March 28, 2022

TO: Members, Senate Judiciary Committee

SUBJECT: SB 1189 (WIECKOWSKI) BIOMETRIC INFORMATION
OPPOSE/JOB KILLER – AS INTRODUCED FEBRUARY 17, 2022
SCHEDULED FOR HEARING – APRIL 5, 2022

The California Chamber of Commerce and the undersigned organizations respectfully **OPPOSE SB 1189 (Wieckowski)** as introduced February 17, 2022, as a **JOB KILLER** because it imposes new, untenable restrictions on the use and disclosure of biometric information in a manner that would undermine the California Privacy Rights Act (CPRA) limited private right of action for data breaches. **SB 1189** will create legal liability for businesses large and small potentially in the millions to tens of millions of dollars while not providing any exceptions such as for the use of biometric data for safety, security, or other reasonable purposes. The CPRA is a comprehensive, industry neutral, technology neutral, and measured statutory scheme that already provides strong consumer privacy protections around the collection, use, and disclosure of all Californians' personal information – including biometric information. Notably, states that have enacted biometric information specific laws like this bill *all* lack a comparable statute to the CPRA, and only one of those states includes a private right of action in their biometric information law: Illinois.[1]

Despite California's existing protections for biometric information, **SB 1189** seeks to: (1) expand the definition of biometric data from that in the CPRA to capture even technology that can be used – but is *not* used or intended to be used – to establish individual identity; (2) prohibit the collection or disclosure of biometric data without first acquiring informed affirmative consent from the individual from whom the biometric data is collected; (3) prohibit a business from ever profiting from a person's biometric data; and, (4) establish a new private right of action that authorizes not only punitive damages, but also the greater of either actual damages or statutory damages. There are several practical consequences of these proposed changes that should be seriously considered:

- Results in Onslaught of Class Actions with No Harm Needed

  SB 1189 poses significant liability risks to businesses, opening the floodgates to potentially abusive class action lawsuits that are based on minor, technical violations, instead of actual injury. This is not just a matter of speculation. One need only look to Illinois' Biometric Information Privacy Act (BIPA) to see the avalanche of class action lawsuits that would ensue, often for minor technical

[1] Illinois, Texas, and Washington have biometric specific bills whereas California, Colorado, Virginia, and Utah have more expansive privacy acts protecting personal information. Of the three, only Illinois's Biometric Information Practices Act includes a private right of action.

violations which resulted in no harm to the individual who knew that their biometric information was being used and the purpose for that use (such as where a person knows their fingerprint is scanned to clock in and out of work). Illinois has seen over 1,100 class action suits against companies of all types and sizes since 2017. According to the National Law Review, BIPA cases in 2021 "settled in the six-, seven-, eight-, and even nine-figure ranges, even in cases where there have been no allegations that the plaintiffs' biometric data was hacked or improperly accessed by a nefarious third party."[2] That is what this bill is ultimately about, not affirmative consent.

- Leads to Limitations and Removal of Products and Operations

  SB 1189 will invariably result in some businesses having to either remove certain lines of business operations, if not their entire business, from California not only because of the liability risks illustrated above, but also because it prohibits a private entity from making any profit from a person's biometric data. There is an important distinction between prohibiting monetization of biometric data unrelated to the business purpose for which the consumer shared that data with a business and, as a practical matter, precluding certain businesses from using that information even upon receipt of affirmative consent by prohibiting them from making any profit from biometric information. This bill does the latter. That places a business in the untenable position of either violating the law subject to significant liability or providing their services and products for free.

  As we have seen happen in Illinois, **SB 1189** will most certainly lead to limitation or the removal of certain companies or products from the market that currently provide significant benefit to Californians, such as helping provide security through doorbells; preventing identity fraud through use of voice recognition systems; preventing overdoses by way of technology that safely dispenses medicine using biometrics; preventing theft at bank ATMs or securing entire facilities or locations holding sensitive data by way of tools such as fingerprint scanners; helping persons with blindness with their surroundings, including by identifying friends and family through use of facial recognition technology; and more.

