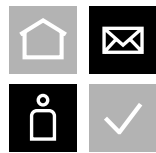


★ ★ ★ ★ ★ **OFFICIAL VOTER INFORMATION GUIDE** ★ ★ ★ ★ ★

California General Election

Tuesday, November 3, 2020

Polls Are Open From 7:00 a.m. to 8:00 p.m. on Election Day!



VOTE SAFE

C A L I F O R N I A

Every registered voter in California will receive a vote-by-mail ballot in the General Election. Learn more about changes to the election inside.



Certificate of Correctness

I, Alex Padilla, Secretary of State of the State of California, do hereby certify that the measures included herein will be submitted to the electors of the State of California at the General Election to be held throughout the State on November 3, 2020, and that this guide has been correctly prepared in accordance with the law. Witness my hand and the Great Seal of the State in Sacramento, California, this 10th day of August, 2020.

Alex Padilla, Secretary of State

QUICK REFERENCE GUIDE

**PROP
24**

**AMENDS CONSUMER PRIVACY LAWS.
INITIATIVE STATUTE.**

SUMMARY

Put on the Ballot by Petition Signatures

Permits consumers to: prevent businesses from sharing personal information, correct inaccurate personal information, and limit businesses' use of "sensitive personal information," including precise geolocation, race, ethnicity, and health information. Establishes California Privacy Protection Agency. Fiscal Impact: Increased annual state costs of at least \$10 million, but unlikely exceeding low tens of millions of dollars, to enforce expanded consumer privacy laws. Some costs would be offset by penalties for violating these laws.

WHAT YOUR VOTE MEANS

YES A YES vote on this measure means: Existing consumer data privacy laws and rights would be expanded. Businesses required to meet privacy requirements would change. A new state agency and the state's Department of Justice would share responsibility for overseeing and enforcing state consumer privacy laws.

NO A NO vote on this measure means: Businesses would continue to be required to follow existing consumer data privacy laws. Consumers would continue to have existing data privacy rights. The state's Department of Justice would continue to oversee and enforce these laws.

ARGUMENTS

PRO YES ON PROP. 24 TO STRENGTHEN PRIVACY RIGHTS
Parents, Common Sense Media, the California NAACP and a Nobel Prize winning economist say vote YES on PROP. 24. Make privacy laws stronger! Protect kids online! Strengthen privacy laws and hold corporations accountable when they violate your fundamental rights. YES ON PROP. 24!

CON Proposition 24 reduces your privacy rights in California. Proposition 24 allows "pay for privacy" schemes, makes workers wait years to learn what confidential information employers collect on them, and makes it harder to stop tech giants from selling your information. Proposition 24 was written behind closed doors with input from social media corporations.

FOR ADDITIONAL INFORMATION

FOR

Robin Swanson
Californians for Consumer Privacy
1020 16th Street #31
Sacramento, CA 95814
(916) 440-0424
info@caprivacy.org
www.caprivacy.org

AGAINST

Californians For Real Privacy
CaliforniansForRealPrivacy.org
mail@RealPrivacyNoOn24.org
(415) 634-0335

**PROP
25**

**REFERENDUM ON LAW THAT REPLACED
MONEY BAIL WITH SYSTEM BASED ON
PUBLIC SAFETY AND FLIGHT RISK.**

SUMMARY

Put on the Ballot by Petition Signatures

A "Yes" vote approves, and a "No" vote rejects, law replacing money bail with system based on public safety and flight risk. Fiscal Impact: Increased costs possibly in mid hundreds of millions of dollars annually for a new process for release from jail prior to trial. Decreased county jail costs, possibly in high tens of millions of dollars annually.

WHAT YOUR VOTE MEANS

YES A YES vote on this measure means: No one would pay bail to be released from jail before trial. Instead, people would either be released automatically or based on their assessed risk of committing another crime or not appearing in court if released. No one would be charged fees as a condition of release.

NO A NO vote on this measure means: Some people would continue to pay bail to be released from jail before trial. Other people could continue to be released without paying bail. Fees may continue to be charged as a condition of release.

ARGUMENTS

PRO Yes on 25 replaces money bail with a fairer, safer and less costly process. Currently, if a person can afford to pay a bail bond company, they go free until trial. If they can't afford to pay, even if they're innocent, they stay in jail. That's blatant discrimination. Vote YES.

