Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Riding California's wave of regulatory developments

An e-Book publication sponsored by JUMIO

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

JUMIO®

Jumio offers end-to-end identity verification and authentication solutions that help businesses fight fraud, meet compliance mandates (e.g., AML and KYC) and onboard good customers faster. Jumio uses augmented intelligence, AI, machine learning, 3D liveness detection and expert human review to quickly and reliably verify a user's online identity and answer the fundamental question—are you really you? www.jumio.com

Inside this e-Book

California first to enact a take on EU data protections

California has passed an extensive slate of data privacy rules that take their cue from the EU's General Data Protection Regulation. **Joe Mont** reports.

California, home to many of the world's top tech firms, has become the first state in the nation to enact a law that, in large part, mirrors the data protection and privacy standards of the European Union General Data Protection Regulation.

In June, Gov. Jerry Brown signed the bill, the California Consumer Privacy Act of 2018, into law. It empowers consumers to control how companies use, sell, or share their personal data. Similar to the recently passed EU standards, California customers will also have the right to demand that specific data be deleted from an online enterprise's databases.

The legislation builds upon longstanding privacy protections in the state.

In 1972, California voters amended the California Constitution to include the right of privacy among the "inalienable" rights of all people. "Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information," it says.

Subsequently, the California legislature adopted measures to safeguard resident's privacy, including the Online Privacy Protection Act, the Privacy Rights for California Minors in the Digital World Act, and Shine the Light, a California law intended to provide residents the "who, what, where, and when' of how businesses handle consumers' personal information.'

California, a prologue to the 2018 bill explains, "is one of the world's leaders in the development of new technologies and related industries."

"Yet the proliferation of personal information has limited Californians' ability to properly protect and safeguard their privacy," it adds. "It is almost impossible to apply for a job, raise a child, drive a car, or make an appointment without sharing personal information. As the role of technology and data in the daily lives of consumers increases, there is an increase in the amount of personal information shared by consumers with business-

es. California law has not kept pace with these developments and the personal privacy implications surrounding the collection, use, and protection of personal information."

Among the personal data companies collect and profit from, it notes: where a consumer lives and how many children a consumer has, how fast a consumer drives, their personality, sleep habits, biometric and health information, financial information, and precise geolocation information.

To drive the need for legislative action home, the bill reminded legislators of March revelations that, through Facebook, tens of millions of people had their personal data misused by the data-mining firm Cambridge Analytica. The list of other data breaches keeps growing with high-profile data leaks at Uber, Yahoo, Equifax, and, most recently, Exactis, a Florida-based marketing and data-aggregation firm, that exposed information on individuals and businesses involving as many as 340 million records.

A covered "business" is defined in the law as any for-profit entity that either does $24 million in annual revenue; holds the personal data of 50,000 people, households, or devices; or does at least half of its revenue in the sale of personal data. Consumers, for purposes of the law, are defined as California residents, specifically "every individual who is in the state for other than a temporary or transitory purpose," and "every individual who is domiciled in the state who is outside the state for a temporary or transitory purpose."

The law would be enforced by the state attorney general and create a private right of action for unauthorized access to a consumer's personal information. Failure to address an alleged violation within 30 days could lead to a $7,500 fine per violation, which could be per record or customer file.

California's legislation will supersede a proposed ballot initiative, the California Consumer Privacy Act, financed by real estate mogul Alastair Mactaggart and a coalition he founded—Californians for Consumer Privacy. His efforts raised more than $3 million and collected more than 625,000 signatures to put their proposal up to a state-wide vote. The initiative was slated to appear on November ballots.

The proponents, however, agreed to withdraw their ballot initiative if state legislators met a June 28 deadline for passing their own bill. That date was also the state's deadline for removing items from the November ballot.

Against that backdrop, Assembly Bill 375 was pulled from the legislative backlog in response and resubmitted to both chambers of the state legislature by Democrats Sen. Bob Hertzberg and Assembly Member Ed Chau.

"[This] will be the best privacy law in the country," Hertzberg said. "It integrates many of the elements of the initiative and provides Californians with significantly more control over personal information alongside an explicit protection of those rights."

"At a time when federal regulators are rolling back protections, we're moving forward here in California," said California Senator Bill Dodd. "This bill will be the strongest of its kind in the nation and enact safeguards we need in the 21st Century. Big Data is Big Business. It's time we regulate it appropriately and hold bad actors accountable."

Throughout the legislative process, some of California's largest tech companies had lobbied, typically behind-the-scenes, to either kill or rewrite any legislative effort spawned by the ballot initiative.

According to records on file with California's Secretary of State, among the donors to a coalition, the Committee to Protect California Jobs, fighting the ballot initiative, prior to the new legislation were: Alliance of Automobile Manufacturers (donating $200,000 towards lobbying costs); AT&T ($200,000), Comcast (C$200,000), Facebook ($200,000) Google ($200,000), Verizon ($200,000), Amazon ($195,000), and Microsoft ($195,000). Facebook later announced in April, after a series of tense data privacy hearings before Congress, that it was dropping its opposition.

"Now that they have seen the error of their ways,

INSIDE THE REGULATION

Beginning Jan. 1, 2020, the legislation will:

- Grant a consumer the right to request deletion of personal information and require the business to delete that data upon receipt of a verified request;
- Grant a consumer a right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of third parties to which the information was sold or disclosed;
- Authorize a consumer to opt out of the sale of personal information by a business and prohibit a company from discriminating against consumers for exercising this right, including by charging a different price or providing the consumer a different quality of goods or services;
- Authorize businesses to offer financial incentives in exchange for the collection of personal information;
- Prohibit a business from selling the personal information of a consumer under 16 years of age, unless affirmatively authorized;
- Provide for its enforcement by the Attorney General and would provide a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's nonencrypted or nonredacted personal information;
- Create a Consumer Privacy Fund funded by fines and penalties; and
- Authorize a business, service provider, or third party to seek the AGI's opinion on how to comply with its provisions.

we hope they will work with us proactively to protect the personal information of all Californians, and support us publicly and financially," Mactaggart said at the time. "We call on the remaining corporations who have contributed to the Super PAC opposing this common-sense measure to drop their opposition. Google, AT&T, Verizon and Comcast: if you are not selling our personal information, why are you spending a million dollars to oppose us? Voters overwhelmingly support this measure, and protecting consumers is not only a good business decision, but the right thing to do."

The Internet Association, whose membership includes many of California's tech companies, would later announce that, despite lingering concerns, it would step away from any effort to derail a data privacy bill.

"Maintaining people's privacy and security has always been and remains a top priority of internet platforms," Vice President of State Government Affairs Robert Callahan said in a statement after the bill's passage and gubernatorial enactment. "Trust with IA member products and services is essential to a thriving internet, and the internet industry is committed to providing people with information and tools to make informed choices about how their personal information is used, seen, and shared online."

"Data regulation policy is complex and impacts every sector of the economy, including the internet industry," he added. "That makes the lack of public discussion and process surrounding this far-reaching bill even more concerning. The circumstances of this bill are specific to California. It is critical going forward that policymakers work to correct the inevitable, negative policy and compliance ramifications this last-minute deal will create for–– California's consumers and businesses alike."

Chau, for his part, conceded that the legislation he helped draft will likely need to be closely reviewed.

"The attorney general may have some issues that we need to fine tune," he said during a press conference on Thursday. "There also may need to be some immediate technical clean-up we must work on." ■

California data privacy law creates complications beyond GDPR compliance

To hear some analysts and compliance experts describe it, California's Consumer Privacy Act of 2018 is essentially a scaled-back version of Europe's GDPR. **Joe Mont** has more.

In many respects, the General Data Protection Regulation is, on the surface, a more complicated bit of legislation, and one with more moving parts to consider within its 99 Articles. By comparison, California's law does, indeed, seem far more streamlined.

