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.