CON Prop. 25 was written by Sacramento politicians to take away every Californian's option to post bail and replaces this right with a new DISCRIMINATORY system of computer-generated PROFILING administered by government bureaucrats—costing taxpayers hundreds of millions of dollars a year. Prop. 25 is unfair, unsafe and costly. Vote NO on Prop. 25.

FOR ADDITIONAL INFORMATION

FOR

Yes on Prop. 25, End Money Bail
1130 K Street, Suite 300
Sacramento, CA 95814
(213) 373-5225
info@yesoncaprop25.com
yesoncaprop25.com

AGAINST

No on Prop. 25—Stop the Unfair, Unsafe and Costly Bailot Proposition
(916) 209-0144
info@stopprop25.com
StopProp25.com

PROPOSITION
24 AMENDS CONSUMER PRIVACY LAWS.
INITIATIVE STATUTE.

OFFICIAL TITLE AND SUMMARY

PREPARED BY THE ATTORNEY GENERAL

The text of this measure can be found on the Secretary of State's website at voterguide.sos.ca.gov.

- Permits consumers to: (1) prevent businesses from sharing personal information; (2) correct inaccurate personal information; and (3) limit businesses' use of "sensitive personal information"—including precise geolocation; race; ethnicity; religion; genetic data; private communications; sexual orientation; and specified health information.
- Establishes California Privacy Protection Agency to additionally enforce and implement consumer privacy laws and impose fines.
- Changes criteria for which businesses must comply with laws.
- Prohibits businesses' retention of personal information for longer than reasonably necessary.
- Triples maximum penalties for violations concerning consumers under age 16.
- Authorizes civil penalties for theft of consumer login information, as specified.

SUMMARY OF LEGISLATIVE ANALYST'S ESTIMATE OF NET STATE AND LOCAL GOVERNMENT FISCAL IMPACT:

- Increased state costs of at least \$10 million annually for a new state agency to oversee and enforce consumer privacy laws.
- Increased state costs, not likely to exceed the low millions of dollars annually, for increased court and Department of Justice enforcement workload. Some or all of these costs would be paid by penalties collected for violations of consumer privacy laws.
- Unknown impact on state and local tax revenues due to economic effects resulting from new requirements on businesses to protect consumer data.

ANALYSIS BY THE LEGISLATIVE ANALYST

BACKGROUND

BUSINESSES COLLECT AND USE CONSUMER DATA

Businesses collect data about consumers from different sources. These include (1) public sources, (2) consumers themselves (such as when consumers create an account), or (3) other businesses (such as by purchasing data). Businesses use the data in different ways, such as to improve their sales or customer service. Businesses can also use the data to provide services to other businesses. For example, some Internet companies provide free services and collect data from consumers who use them. These companies then use the data to target ads at consumers for other businesses. Finally, businesses sometimes use data to make predictions about consumers' views and preferences (such as their lifestyles).

CERTAIN BUSINESSES MUST MEET CONSUMER DATA PRIVACY REQUIREMENTS

Under state law, certain businesses that operate in California and collect personal data must meet consumer data privacy requirements. (Personal data include information such as names, Internet or purchase activity, and predictions about consumers.) These businesses generally (1) earn more than \$25 million in annual revenue; (2) buy, sell, or share the personal data of 50,000 or more consumers, households, or devices annually; or (3) earn 50 percent or more of their annual revenues from selling personal data.

Specifically, these businesses must:

- **Notify Consumers of Data Collection.** Businesses generally must tell consumers if they collect or sell personal data. They must also tell consumers how they will use the data.

ANALYSIS BY THE LEGISLATIVE ANALYST

CONTINUED

- ***Comply With Personal Data Privacy Rights.*** State law provides consumers with certain rights that businesses must comply with. For example, consumers can request free reports on their personal data that are collected or sold by the business. Consumers can also generally tell businesses to delete their personal data (such as names or student grades and testing results). Finally, consumers can tell businesses to not sell their personal data. Businesses must tell consumers of their personal data rights.
- ***Not Treat Consumers Who Make Use of Their Rights Differently.*** For example, businesses cannot charge different prices or provide different levels of service to consumers who make use of their personal data rights. However, businesses can encourage consumers to allow them to collect and sell personal data, such as by providing consumers payments or discounts.