Appearances, however, can be deceiving, warns John Tsopanis, privacy product manager for 1touch.io, a purveyor of network mapping and automated data discovery software solutions. "If we are talking from an American company's point of view, I honestly believe that California's new law is more stringent and forces more work to be done by those companies than European companies are required to do under GDPR," he says. "This is earth-shattering, groundbreaking legislation. The implications of it, and the work that needs to be done by almost all companies in America, is monumental."

In late June, California, home to many of the world's top tech companies, became the first state in the nation to enact a law that, in large part, attempts to mirror European data protection and privacy standards of the European Union's General Data Protection Regulation. It will take effect on Jan.1, 2020.

Similar to GDPR, California customers will have the right to demand that specific data be deleted from an online enterprise's databases. The legislation will:

» Grant consumers the right to request deletion of personal information and require the business to delete that data upon receipt of a verified request;
» Give consumers the right to request that a business that sells the consumer's personal information, or discloses it for a business purpose, disclose the categories of information it collects and the identity of third parties to whom it was sold or disclosed;
» Authorize consumers to opt out of the sale of personal information by a business and prohibit a company from discriminating against consumers for exercising their right to do so;
» Authorize businesses to offer financial incentives in exchange for the collection of personal information;
» Prohibit businesses from selling the personal information of a consumer under 16 years of age, unless affirmatively authorized;
» Allow for the law's enforcement by the California's Attorney General; and
» Provide a private right of action in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer's non-encrypted or non-redacted personal information.

A covered "business" is defined in the law as any for-profit entity that either does $24 million in annual revenue; holds the personal data of 50,000 people, households, or devices; or does at least half of its revenue in the sale of personal data. Consumers, for purposes of the law, are defined as California residents, specifically "every individual who is in the state for other than a temporary or transitory purpose."

Failure to address a violation of the law within 30

days could lead to a $7,500 fine per violation, which could be defined as for record or customer file.

As detailed as the law may seem, plenty of opportunities for it to be reshaped remain, with even tougher privacy protections or more business-friendly amendments, says Laura Jehl a partner with law firm BakerHostetler and co-chair of its GDPR practice. She addressed the California law during a more general discussion of GDPR during a webcast last week. "There is no guarantee the law will take effect in its current state," she said. "Almost immediately after the law took affect, the tech companies once again focused their money and energy on attacking it. Amendments have already been proposed, and there are more likely to be proposed by other groups."

"This thing is not done yet. Before you waste too much time learning every provision and figuring how to comply with it—and whether it requires different steps than GDPR compliance, how much more budget you need to request in the next budget cycle, and whether or not your company will revolt and refuse to give you any more money because you just had GDPR—all remains to be determined. Hold your fire but do keep your eye on California."

That there may be amendments to the law is, itself, a concession to California's powerful and profitable tech sector. "One of the concerns about the ballot initiative is that it had a crazy supermajority, a 70 percent vote to change or amend the law," Jehl said. "The tech companies were really unhappy with that, so both sides came together and agreed they would draft a less onerous bill. A supermajority is no longer needed for amendments."

Although the legislation is often thought of as "California's GDPR," and there is indeed "a high degree of overlap between the two" the data privacy regimes are far from identical," Jehl explained. She described it as a broader, consumer-focused piece of legislation than the personal data scope of GDPR.

Both similarities and differences can be found in even how the two regimes approach personal data.

In the California law, Jehl said, "personal information is broadly defined to include identification of or association with a consumer or household, including demographics, usage, transactions and inquiries, preferences, biometrics, employment information, predictions, inferences drawn to create a profile about a consumer, and education information. This excludes publicly available information from public government records." It remains unclear whether de-identified data and aggregate consumer information is included.

Under GDPR, personal data is broadly defined as any data that permits identification of a data subject, directly or indirectly. Examples include names, ID numbers, location data, online identifier such as IP addresses, or reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject.

The California law comes at a precarious time for U.S. companies struggling since GDPR's May 25 deadline to "grapple with the practical realities of implementing their compliance programs, a BakerHostetler client alert states. "In almost all cases, many loose ends remain. As EU regulators issue new guidance and contemplate enforcement, businesses must be prepared to adapt their strategies to respond to new interpretations and changing circumstances," it added.

While GDPR covers cross-border transfers, the Consumer Privacy Act applies to inter-state and international consumers served by a California business.

Tsopanis, the privacy product manager for 1touch.io, warns against taking a wait-and-see attitude regarding California's law. "Although they may not realize it yet, every technology and Fortune 500 company in America is going to be affected," he says. "It doesn't matter what state a business is based in; if it collects data on California citizens or works with a third-party supplier based in California—and what large business doesn't work with a California tech company?—it will be required to maintain compliance with the new law."

California's AB 375 goes into effect in 18 months, he says, adding, " Ask any European company now grappling with GDPR: 18 months is no time at all. If

U.S. companies are not preparing now, their risk exposure is poised to go through the roof in January 2020."

In action, Tsopanis says, the law will hone the focus on subject access requests. "It essentially allows upwards of 40 million Californians to easily access, on a company's webpage, a link that says, 'Do not sell my personal data,' and they can request, from that company, a report on what personal information it has on them, who they have sold it to and why they are processing it. The citizen does not have to be a customer or have an account with that company to make that request." That, he says, "is a huge obligation and a huge burden on all American companies."

To provide that report within 45 days, firms may need to scour their entire company to find out if they have any personal information on that one California citizen, then provide them with a full report on what that information is, who the sold it to, and the contact name and addresses of the people that they sold it to.

"The definition of personal information in this California Privacy Act is much broader than in the GDPR," Tsopanis adds. "It includes unique identifiers— which are things like cookies IP addresses, and device numbers. What that means is if, in the course of the 12 months, 50,000 California residents visit your web-based storefront in Maine, based on your cookie settings you are liable under this legislation... It is almost impossible, if you are a business in a state outside of California—the fifth largest economy in the world—to not process the data of California residents.

Nearly every firm, within their privacy notices, will need to have a second section for California residents, Tsopanis says. "It needs to tell them that you are not allowed to sell their personal data. The link needs to be clear, conspicuous and on every business home page."

Tsopanis warns that what makes the California law potentially more serious than GDPR is that in the response to requests, a company will need to detail all of the entities it has sold data to. "This is not a requirement in the EU GDPR, which captures consent for third-party processing of data in the privacy notice before information is collected."

"The amount of buying and selling of data is absolutely off the hook," he adds. "Each company is going to need to disclose, for the previous 12 months, what their buying and selling of data practices were and what happens when that data is in the hands of citizens who game that information. This is going to blow open an entire system that U.S. consumers never knew existed."

A nuanced review of the rule reveals additional challenges for companies, Tsopanis says. "It essentially says that when you get an access request you need to disclose which companies you sold that data to in the past year, and why you sold it," he explains. "To legally sell data to a third party, the law says that there has to be a contract in place that prohibits the third arty from then reselling personal information or processing it for a reason that wasn't explicitly named in the contract. This is going to be a major problem for the entire network of data sellers and buyers, because clearly there us a obliteration of selling data after the initial access to everyone." Also, if that third party is breached while using your data in a way that wasn't specifically outlined in the contract, the initial company is also liable for that breach.

Monitoring these third parties is one of the major challenges imposed by the new law. "You've got to do really good and fast third party risk management and due diligence on your major suppliers and digital marketing agencies," Tsopanis says. "You need assurances from the companies you sell data to that they are not being cowboys with it.