- Creates Confusion in Operability

  SB 1189 creates confusion not only in terms of operability with the CPRA by providing alternate and conflicting restrictions around the use and disclosure of this specific type of personal information, but also in terms of conflicts between its own provisions. Namely, the bill prohibits the disclosure of biometric information unless certain conditions are met, including: "*The disclosure completes a financial transaction requested or authorized by the subject of the biometric information* or the subject's legally authorized representative." In another provision, however, the bill states that "[a] private entity shall not sell, lease, trade, use for advertising purposes, *or otherwise profit from a person's biometric information*." (*Compare* proposed section 1798.304 to proposed section 1798.303; emphases added.) Disclosing a person's biometric information to complete a financial transaction would likely constitute "a profit from a person's biometric information". In other words, in fulfilling the consumer's express request consistent with this bill, the entity will have exposed itself to significant liability under the bill as well.

- Results in Overbroad Application

  SB 1189 will needlessly capture existing technologies that are not used, nor ever intended to be used, to identify a particular individual by expanding the definition of biometric information used in the CPRA. Consider for example filter technologies that can place silly animal ears, makeup, or sunglasses on a person using facial geometry measurements– those would appear to fall within the scope of this bill simply because the technology involved could theoretically be used to identify a person, ignoring the fact that it is never used or even intended to be used to identify the individual using the filter. Imagine now if a user then turns their camera to apply a filter to another person's face without forewarning, and that person has not provided affirmative consent. Stated another way, this bill exposes companies that do not gather biometric information to potentially crippling litigation.

[2] Class Action Cases Continue for Illinois BIPA (natlawreview.com)

- Fails to Include Reasonable Limitations

  Even if affirmative consent is generally justified, **SB 1189** fails to recognize situations warranting reasonable exemptions. As a matter of public policy, it is not always beneficial or appropriate to mandate advance affirmative consent when the outcome would result in outrageous circumstances such as domestic violence shelters needing to obtain express written consent from abusers to use security technology like security cameras or video doorbells to identify security threats; businesses requiring the consent of criminals to use fingerprint technologies to prevent entry of unauthorized personnel or keep airports safe; or the like. Particularly given the extensive protections that exist at law under the CPRA for this information, the negative consequences of this bill clearly outweigh any benefit it might hope to create.

These overbroad, inconsistent, and unnecessary proposed requirements will potentially eliminate consumer products, expose companies to costly class action litigation, and discourage or limit their workforce in California.

For these reasons, we respectfully **OPPOSE SB 1189 (Wieckowski)** as a **JOB KILLER**.

Sincerely,

Ronak Daylami
Policy Advocate
California Chamber of Commerce
on behalf of

American Property Casualty Insurance Association – Denneile Ritter
Association of National Advertisers – Christopher Oswald
California Chamber of Commerce – Ronak Daylami
California Bankers Association – Melanie Cuevas
California Business Properties Association – Matthew Hargrove
California Land Title Association – Anthony Helton
California Retailers Association – Margaret Gladstein
California Trucking Association – Nick Chiappe
Cemetery and Mortuary Association of California – Jerry Desmond
Civil Justice Association of California – Jaime Huff
Electronic Transactions Association – Max Behlke
Insights Association – Howard Fienberg
NetChoice – Carl Szabo
Plumbing Manufacturers International – Jerry Desmond
Security Industry Association – Don Ericson
Software & Information Industry Association – Divya Sridhar
State Privacy & Security Coalition – Andrew Kingman
TechNet – Dylan Hoffman
Technology Industry Association – Madeline Cline

cc: Legislative Affairs, Office of the Governor
Carlos Puentes, Office of Senator Wieckowski
Consultant, Senate Judiciary Committee
Morgan Branch, Consultant, Senate Republican Caucus