Businesses can face penalties of up to \$2,500 for each violation of these requirements. Penalties increase to up to \$7,500 for intentional violations. Penalties only may be applied if businesses fail to address the violation within 30 days of being told of the violation. Only the California Department of Justice (DOJ) can seek these penalties. Penalty revenues are generally deposited into the state's Consumer Privacy Fund (CPF). CPF revenues must first be used to pay for state trial court and DOJ costs related to certain consumer privacy laws. The Legislature can allocate any remaining funds for other purposes.

BUSINESSES MUST MEET DATA BREACH REQUIREMENTS

A data breach occurs when people access information, such as consumer data, without permission. State law requires businesses take reasonable steps to protect consumer data from breaches. Businesses must also tell people if their data were accessed in a data breach. Breaches of certain personal data can result in penalties of \$100 to \$750 per consumer per event or actual damages—whichever is greater. A consumer

affected by such a breach can seek to collect these penalties if a business fails to address the breach within 30 days of being told to do so. DOJ may also generally seek penalties for data breaches. Some of these penalties could be deposited into the CPF.

DOJ ENFORCES CONSUMER PRIVACY AND DATA BREACH LAWS

DOJ enforces the state's consumer privacy and data breach laws in two major ways. First, DOJ develops regulations that provide more details on how businesses and consumers must obey the laws. For example, these regulations include rules for how businesses must handle requests to not sell personal data. Second, DOJ prosecutes crimes (such as identity theft) or files lawsuits in state trial courts against those who break these laws.

PROPOSAL

Proposition 24 (1) changes existing consumer data privacy laws, (2) provides new consumer privacy rights, (3) changes existing penalties and limits the use of penalty revenues, and (4) creates a new state agency to oversee and enforce consumer data privacy laws. If approved, most of this proposition would take effect in January 2023. Some portions of the proposition, such as the creation of the new state agency and requirements for developing new regulations, would go into effect immediately.

CHANGES EXISTING CONSUMER DATA PRIVACY LAWS

Changes Which Businesses Must Meet Data Privacy Requirements. This proposition changes which businesses are required to meet state consumer data privacy requirements. These changes would generally reduce the number of businesses required to meet these requirements. For example, consumer data privacy requirements currently apply to businesses that buy, sell, or share for business purposes the personal data of 50,000 or more consumers, households, or devices annually. The proposition (1) no longer counts devices and (2) increases the annual threshold to 100,000 or more consumers or households.

ANALYSIS BY THE LEGISLATIVE ANALYST

CONTINUED

Changes Existing Consumer Data Privacy

Requirements. This proposition changes the consumer data privacy requirements that businesses must meet. In some cases, it adds new requirements. For example, the proposition requires businesses to now notify consumers of the length of time they will keep personal data. In other cases, it removes requirements. For example, businesses could refuse to delete student grades or other information under specific conditions.

PROVIDES NEW CONSUMER PRIVACY RIGHTS

This proposition provides consumers with new data privacy rights. These include the right to:

- **Limit Sharing of Personal Data.** Consumers could direct businesses to not share their personal data.
- **Correct Personal Data.** Consumers could direct businesses to take reasonable efforts to correct personal data that they possess.
- **Limit Use of “Sensitive” Personal Data.** The proposition defines certain pieces of personal data as sensitive. Examples include social security numbers, account log-ins with passwords, and health data. Consumers could direct businesses to limit use of their sensitive personal data only to (1) provide requested services or goods and (2) fulfill key business purposes (such as providing customer service).

CHANGES EXISTING PENALTIES AND LIMITS USE OF PENALTY REVENUES

This proposition permits a new penalty of up to \$7,500 for violations of the consumer privacy rights of minors. The proposition also eliminates the ability of businesses to avoid penalties by addressing violations within 30 days of being told of the violation. In addition, the proposition makes data breaches of email addresses along with information that would permit access to an account (such as a password) subject to penalties. The proposition also specifies that businesses which suffer a data breach because reasonable security procedures were not in place can no longer avoid

penalties by putting them in place within 30 days after the breach.

In addition, the proposition limits the Legislature’s ability to use CPF revenues for purposes other than consumer privacy. After paying for state trial court and DOJ costs each year, the proposition requires 91 percent of the remaining funds be invested by the state with any interest or earnings sent to the state General Fund. The remaining 9 percent of funds would support public education on consumer privacy and fighting fraud resulting from data breaches.