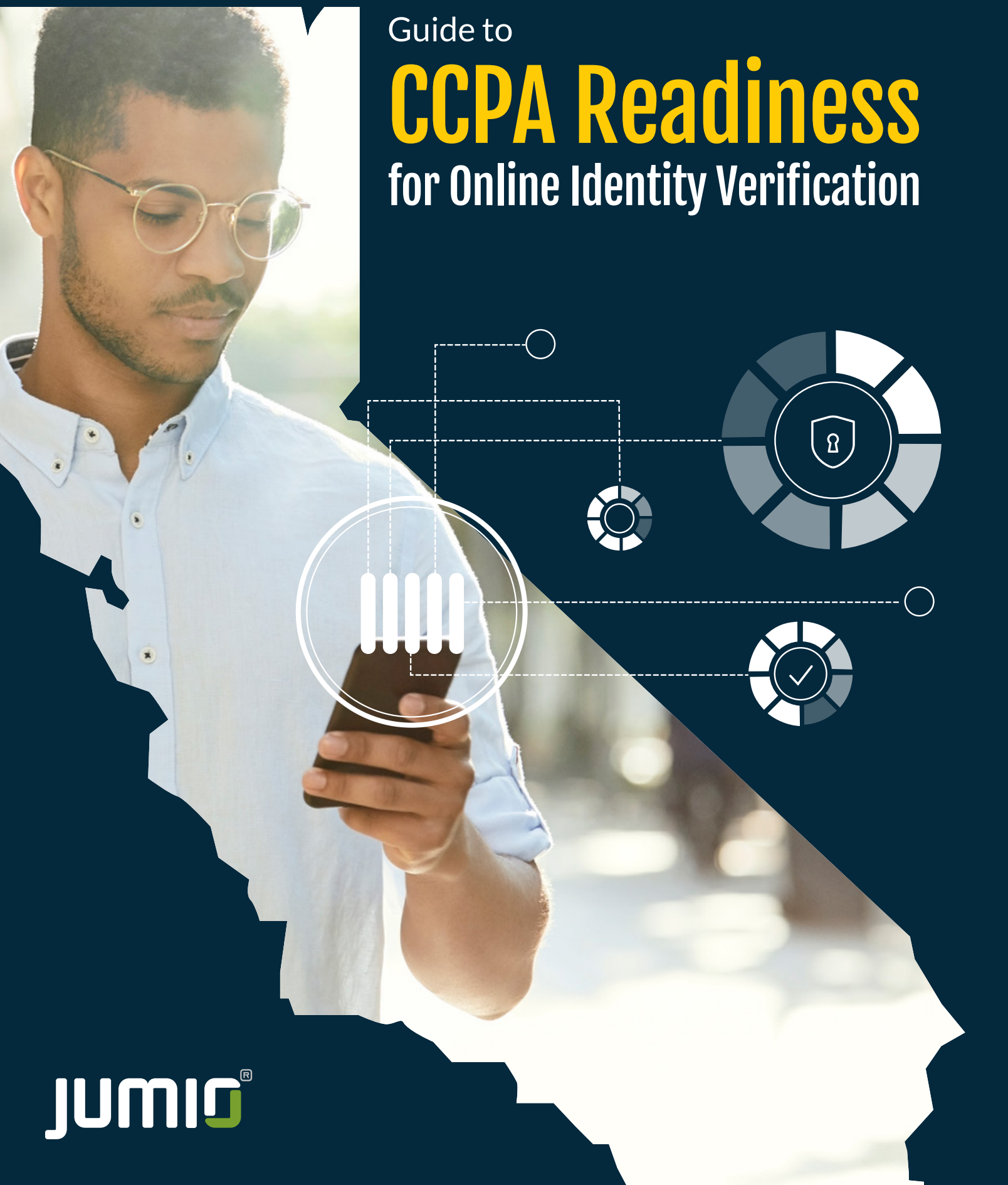
A similar lesson was learned post-GDPR. Firms are demanding third-party ISO 2701 updates and GDPR audits done by the Big Four. "We are seeing a lot of professional services auditing and checking to provide assurances between third parties," he says. "That's already an established market here in Europe."

The advice for company's facing either a data privacy regime is to focus on the basics. "Companies need to answer basic questions: what data do I have, where is it, who am I sharing it with and what rules do I have," Tsopanis says. "Keep it simple. Find your information, categorize it, and have some rules around it." ■

Guide to

CCPA Readiness

for Online Identity Verification



jumio®

Welcome to consumer protection in the digital age.

The lines between the digital and physical worlds are officially blurry. According to a 2018 Pew Research study, one in four Americans say they are online almost constantly and three quarters of Americans go online at least daily. Consumers are doing everything from catching a ride, sending money to a friend, opening a bank account, renting a vacation home and so much more, all with a few clicks and swipes. Along the way, consumers are leaving a digital trail of information that can and will be used against them if in the wrong hands.

The California Consumer Privacy Act (A.B. 375) is an unprecedented privacy law that grants California residents sweeping rights concerning the collection and use of their information. Once the law becomes effective on January 1, 2020, covered businesses can expect to weather a flurry of consumer requests, which can encompass information collected from January 1, 2019 forward.

A recent TrustArc study found the vast majority of companies have a very long way to go to become compliant with the CCPA. An alarming 86 percent of the study's respondents say they have not completed preparations to become compliant.

The CCPA defines both consumers and covered businesses broadly, grants far-reaching rights to consumers, and imposes extensive obligations on covered businesses. Compliance with other progressive privacy regulations such as the European Union's General Data Protection Regulation (GDPR) does not ensure compliance with the CCPA. California's ground-breaking legislation may encourage other states to follow suit, with some already considering similar legislation.

1 in 4 Americans say they are online almost constantly

What is the CCPA?

The CCPA affords California residents an array of new rights, starting with the right to be informed about what kinds of personal data companies have collected and why it was collected. Among other novel protections, the law stipulates that consumers have the right to request the deletion of personal information, opt out of the sale of personal information, and access the personal information in a "readily useable format" that enables its transfer to third parties without hindrance.

The CCPA will accomplish three major objectives for California residents, giving them the right to:

1

Know what information businesses are collecting about them

2

Tell a business not to share or sell their personal information

3

Protections against businesses that do not uphold the value of their privacy

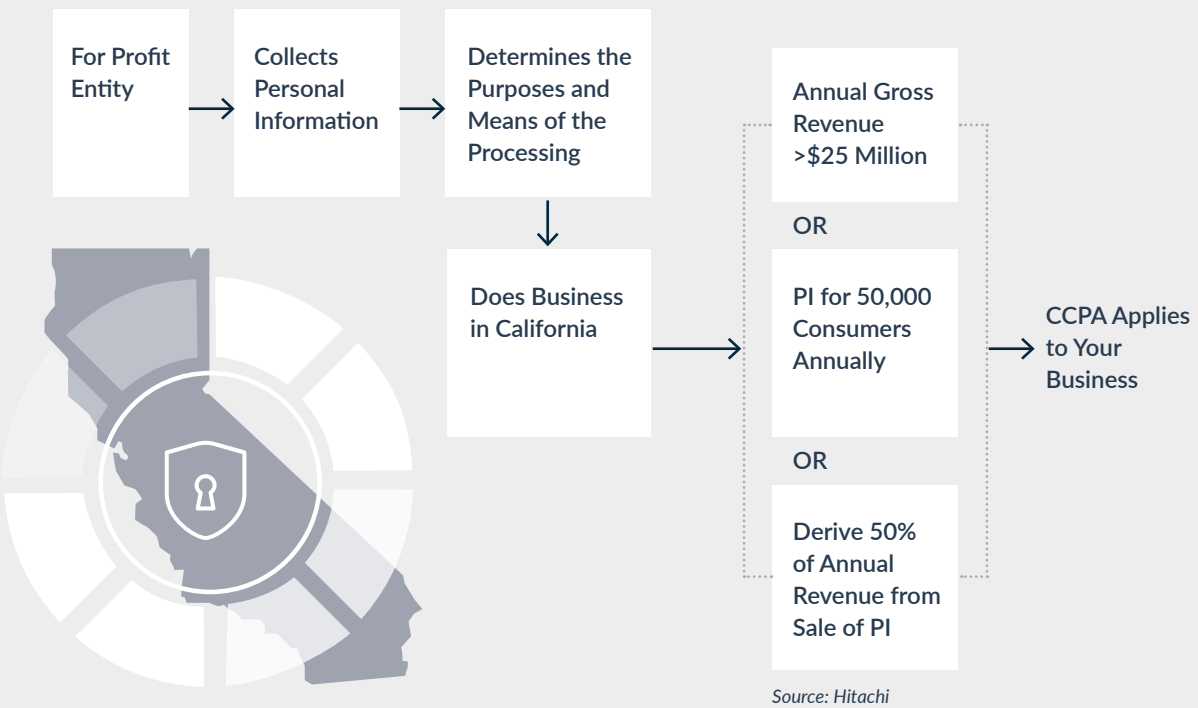
While the law, which goes into effect January 1, 2020, technically applies only to California residents, it will most likely have much broader implications. In fact, it will likely be the strictest data privacy law in the United States, and will require data privacy protections and requirements similar to or broader than those imposed by GDPR, which became effective on May 25, 2018. Consider that most major companies that deal in consumer data, from retailers to cellular network providers to internet companies, have some Californian customers.

