ARGUMENTS IN OPPOSITION:** A coalition of internet service providers, including AT&T, Verizon, T-Mobile, and Sprint, among others, writes in opposition:

The bill is an overreaction to Congressional action repealing privacy rules passed by the Federal Communications Commission that were never in effect. Importantly, Congressional action did nothing to take away existing privacy protections from consumers, including protections in Section 222 of the Communications Act.

AT&T specifically notes that the “imposition of onerous privacy regulations solely on Internet service providers – and not other companies that collect and use consumer data – would give consumers a false sense of security that their online privacy is being protected. As federal and state governments have long recognized, consumer privacy laws should be based on the sensitivity of the data involved and how it is being used, not the company holding the data.”

A coalition of advertising and marketing associations, including the Data & Marketing Association, Association of National Advertisers, and American Advertising Federation writes the following in opposition:

The recent repeal of the [FCC] Broadband Privacy Rules does not mean that consumers will be left unprotected. In fact, Internet Service Providers (“ISPs”) have been and will continue to be substantially regulated at the federal level. Prior to the FCC’s decision to adopt the Broadband Privacy Rules, it issued a wide-ranging enforcement advisory opinion, making it clear that the Communications Act (Section 222) applies to ISPs. The guidance continues to apply today.

**ASSEMBLY FLOOR:** 77-0, 5/11/17

**AYES:** Acosta, Aguiar-Curry, Travis Allen, Arambula, Baker, Berman, Bigelow, Bloom, Bocanegra, Bonta, Brough, Burke, Caballero, Calderon, Cervantes, Chau, Chávez, Chen, Chiu, Choi, Chu, Cooley, Cooper, Cunningham, Dababneh, Daly, Eggman, Flora, Fong, Frazier, Friedman, Gallagher, Cristina Garcia, Eduardo Garcia, Gipson, Gloria, Gomez, Gonzalez Fletcher, Gray, Grayson, Harper, Holden, Irwin, Jones-Sawyer, Kalra, Kiley, Lackey, Levine, Limón, Low, Maienschein, Mathis, Mayes, McCarty, Medina, Melendez, Mullin, Muratsuchi, Nazarian, Obernolte, Quirk, Quirk-Silva, Reyes, Ridley-

Thomas, Rodriguez, Rubio, Salas, Santiago, Steinorth, Mark Stone, Thurmond,  
Ting, Voepel, Waldron, Weber, Wood, Rendon  
NO VOTE RECORDED: Dahle, O'Donnell, Patterson

Prepared by: Christian Kurpiewski / Margie Estrada / JUD. / (916) 651-4113  
9/15/17 18:20:46

\*\*\*\* **END** \*\*\*\*