CREATES NEW STATE ENFORCEMENT AGENCY

This proposition creates a new state agency, the California Privacy Protection Agency (CPPA), to oversee and enforce the state’s consumer privacy laws. CPPA would be governed by a five-member board and have a wide range of responsibilities. For example, the agency would investigate violations, assess penalties, and develop regulations. Any CPPA decision related to a complaint against a business or a penalty could be reviewed by the state trial courts. This proposition provides \$10 million annually (adjusted over time) from the state General Fund to support the agency’s operations. Some of DOJ’s current responsibilities would be shifted to CPPA, such as developing regulations. The proposition requires the development of a wide range of new regulations. For example, this includes rules for correcting consumer personal data and determining whether businesses must carry out a review of their ability to protect data. However, DOJ could still enforce consumer data privacy laws by prosecuting crimes and filing lawsuits in the state trial courts. If DOJ chooses to take such action or pursue an investigation, DOJ could direct CPPA to stop any investigations or enforcement activities the agency might be pursuing at the same time.

FISCAL EFFECTS

Proposition 24 would impact state costs and state and local tax revenues. The actual size of these effects, however, is uncertain and would

ANALYSIS BY THE LEGISLATIVE ANALYST

CONTINUED

depend largely on how consumers, businesses, and government respond to the proposition. For example, it is unclear how businesses would change their operations and how many violations of this proposition would be investigated and result in penalties.

Increased State Costs for New Agency. As discussed above, this proposition creates a new state agency to oversee and enforce consumer privacy laws. While some workload would shift from DOJ, state costs would also increase because of new or expanded workload. This proposition provides from the state General Fund at least **\$10 million annually** (adjusted over time) to support increased state costs for CPPA operations. This amount is less than 1 percent of the state's current General Fund budget. Depending on how the agency carries out its responsibilities, it is possible that CPPA's actual workload costs could be higher.

Increased State DOJ and Court Costs. This proposition would impact both DOJ and state court workload. DOJ workload could increase if it chooses to investigate and/or file more cases against businesses that do not meet state consumer data privacy laws. However, this workload could be partially or fully offset by reductions in workload from shifting responsibilities from DOJ to CPPA. Additionally, state court workload could increase if the proposition results in more court cases being filed. The costs of the increased workload would depend on the number of investigations started and the types of cases filed in state courts. In total, increased state costs to DOJ and trial courts are not likely to exceed the low millions of dollars annually. Some or all of these costs would be paid by increased revenue from penalties collected from businesses that violate consumer privacy laws.

Potential Impacts on Tax Revenues. The proposition would have various impacts on business and consumers, which could then impact state and local tax revenues. On the one hand, the proposition could reduce tax revenues. This would happen if the cost of meeting the proposition's requirements, such as to correct consumer data, reduces the profit earned by businesses. As a result, businesses would pay less in taxes to state and local governments. On the other hand, the proposition could increase tax revenues. For example, this proposition could reduce the severity or number of data breaches. If this results in businesses and consumers losing less money, tax revenues would increase if consumers then spend more on taxable items and/or businesses earn more revenue. The total net impact on the economy and state and local revenue is unknown.

Visit <http://cal-access.sos.ca.gov/campaign/measures/> for a list of committees primarily formed to support or oppose this measure.

Visit <http://www.fppc.ca.gov/transparency/top-contributors.html> to access the committee's top 10 contributors.

If you desire a copy of the full text of this state measure, please call the Secretary of State at (800) 345-VOTE (8683) or you can email vigfeedback@sos.ca.gov and a copy will be mailed at no cost to you.

★ ARGUMENT IN FAVOR OF PROPOSITION 24 ★

The world's biggest corporations are collecting deeply personal and private information about all of us. Sadly, our current laws aren't strong enough to protect us or our families from those who would abuse our most personal information.

In 2018, the Legislature enacted the California Consumer Privacy Act. But since then, industry has repeatedly tried to weaken and limit enforcement of this law.

Consumers need stronger protections. That's why we've introduced the California Privacy Rights Act of 2020, to strengthen current privacy laws.

In addition to monitoring our kids, many corporations track us constantly, from gym to office to clinic; they know our friends, jobs, weight, where we eat and how fast we're driving, our private searches and what we look at online. They also track and sell sensitive information like our race, sexual orientation, and religion.

We believe we should be in control of our own information, and have the right to stop the use of our most sensitive personal information.