Does the CCPA apply to your organization?

Affected businesses are for-profit entities doing business in California that meet certain revenue or data collection volume requirements. Principally, all California residents are protected under the CCPA with respect to any information that relates to them. This means that companies around the world have to comply with the CCPA if they receive personal data from California residents and if they — or their parent company or a subsidiary — exceed one of three annual thresholds:

- ✓ The company has gross revenues of **$25 million** or more
- ✓ The company receives, sells or shares information of **50,000** or more California residents or devices
- ✓ The company derives **50 percent** or more of its revenue from selling consumers' personal information

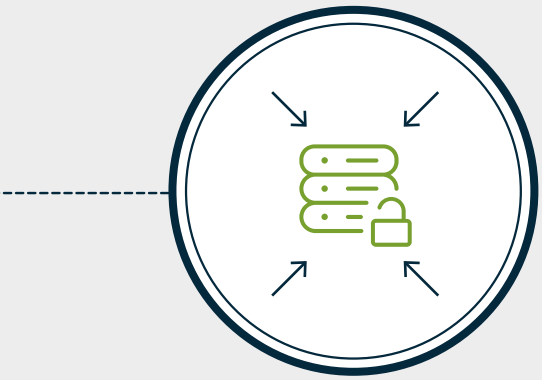
CCPA Decision Matrix



Source: Hitachi

The Nitty Gritty

The CCPA requires organizations to implement procedures such as the right to access, the right to delete, the right to opt out of the sale of personal information, the right to opt in for children, non-discrimination and changes to privacy notifications.



Right to Access

Organizations subject to the CCPA must honor consumers' requests regarding the right to access their personal information. The disclosure process of the information requested must be free of charge for a consumer and sent by physical mail or electronically. The CCPA limits the right to access to two times a year. In other words, organizations can't be required to honor more than two requests, by one consumer, within a period of 12 months. Organizations do not need to retain personal information in order to comply with the law.

Right to Delete

Organizations subject to the CCPA have an obligation to honor consumers' requests regarding the right to delete their personal information. There are a few exceptions regarding the consumer's right to delete, which grants the company the right to deny such a request (1798.105).

Right to Opt Out

Organizations subject to the CCPA need to provide a clear and conspicuous link entitled “Do Not Sell My Personal Information” on their website and in their privacy policy by January 1, 2020. The link must provide the consumer the option to opt out of the sale of their personal information (1798.135 (a)(1)).

Furthermore, organizations are not allowed to force a consumer to create an account in order to be able to opt out. Also, businesses are not allowed to use any information gathered on the consumer during the opt-out process.

Lastly, organizations must wait a minimum of 12 months after completion of the opt-out process before inviting the consumer to opt-in back to the sale of their personal information.

Note: California provides consumers the right to opt out of the sale of personal information. For a sale to occur, there is no obligation to have an exchange of money. Disclosures by any means (orally, written or electronically) can be considered as a sale.

Children’s Information

Contrary to the regular opt-out process requiring a consumer to demand the right to opt out, businesses must expressly collect the consent of children under 16 (consent of the parent for those under 13) to sell their personal information.

In other words, children under 16 do not have to opt out in order to protect the sale of their personal information. It is not sellable unless expressly authorized otherwise (1798.120 (d)).

An organization subject to the CCPA can’t willingly disregard the consumer’s age in order to proclaim that they did not have the knowledge of dealing with a child’s information. As a result, they will most likely have to ask consumers about their age in order to comply with the restrictions.

Privacy Policies

Section 1798.100 requires organizations to disclose (at or before the collection) the categories of personal information collected and the purpose regarding their collection and later usage.

Section 1798.120 (b) requires organizations that sell consumers' personal information to notify such consumers about the probability of their information being sold and their right to opt out. In accordance with the CCPA, organizations have a delay of 18 months to comply.

Two different lists are required in the organization's privacy policy:

- a list of the categories of personal information sold in the last 12 months, and
- a list of the categories of personal information disclosed about consumers for a business purpose in the last 12 months.

If the company has not sold or disclosed personal information, it still must publish a statement informing consumers to that effect.

The notices and information provided by an organization must be easily understandable and accessible to the average consumer or consumer with disabilities. These notices must be in the language commonly used to communicate with consumers.

Lastly, it will be mandatory for organizations to update their privacy policy notifications at least every 12 months in order to keep up to date the categories of personal information collected and sold.

Limitations of the CCPA

CCPA only protects California residents. Therefore, it only applies to people, companies or organization doing businesses within the state of California. The act doesn't apply if the collection or sale of personal information took place outside of California. If this information was collected and then sold while the California resident was outside of the state, there would be no violation of the resident's rights.

Disclosure to service providers is not prohibited when a consumer exercises the right to opt out. Businesses may not discriminate against people who exercise their rights unless it meets the Financial Incentives Exception. This exception grants businesses the right to entice consumers to consent to the collection, sale or deletion of personal information in exchange for financial incentives (1798.125 (b)).

As opposed to the GDPR, the CCPA does not include areas such as privacy by design and privacy by default, foreign company registration requirement, data protection impact assessments, 72-hour breach notification, data protection officer requirement and restrictions on cross-border data transfers.

Consequences of Non-Compliance

A CCPA violation for the purposes of a lawsuit by the California Attorney General occurs if the business receives notification of the alleged noncompliance and fails to resolve the alleged violation within 30 days (1798.155 (a)). Intentional violations of the CCPA can bring civil penalties of up to $7,500 for each violation in a lawsuit brought by the California Attorney General (1798.155 (b)).

Consumer lawsuits provide for statutory damages of between $100 and $750 per consumer per incident or actual damages, whichever is greater. The lawsuits only apply to certain disclosures of personal information where a business failed to implement or maintain reasonable security procedures and practices.

Damages from class action lawsuits can start at **$5M** (based on 50,000 records) and go up from there.

What's the Difference Between the CCPA and GDPR?

The EU's General Data Protection Regulation (GDPR), which went into effect in May 2018, is similar to the CCPA in that its aim is to give consumers greater control over their data. Companies who have gone through GDPR compliance will have a leg up on CCPA preparations, but the two are not identical. Two differences will most impact marketers:

GDPR

GDPR is considerably stricter about what data processing is legally permissible. It requires affirmative consent for any data processing — not just reselling data but collecting it in the first place. In comparison, the CCPA assumes permission (except for children under the age of 16) and only requires that consumers be able to revoke that permission by opting out.