OUR PERSONAL INFORMATION—AND OUR CHILDREN'S—IS BEING ABUSED:

Giant corporations make billions buying and selling our personal information—apps, phones, and cars sell your location constantly. The California Privacy Rights Act gives you the power to stop businesses tracking you precisely, like selling how many times you go to the gym or fast food restaurants to health insurers—without your knowledge or permission.

Worse, these corporations don't keep your information safe. In 2018, there were a whopping 1,244,000,000 data breaches in the U.S., with over 446,000,000 records exposed, leading to massive identity theft. This measure holds big businesses accountable by imposing huge fines if they're negligent and don't keep your or your kids' health information, or Social Security numbers safe.

THE CALIFORNIA PRIVACY RIGHTS ACT WOULD:

1. **PROTECT YOUR MOST PERSONAL INFORMATION**, by allowing you to prevent businesses from using or sharing sensitive information about your health, finances, race, ethnicity, and precise location;

2. **Safeguard young people, TRIPLING FINES** for violations involving children's information;

3. **Put new limits on companies' collection and use of our personal information**;

4. **Establish an enforcement arm—the California Privacy Protection Agency—to defend these rights and hold companies accountable, and extend enforcement including IMPOSING PENALTIES FOR NEGLIGENCE** resulting in theft of consumers' emails and passwords.

5. **MAKE IT MUCH HARDER TO WEAKEN PRIVACY** in California in the future, by preventing special interests and politicians from undermining Californians' privacy rights, while allowing the Legislature to amend the law to further the primary goal of strengthening consumer privacy to better protect you and your children, such as opt-in for use of data, further protections for uniquely vulnerable minors, and greater power for individuals to hold violators accountable. **VOTE YES ON PROP. 24 TO SUPPORT THE CALIFORNIA PRIVACY RIGHTS ACT:**

California led the nation in enacting privacy rights, but big corporations are spending millions lobbying to weaken our laws. Instead, we need to make California privacy laws stronger. We need to safeguard our privacy protections, and hold corporations accountable when they violate our fundamental rights.

For more information, visit: www.caprivacy.org.

Please join us and **VOTE YES ON PROP. 24.**

JAMES P. STEYER, CEO
Common Sense Media

ALICE A. HUFFMAN, President
California NAACP

CELINE MACTAGGART, Director
Californians for Consumer Privacy

★ REBUTTAL TO ARGUMENT IN FAVOR OF PROPOSITION 24 ★

We work every day to protect the rights of all Californians. We **OPPOSE** Proposition 24 because it stacks the deck in favor of big tech corporations and reduces your privacy rights.

If Proposition 24 **REALLY** strengthened privacy protections, we'd fight for it. But the truth is, its 52 pages are full of giveaways to social media and tech giants.

Proposition 24's funder hopes you won't read its fine print. If you do, you'll see it reduces your rights under current law, giving big tech businesses new ways to collect your private information, like data from health and financial apps, and tracking where you go.

Proposition 24 asks you to approve "pay for privacy," letting companies charge more to safeguard your personal information. It's hard enough for financially strapped Californians to access high-speed internet for essential services, healthcare, and school during a pandemic. Pay for privacy has racially discriminatory impacts, disproportionately pricing out working people, seniors, and

Black and Latino families. All Californians deserve privacy, not just the wealthy.

Proposition 24 restricts Californians from enforcing your own privacy rights in court. It wants you to trust a brand new state agency, created during a budget crunch, to protect your rights.

Proposition 24 was written behind closed doors with input from the same tech companies with histories of profiting off of your personal information in unfair and discriminatory ways. It puts more power in the hands of tech companies like Facebook that already have too much power. It protects big tech business, not people. **Vote NO on Proposition 24.**

KEVIN BAKER, Director
Center for Advocacy and Policy, American Civil Liberties Union (ACLU) of California

NAN BRASMER, President
California Alliance for Retired Americans

JOHN MATHIAS, Deputy Senior Campaign Director
Color of Change

★ ARGUMENT AGAINST PROPOSITION 24 ★

Vote NO on Proposition 24 because it was written behind closed doors with input from giant tech corporations that collect and misuse our personal information—while the measure's sponsor rejected almost every suggestion from 11 privacy and consumer rights groups. Proposition 24 reduces privacy protections by severely weakening your rights under current California law.

Make no mistake—the privacy of every Californian is at stake!