CCPA

The CCPA's disclosure requirements differ from GDPR's, including notifying consumers of their rights under the CCPA and what categories of information have been shared with or sold to third parties within the last year.

PwC provides a more detailed comparison of the two laws' requirements.

NOTE: Legal experts speculate that, although GDPR is the more comprehensive law, the CCPA will be more strictly enforced, because the U.S. generally has more rigorous regulatory oversight than the EU.

The Role of CCPA in Online Identity Verification

Enter online identity verification. Online customer identity verification providers have come on the scene with increasing urgency to help ensure trust and safety among customers and users of online services across a spectrum of industries. The role of online identity verification is to tie your customers' digital identities (who they claim to be) to their real world identities (who they are in real life). This "match" is key to building a strong online brand, preventing fraud and converting good customers.

Companies have utilized a range of approaches to achieve a desired level of confidence in the identities of their customers. For some, confirming a valid government-issued ID (passport, driver's license) is enough and can be accomplished using the camera on a smartphone or computer. Other companies are comfortable with two-factor authentication or knowledge based authentication (KBA). Still others demand a more thorough identity verification (including ID checks, supporting documentation and biometric verification).

On one hand, each layer of trust and safety brings a layer of confidence, fraud prevention and risk reduction. On the other hand, each layer requires online users to divulge more information that, if not handled appropriately, could later be used by scammers to assume their identities.

How is your online identity verification program impacted by the CCPA?

Because many forms of identity verification collect personal information including information on government-issued IDs, biometric information and/or pictures of consumers, these solutions are bound to comply with the CCPA. The CCPA broadly defines personal information to cover types of information not traditionally considered personal information in the United States, including:

NOTE: The CCPA provides an exception for publicly available information. Publicly available information refers to any information that is lawfully made available from either the federal, state or local government. It is not considered publicly available information if the information is used in a way that does not match with the purpose for what it has been maintained.

What should you look for in a compliant identity verification solution?

CCPA-compliant solutions should be transparent about the types of personal data collected as part of the identity verification process. Your chosen identity verification solution must be able to equip your customers with a complete list of the personal data collected and it must be able to manage consumer requests for deletion of personal data after the identity verification has been performed. And clearly, your chosen solution should not be reselling consumer data without prior acknowledgment and businesses should seek written confirmation that consumer data is kept strictly confidential.

Like GDPR, CCPA-compliant solutions should store PII data securely and have predetermined data retention policies in place to assure the timely deletion of that data. Compliant solutions should have the ability to manually override retention policies and have consumer data deleted upon written request. Identity verification solutions that are already PCI-DSS compliant have a significant head start because of the security and data protection mandates they must meet and vet with independent auditors. Likewise, any solution that is already GDPR compliant should be able to tick most, if not all, of the compliance mandates of the CCPA.

Verifying Consumers
Requesting CCPA Information

The CCPA offers sweeping new rights to Californians including the right to know what information businesses are collecting about them and the right to tell a business not to share or sell their personal information. But, how does a business know that the consumer who is exercising these rights is the actual account owner?

Account takeover is an emerging form of online fraud which involves a criminal gaining unauthorized access to a user's account and using it for some type of personal gain. Large-scale data breaches, phishing and social engineering attacks have made it easier for fraudsters to assume the online identities of legitimate account owners. This means when a request is made by a consumer to know what information has been collected about them, the business must ensure that they do not inadvertently divulge personal information to a would-be fraudster.

The most reliable way to ensure that data is securely shared with the actual account is via biometric authentication.

Face-based biometrics are not only far more convenient for consumers than traditional methods of online verification, but they are much more secure. They cannot be hacked or duplicated. The data can be kept on the device, rather than on a server or in the cloud, and can remain secure even if the device is stolen. Just as important, face-based biometrics offers a simple one-step solution to the problem of remembering a vast array of PIN codes and passwords.

How does face-based authentication work?

At Jumio, this new biometrics-based approach starts with account set-up. New users are asked to use their smartphone or webcam to capture a picture of their government-issued ID and a selfie, which are then compared to each other to deliver a definitive match/no match decision. As part of the identity proofing process, Jumio creates a 3D face map of the user, which is then stored and bound to the new customer during the initial enrollment process.

3D face-mapping contains 100 times more data points than a 2D photo, and is required to accurately recognize the correct user's face while concurrently verifying their human liveness.

Spoofing attacks by fraudsters are on the rise to fool the selfie requirement. Spoofing attempts generally use a photo, video or a different substitute for an authorized person's face in order to acquire someone else's privileges or access rights. To foil these attempts, modern identity verification companies leverage certified liveness detection that captures biometric data through a smartphone's front-facing selfie camera or a desktop computer's webcam.

Now, let's assume that a California-based consumer makes a CCPA request to know what data has been captured by the organization. Companies want to ensure that the CCPA requestor is the legitimate account owner. Instead of relying on a username and password, the user only needs to capture a new selfie. Because a complete face map was captured when the account was created, the user just needs to take a fresh selfie (one close up and one a little further away). A new face map is then compared to the original 3D face map captured during enrollment and a match/no match decision is made. This authentication process takes just seconds to complete.

This type of authentication enables online companies to reliably authenticate CCPA requests and ensure that information is only shared with legitimate customers, not bad actors posing as customers to secure personal information. It also nullifies the risk of account takeover since it does not rely on a username and password which could have easily been stolen from the dark web, phishing or social engineering.

How Jumio Can Help

Jumio enables any business that captures data from California residents with the requisite data security, transparency and retention policies to comply with the CCPA. Jumio will never sell consumer data to third parties. Just as importantly, Jumio stores and protects consumer data, captured during the identity verification process, under strict PCI-DSS data security requirements.

Jumio has the ability to delete any data captured during the online identity verification process, including information captured from government-issued IDs, biometric information and selfie images. Business customers can enforce strict data retention periods or have the identity information deleted automatically after a verification decision has been rendered.

Across industries, companies are finding that establishing trust and safety goes hand in hand with having a strong customer identity verification process. The processes you enable to verify the identities of your users and customers must be secure, accurate and compliant while also contributing to a smooth and seamless onboarding experience. While it may feel impossible to achieve all of these goals, the fact is, customers expect it. Your customers want to engage with companies that have strong measures in place to deter fraud and protect personal privacy, but not at the expense of a fast and easy customer experience.

How to Get Ready for 2020

To prepare for the CCPA coming into effect on January 1, 2020, we have gathered a few best practices for organizations subject to CCPA:

Risk Management

Organizations should start identifying risks in their data procedures and create new risk management policies accordingly.

Privacy Policy and Data Collection

Organizations should rethink their communication methods and privacy policy. They must ensure that every consumer is aware of their data collection policy and that consent has been given in order to rightfully delete the personal information collected.

Necessary Data

In order to minimize their risks, organizations should only keep data that is necessary to the direct service of the business.

Data Tracking System

As consumers will have the right to request data collected within the past 12 months starting on January 1, 2020, organizations should have a data tracking system in place as soon as possible in order to be compliant with the period of the past 12 months.

Process for Consumer Authentication

While data privacy is at the heart of CCPA, companies need to ensure that they're only releasing data to the actual account owner, and not a fraudster posing as the legitimate user.

In Closing

If your business is doing business in the state of California and both collecting and processing the personal information of California residents, you may be subject to the California Consumer Privacy Act.

If you are indeed subject to the CCPA, you will have to start thinking about how your business collects the personal information of Californian citizens and residents, and what you will need to do to be ready for the January 1, 2020 deadline. You will need to define a clear path towards CCPA compliance to avoid any financial, legal or reputational damage that may result from non-compliance.

Lastly, data privacy experts speculate that businesses may tend to choose to apply this new law to all of their consumers rather than limit it to California residents only. If so, the California Consumer Privacy Act may become the de facto standard in the U.S.

jumio®

jumio.com

Tech companies haggle over data privacy law

Well past the point of omens, it seems that a federal consumer privacy law is imminent. But what should that law be? And, asks **Joe Mont**, how should it mimic GDPR & California rules?

"A decade from now, we may look back and view this past year as a watershed with respect to the issue of consumer data privacy," said Sen. John Thune (R-S.D.), chairman of the Senate Commerce Committee, while surveying a row of executives from some of the largest tech companies—AT&T, Amazon, Google, Twitter, Apple, and Charter Communications.

"The question is no longer whether we need a federal law to protect consumers' privacy. The question is what shape that law should take."

The Senator's comments were made at a Wednesday hearing, "Examining Safeguards for Consumer Data Privacy," which explored the privacy policies of top technology and communications firms, reviewed the current state of consumer data privacy,

and explored possible approaches to more effectively safeguarding privacy.

Thune laid out some recent events to make his case for the sea change in how data privacy is perceived: the massive 2017 Equifax data breach; the Congressional hearing with Facebook CEO Mark Zuckerberg convened after revelations that political intelligence firm Cambridge Analytica had acquired access to the personal data of millions of unwitting Facebook users; the European Union's General Data Protection Regulation (GDPR), which took effect in May and came with many privacy-related mandates and severe penalties for violators; and the June 28 signing of the California Consumer Privacy Act (CCPA) into law.

"These developments have all combined to put the issue of consumer data privacy squarely on Congress's doorstep. What can Congress do to promote clear privacy expectations without hurting innovation?" Thune asked.

Tech companies support privacy legislation

Another advocate of federal legislation was Bud Tribble, vice president of software technology at Apple, who stressed the company's strong support of "federal privacy legislation that reflects Apple's long-held view that privacy is a fundamental human right."

Tribble described data privacy as central to how Apple designs products. "Some would call this 'privacy by design,' " he added. "It means that we challenge ourselves to minimize the amount of personal information we collect. Can the information we do collect be less identifiable? Can we process information on the device instead of sending it to servers? We want your device to know everything about you; we don't feel that we should."

Amazon associate general counsel Andrew DeVore discussed the business benefits of establishing consumer trust at the online retailer. "We have known from our very beginnings as an online bookstore that maintaining customer trust is essential to our success," he said. "Our customers trust us to handle their data carefully and sensibly in a secure and appropriate manner in line with their expectations. Any privacy mistake risks the loss of that trust and serious reputational damage even if there is no violation of privacy laws."

Beyond internal efforts, however, there are current and future legislative demands to meet, DeVore said.

"While our longstanding commitment to privacy aligned us well with the GDPR principles, meeting its specific requirements for the handling, retention, and deletion of personal data required us to divert significant resources to administrative and recordkeeping tasks and away from inventing new features for customers and our core mission of providing better service, more selection, and lower prices," he said. "We encourage Congress to ensure that additional overhead and administrative demands any legislation might require actually produce commensurate consumer privacy benefits."

Another supporter of a uniform national framework, Rachel Welch, SVP for policy and external affairs at Charter Communications, said such a framework "should start with the consumer and be grounded in the concept of empowering and informing consumers to control the personal information that is collected about them online."

It should, Welch said, focus on a series of core principles, such as:

- The best way to ensure consumers have control over their data is through opt-in consent, with no more pre-ticked "boxes," take-it-or-leave-it offers, or other default consents;
- The use of personal data should be reasonably limited to what the consumer understood at the time consent was provided;
- Companies should ensure that consent is renewed with reasonable frequency;
- Explanations about how companies collect, use, and maintain consumers' data should be easy to understand and readily available;
- Privacy policies should be separate from other

terms and conditions of service;
» Consumers should know that their personal information is being treated with the same level of protections wherever they go on the internet; and
» There should be a single national standard that protects consumers' online privacy regardless of where they live, work, or travel.

"Whether a consumer's information is adequately protected should not differ based on which state he or she is logging in from," Welch said. "A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation on the internet—which is a borderless technology." She, like several of her colleagues, agreed that the Federal Trade Commission (FTC) "is the appropriate agency to oversee and enforce online privacy and data security."

One of those colleagues, Leonard Cali, SVP of global public policy for AT&T, spoke strongly of the need for a uniform law with the FTC as overseer, while warning against the risk of multiple, conflicting laws.

"Perhaps for the first time, there is widespread agreement among industry, policy makers, and many consumer groups of the need for a new and comprehensive federal privacy law," testified Leonard Cali, senior vice president of global public policy for AT&T. "Consumers rightly expect that consistent privacy protections will apply regardless of which app, device, service, or company is collecting and using their personal information."

He warned, however, of an increasing risk that "we will end up with a patchwork quilt of inconsistent privacy regulations at the federal and state level, which will only serve to confuse consumers and stifle innovation."

The emergence of GDPR, and California's variation, serve to further call out the need for a federally based legislative approach, Cali said. "Like GDPR, many of the California requirements are highly prescriptive, and ambiguities and errors in its language leave open serious questions about how it will be enforced and interpreted," he testified. "For both, there also remain serious questions about their ultimate impact on consumers, desirable new technologies like AI, and the marketplace."

"I am not here to provide Congress a laundry list of the possible negative implications of the California law," Cali added. "The more important point for Congress to understand is that the passage of the law and interest of other states in legislation raise the imminent risk that companies and consumers will soon face a patchwork of inconsistent state privacy laws. Indeed, 26 state privacy bills were introduced this year alone."

"While each state may adopt its own set of privacy permissions and restrictions, providers struggling with compliance may have no choice but to adopt the most restrictive elements of each state's law, given the impracticability of complying with multiple state rules when offering mobile and internet services that, by their nature, have no state boundaries," he added. "The result may be a more restrictive privacy framework than any state intended with less innovation, investment and consumer welfare than any state anticipated."

Cali added that a "national privacy framework" could be overseen by the FTC and should define sensitive and non-sensitive data and its appropriate treatment. Likewise, data security and breach-notification legislation "should establish a reasonable, flexible, and consistent national framework," he said.

Primarily, the FTC, which has brought more than 500 enforcement actions for privacy and data security violations, including cases involving major internet and telecommunications companies, seeks enforcement actions for "unfair or deceptive acts or practices in or affecting commerce," under Section 5 of the Federal Trade Commission Act—this includes false promises of how consumer data is used and secured. As states adopt privacy laws that clash with the FTC's longstanding framework, the agency's position as the nation's leading privacy regulator will inevitably be eroded.

In short, according to Cali, federal legislation is necessary to codify a privacy law that builds on and

strengthens the FTC's role as the nation's preeminent privacy "cop on the beat."

Sen. Brian Schatz (D-Hawaii) questioned the consistent promotion by panelists of the FTC as the likely agency at the heart of any federal legislation, especially after suggestions to ramp up its resources and rulemaking authority were met with tepid reactions. "Some of these companies are saying, 'We want a new law, we want to preempt the states from acting, but we don't really want to give the FTC authority to make new rules in this space,' " he said.

"The problem right now is that if there is a violation, the FTC may or may not have a rule that is specifically being violated. So, the only thing you can do is go to the company and say, 'We are notifying you that you are violating Section 5, let's enter into a consent decree' and then, only if you violate that consent decree, is there the authority to fine," Schatz said. "Then it just becomes a cost of doing business to 'move fast and break things.'"