The real winners with Proposition 24 are the biggest social media platforms, giant tech companies and credit reporting corporations who get more freedom to invade the privacy of workers and consumers, and to continue sharing your credit data. Here's what they won't tell you about the 52 pages of fine print:

Proposition 24 asks you to approve an Internet “pay for privacy” scheme. Those who don't pay more could get inferior service—bad connections, slower downloads and more pop up ads. It's an electronic version of freeway express lanes for the wealthy and traffic jams for everyone else.

Currently, employers can obtain all kinds of personal information about their workers and even job applicants, including things like using a pregnancy tracking app, where you go to worship or if you attend a political protest. Proposition 24 allows employers to continue secretly gathering this information for more years to come, overriding a new law that lets workers know what sensitive private information their bosses have beginning January 1, 2021.

Under California law, your privacy rights follow you wherever you go. But with Proposition 24, the minute you travel out of state with a phone, wearable device, or computer, big tech companies are allowed to capture the health, financial,

and other confidential information you stored on your device.

You can set web browsers and cell phones to send a signal to each website you visit and app you use to stop selling your personal data, so you don't have to think about it each time. Proposition 24 would allow companies to disregard those instructions and shift the burden to you to notify each and every website and app individually to protect your data. Proposition 24's new enforcement agency sounds good, but when tech corporations get caught violating your privacy, all they have to do is cooperate with the agency and their only penalty could be a slap on the wrist.

California's new privacy law just took effect this year. Smaller businesses spent a lot of money to comply with the new regulations. Before we even know how this new law is working, Proposition 24 rewrites it, forcing smaller businesses to absorb even more costs at a time that the economic slowdown has many businesses on the verge of closing their doors.

Proposition 24 was written to accommodate big social media platforms and the Internet and technology companies that spend tens of millions of dollars a year to lobby government at all levels to avoid laws that hurt their profits. Proposition 24 is a bonanza for them—and a big step back for consumer privacy. Please Vote NO on Proposition 24.

www.CaliforniansForRealPrivacy.org

TRACY ROSENBERG, President
Californians for Privacy Now

RICHARD HOLOBER, President
Consumer Federation of California

DOLORES HUERTA, Labor and Civil Rights Leader

★ REBUTTAL TO ARGUMENT AGAINST PROPOSITION 24 ★

COMMUNITY LEADERS SUPPORT PROP. 24

Prop. 24 allows the Legislature to pass stronger privacy laws, including stricter prohibitions on companies treating consumers differently for their privacy choices.

YES ON 24 TO STOP ATTEMPTS TO WEAKEN PRIVACY

“I have witnessed many attempts to weaken California's privacy laws by deceptively named groups. Prop. 24 protects sensitive personal information, children's privacy, and helps stop identity theft. It's even stronger than the California Consumer Privacy Act. Please vote YES on Prop. 24.”—*Senator Robert M. Hertzberg, Joint Author, California Consumer Privacy Act*

YES ON 24 TO SUPPORT ECONOMIC FAIRNESS

“Monopolies like Facebook and Google make enormous profits by using your private information to manipulate what you see online. Vote YES on PROP. 24, to take back control over your most valuable commodity: your personal information.”—*Paul Romer, Nobel Prize Winner in Economics*

YES ON 24 TO STOP RACIAL PROFILING ONLINE

“Prop. 24 allows consumers to stop companies from using online racial profiling to discriminate against them.”
—*Alice Huffman, President, California NAACP*

YES ON 24 TO PROTECT HEALTH DATA

“Stop businesses using your most personal health information without your permission. Vote yes on Prop. 24.”—*Brad Jacobs, MD, Past Chair, Academy of Integrative Health & Medicine*

YES ON 24 TO STRENGTHEN CALIFORNIA PRIVACY LAWS

“We are pleased that the California Privacy Rights Act would close loopholes, strengthen enforcement, and help prevent the Legislature from weakening the measure.”

—*Maureen Mahoney, PhD, Consumer Reports*

YES ON 24 TO PROTECT KIDS ONLINE

“Kids are spending so much time online this year! Protect them by voting YES on Prop. 24, which triples fines for violating children's privacy.”—*Alex Traverso, President, Theodore Judah PTA*

JAMES P. STEYER, CEO
Common Sense Media

ALICE A. HUFFMAN, President
California NAACP

CELINE MACTAGGART, Director
Californians for Consumer Privacy