Learning from established laws

When talk turned to specifics of a new federal law, Sen. Thune asked the panel why it should turn to GDPR or California's privacy law provisions to either emulate or bypass. Cali responded that both laws apply to all organizations "uniformly," noting that as a positive element among some of the negatives.

"The challenge with GDPR is that it is overly prescriptive," he added. "It is still early, but you've already seen hundreds of Websites that have gone dark. Smaller companies and start-ups appear to be exiting Europe, and it actually looks like it is strengthening the large incumbent platforms. On top of that, it may, because of the limits on data retention, hurt innovation in things like blockchain and artificial intelligence."

As for California, Cali said, it was hastily drafted. It has, for example, a non-discrimination obligation that could pose a legal threat to something as simple as loyalty cards "where you get a benefit for sharing data with the grocery store."

His hope: "Congress looks at both these laws, learns from them, and does better than them."

Congress, Amazon's DeVore stressed, should also consider possible unintended consequences of the CCPA approach.

"Amazon supports [California's] goals of giving consumers visibility and control when businesses collect and sell their personal information," he said. "But because the CCPA was quickly enacted there was little opportunity for thoughtful review, resulting in some provisions that ultimately do not promote best practices in privacy."

For example, the CCPA's definition of "personal information" goes beyond information that actually identifies a person to include any information that "'could be linked with a person,' which arguably is all information," DeVore claimed. "The result is a law that is not only confusing and difficult to comply with, but that may actually undermine important privacy-protective practices like encouraging companies to handle data in a way that is not directly linked to a consumer's identity."

Keith Enright, Google chief privacy officer, said obligations under GDPR have been "a tremendous challenge," and manpower calculations reach into hundreds of years of full-time equivalencies. Nevertheless, "companies like Google are certainly better able to absorb the compliance costs and a rigorous regulatory regime like that than the burden created for small- and medium-sized businesses," Enright said.

Tribble agreed, citing the 6 million (and growing) developers who call Apple's app store home. "It is very important, when crafting legislation, to look at those businesses and what the burden will be on them in terms of recordkeeping and so forth," he said. "It would be very important to make sure it is not over-burdensome for that class of companies."

A second hearing, planned for early next month, will include privacy advocates as well as other key stakeholders. Alastair MacTaggert, a California privacy activist who spearheaded that state's recent law, and Andrea Jelenik, the head of GDPR enforcement for the European Union, have already agreed to testify. ■

Elizabeth Warren pitches Big Tech breakups

Sen. Elizabeth Warren (D-Mass.), among the ever-growing field of Democrats running for President, might not see much support from Silicon Valley. She is proposing a breakup of Big Tech firms she feels are stifling competition. **Joe Mont** reports.

In her campaign's official blog post on the Website Medium, Elizabeth Warren, on March 8, laid out a plan to break up world-leading technology companies like Facebook, Amazon, and Google.

"Twenty-five years ago, Facebook, Google, and Amazon didn't exist. Now they are among the most valuable and well-known companies in the world. It's a great story—but also one that highlights why the government must break up monopolies and promote competitive markets," Warren wrote.

Today's Big Tech companies have too much power over "our economy, our society, and our democracy," she argued. "They've bulldozed competition, used our private information for profit, and tilted the playing field against everyone else. And in the process, they have hurt small businesses and stifled innovation.

"I want a government that makes sure everybody—even the biggest and most powerful companies in America—plays by the rules. I want to make sure that the next generation of great American tech companies can flourish. To do that, we need to stop this generation of Big Tech companies from throwing around their political power to shape the rules in their favor and throwing around their economic power to snuff out or buy up every potential competitor."

Warren made her case of how a handful of com-

panies gained global dominance: Nearly half of all e-commerce goes through Amazon; and more than 70 percent of all Internet traffic goes through sites owned or operated by Google or Facebook. These companies, she alleged, have used mergers to limit competition. Facebook purchased competitors Instagram and WhatsApp. Amazon used its market power to force smaller competitors like Diapers.com to sell at a discounted rate. Google purchased rival mapping company Waze and rival ad company DoubleClick.

Amazon, she added, "crushes small companies by copying the goods they sell on the Amazon Marketplace and then selling its own branded version" and Google allegedly "snuffed out a competing small search engine by demoting its content on its search algorithm, and it has favored its own restaurant ratings over those of Yelp."

The problem, and attempted resolutions, date back to antitrust concerns with Microsoft in the 1990s. The federal government sued Microsoft for violating anti-monopoly laws by bundling its Internet Explorer with its Windows operating system. "The government's antitrust case against Microsoft helped clear a path for Internet companies like Google and Facebook to emerge," Warren claimed.

"The story demonstrates why promoting competition is so important: It allows new, groundbreaking companies to grow and thrive—which pushes everyone in the marketplace to offer better products and services," she said. "Aren't we all glad that now we have the option of using Google instead of being stuck with Bing?"

Even further back in history, a century ago in the so-called Gilded Age, "waves of mergers led to the creation of some of the biggest companies in American history—from Standard Oil and JPMorgan to the railroads and AT&T," Warren explains. "In response to the rise of these 'trusts,' Republican and Democratic reformers pushed for antitrust laws to break up these conglomerations of power to ensure competition."

In Warren's analysis, weak antitrust enforcement has led to a dramatic reduction in competition and innovation in the tech sector. "Venture capitalists are now hesitant to fund new startups to compete with these Big Tech companies, because it's so easy for the big companies to either snap up growing competitors or drive them out of business," she said, adding first financing rounds for tech startups have declined 22 percent since 2012.

"America has a long tradition of breaking up companies when they have become too big and dominant—even if they are generally providing good service at a reasonable price," Warren argued. "But where the value of the company came from its network, reformers recognized that ownership of a network and participating on the network caused a conflict of interest. Instead of nationalizing these industries—as other countries did—Americans in the Progressive Era decided to ensure that these networks would not abuse their power by charging higher prices, offering worse quality, reducing innovation, and favoring some over others. We required a structural separation between the network and other businesses and also demanded that the network offer fair and non-discriminatory service."

If elected, Warren's administration would restore competition to the tech sector by taking two major initiatives:

Platform utilities

Legislation would require that large tech platforms be designated as "Platform Utilities" and broken apart.

Companies with an annual global revenue of $25 billion or more and that offer to the public an online marketplace, an exchange, or a platform for connecting third parties would be designated as "platform utilities," Warren explains.

These companies would be prohibited from owning both the platform utility and any participants on that platform, her blog details. Platform utilities would be required to meet a standard of fair, reasonable, and non-discriminatory dealing with users. Platform utilities would not be allowed to transfer or share data with third parties.

For those with annual global revenue of between $90 million and $25 billion, their platform utilities

would be required to meet the "same standard of fair, reasonable, and non-discriminatory dealing with users, but would not be required to structurally separate from any participant on the platform."

The blog continues: "To enforce these new requirements, federal regulators, state attorneys general, or injured private parties would have the right to sue a platform utility to enjoin any conduct that violates these requirements, to disgorge any ill-gotten gains, and to be paid for losses and damages. A company found to violate these requirements would also have to pay a fine of 5 percent of annual revenue."

"Amazon Marketplace, Google's ad exchange, and Google Search would be platform utilities under this law," Warren explained. "Therefore, Amazon Marketplace and Basics, and Google's ad exchange and businesses on the exchange would be split apart. Google Search would have to be spun off as well."

Designating anti-competitive mergers

Warren would also appoint regulators committed to reversing illegal and anti-competitive tech mergers.

Examples, she said, are Amazon (Whole Foods, Zappos); Facebook (WhatsApp, Instagram); and Google (Waze, Nest, DoubleClick). Apple was not on the original list, but Warren later confirmed it also was a concern. What would the Internet look like after all these reforms?

"Here's what won't change," she said. "You'll still be able to go on Google and search like you do today. You'll still be able to go on Amazon and find 30 different coffee machines that you can get delivered to your house in two days. You'll still be able to go on Facebook and see how your old friend from school is doing."

What will change: "Small businesses would have a fair shot to sell their products on Amazon without the fear of Amazon pushing them out of business. Google couldn't smother competitors by demoting their products on Google Search. Facebook would face real pressure from Instagram and WhatsApp to improve the user experience and protect our privacy. Tech entrepreneurs would have a fighting chance to compete against the tech giants."

Warren conceded her proposals "won't solve every problem we have with our Big Tech companies."

"We must give people more control over how their personal information is collected, shared, and sold—and do it in a way that doesn't lock in massive competitive advantages for the companies that already have a ton of our data," she said. "We must help America's content creators—from local newspapers and national magazines to comedians and musicians—keep more of the value their content generates, rather than seeing it scooped up by companies like Google and Facebook. And we must ensure that Russia—or any other foreign power—can't use Facebook or any other form of social media to influence our elections."

"More competition means more options for consumers and content creators, and more pressure on companies like Facebook to address the glaring problems with their businesses," she added.

The Information Technology and Innovation Foundation, billed as the world's leading think tank for science and technology policy, said the Warren campaign's call to break up Big Tech companies reflects a "big is bad, small is beautiful ideology run amok."

"The proposal ignores the fact that many of the services Big Tech companies now provide free used to cost consumers money," said ITIF President Rob Atkinson. "Breaking up large Internet companies just because they are large won't help consumers. It will hurt them by reducing convenience, reducing quality of service and innovation, and in some cases leading to the introduction of priced services. Consumers now benefit greatly from having one Amazon, one Google, and one Facebook. The goal of competition policy should be to enhance consumer welfare, not penalize companies for earning market share and operating at scale—yet that is exactly what the Warren proposal would do."

To the extent that Warren is concerned about important issues like privacy, political power, or Russian interference, "the answer is not to break up tech companies but to pass a national privacy framework, campaign finance reform legislation, and laws regarding political ads," he added. ■

California is first state to mandate women on boards

Boards of directors for California public firms will now need to ensure that they seat more women at the table, writes **Joe Mont**.

California's state legislature recently passed SB-826, a bill mandating that companies headquartered in the state include female directors on their boards.

Signed on Sept. 30 by Governor Jerry Brown, it will require that, by the end of 2019, each publicly traded company based in California must include one woman on their board of directors; the quota increases by the end of 2021 based on company size.

The big question that faces the legislation: Can it survive already brewing legal challenges?

In 2013, a state senate resolution urged that by 2017, each public company in California increase the number of women on their board to one, two, or three, depending on the size of the board. California was the first state in the U.S. to adopt this type of resolution.

Nevertheless, as of the December 2016 cutoff date, fewer than 20 percent of the Russell 3000 companies headquartered in California had the minimum number of women directors called for in the resolution. That, in large part, inspired the more formal legislative demand—one that adds enforcement teeth.

No later than the close of the 2019 calendar year, the new legislation requires domestic and foreign publicly held corporations with principal executive offices in California (as reported in their 10-K form filed with the Securities and Exchange Commission) "to have a minimum of one female, as defined, on its board of directors, as specified."

By the close of the 2021 calendar year, the law increases that required minimum number to two female directors if the corporation has five directors or to three female directors if the corporation has six or more directors.

The law instructs California's Secretary of State to publish online reports documenting the number of corporations in compliance with these provisions and impose fines for violations.

Failure to timely file board member information with the Secretary of State will cost companies, for a first violation, $100,000; $300,000 for a second or subsequent violation. These fines are intended to offset the cost of administering the bill.

The legislative text details intended benefits. "More women directors serving on boards of directors of publicly held corporations will boost the California economy, improve opportunities for women in the workplace, and protect California taxpayers, shareholders, and retirees, including retired California state employees and teachers whose pensions are managed by CalPERS and CalSTRS," it says, adding that "studies predict that it will take 40 or 50 years to achieve gender parity, if something is not done proactively."

A 2017 report by Board Governance Research, conducted by University of San Diego professor Annalisa Barrett, is also cited. Among its findings:

- As of June 2017, among the 446 publicly traded companies included in the Russell 3000 index and headquartered in California, representing nearly $5 trillion in market capitalization, women directors held 566 seats, or 15.5 percent of seats;
- More than one-quarter (26 percent) of the Russell 3000 companies based in California have no female directors serving on their boards; and
- Just 12 percent of these companies have three or more female directors on their boards;
- Among the 50 California-based companies with the lowest revenues, just 8.4 percent of the director seats are held by women, and 48 percent of these companies have no women directors; and
- Among the 50 largest California companies, with

an average of nearly $30 billion in 2015 revenues, 23.5 percent of the director seats are held by women and all of the 50 have at least one female director.

A backgrounder that accompanied the legislation provided additional details to bolster the effort. It claims that "numerous independent studies have concluded that publicly held companies perform better when women serve on their boards of directors."

For example, a 2017 study by MSCI found that U.S. companies that began the five-year period from 2011 to 2016 with three or more female directors reported earnings per share that were 45 percent higher than those companies with no female directors at the beginning of the period.

In 2014, Credit Suisse research similarly found that companies with at least one woman on the board had an average return on equity of 12.2 percent, compared to 10.1 percent for companies with no female directors. Additionally, it said, the price-to-book value of these firms was greater for those with women on their boards: 2.4 times the value in comparison to 1.8 times the value for zero-women boards.

There is no shortage of opposition to the law, much of it spearheaded by the California Chamber of Commerce.

In a letter to the state legislature, prior to the vote, it and a coalition of like-minded trade organizations made their case. The law, it chided, would displace an existing member of the board, or promote an individual to the board of directors, "solely on the basis of gender."

"It would place gender as the main criteria of diversity over any other protected classification," the letter adds. "It also likely violates the U.S. Constitution, California Constitution, and California's Civil Rights Act, which places California companies in a legal predicament."

"Gender is an important aspect of diversity, as are the other protected classifications recognized under our laws," the Chamber wrote. "We are concerned that the mandate focuses only on gender and potentially elevates it as a priority over other aspects of diversity."

In a statement upon signing the bill into law, Gov. Brown conceded that such constitutional challenges were not unexpected. He also, by copying the U.S. Senate Judiciary Committee in his letter, took a swipe at the controversial confirmation process for Supreme Court nominee Brett Kavanaugh.

"There have been numerous objections to this bill, and serious legal concerns have been raised," Brown wrote. "I don't minimize the potential flaws that indeed may prove fatal to its ultimate implementation. Nevertheless, recent events in Washington, D.C.—and beyond—make it crystal clear that many are not getting the message."

"We are concerned that the mandate focuses only on gender and potentially elevates it as a priority over other aspects of diversity."

Chamber of Commerce

While California takes the lead among U.S. states seeking greater gender-based board diversity, moves are also afoot internationally. Other countries have addressed the lack of gender diversity on corporate boards by instituting quotas mandating 30 to 40 percent of seats to be held by women directors.

Germany is the largest economy to mandate a quota requiring that 30 percent of public company board seats be held by women; in 2003, Norway was the first country to legislate a mandatory 40 percent quota for female representation on corporate boards. Since then, other European nations that have legislated similar quotas include France, Spain, Iceland, and the Netherlands. ■

Are they REALLY who they say they are?

Know for sure with end-to-end AI-powered identity verification.

- Detect and deter identity fraud and account takeover
- Meet compliance requirements (AML, KYC, GDPR, CCPA)
- Convert good customers quickly and easily

jumio®

When Identity Matters

CCPA is Upon Us:

Get the Guide to CCPA Compliance at jumio.com