mlex
market insight
a LexisNexis® company

INSIGHT | COMMENTARY | ANALYSIS

SPECIAL REPORT
DEC. 12, 2019

What it means for businesses, how it is changing US approaches to data protection, and why its future is already clouded

CCPA

CALIFORNIA CONSUMER PRIVACY ACT

WASHINGTON | NEW YORK | SAN FRANCISCO | SEOUL | TOKYO | BEIJING | SHANGHAI | HONG KONG | JAKARTA | BRUSSELS | LONDON | SÃO PAULO | MELBOURNE | SYDNEY

Introduction

Mike Swift
Chief Global Digital Risk Correspondent

The California Consumer Privacy Act — the most comprehensive data-privacy law in US history — might be described as a small island of certainty surrounded by a fog of questions.

The law will take effect on Jan. 1, creating a series of new protections for California residents and opening the door for class-action litigation to be filed against companies that fail to keep their data safe. California Attorney General Xavier Becerra has begun building the enforcement machine that will apply the CCPA nationally — and perhaps even globally — starting six months later on July 1.

Beyond those predictable mileposts, however, lies a realm of uncertainty. Within a year, California residents could vote to overhaul the CCPA with even more stringent privacy and data-security protections, if millionaire privacy activist Alastair Mactaggart is successful in placing a measure on the statewide ballot in November that would create the first US standalone privacy enforcement agency. Or, sometime after the 2020 US presidential election, Congress could pass a US national privacy bill that takes precedence over the California law.

This paper was written and reported by Mike Swift and Amy Miller in San Francisco, Dave Perera in Washington, Sachiko Sakamaki in Tokyo and Matthew Newman in Brussels.

For profiles of all the reporters involved, please see page 23

In fact, both of those things could happen, muddling the US privacy enforcement picture for years.

There are other questions in the near term: Will the statutory damages built into CCPA fuel a surge of class-action litigation when the law takes effect in January? How successful will Becerra's new privacy team at the California Department of Justice be once enforcement of the CCPA's four new baseline privacy rights begins later in 2020? Will anyone file a court challenge to CCPA, potentially defanging a law that has been criticized for being hastily and sloppily drafted? Will other tech giants follow the lead of Microsoft and observe CCPA nationally — not just for their users in California — making it the de facto law of the land? Or will other states, such as New York and Washington, pass their own comprehensive privacy laws that make CCPA just one of many state laws?

The questions just keep coming. Most of the answers, however, will have to wait. If business craves regulatory certainty, the forthcoming effective date of CCPA will provide precious little of it. Jan. 1 will just be the beginning of a three-dimensional game of political, judicial and regulatory chess that wise companies will monitor closely over the next few years.

mlex market insight
a LexisNexis® company

Just about the only clear fact is that in less than a month's time, tens of thousands of companies that collect or sell the personal data of Californians must be ready to comply with a complex and comprehensive new privacy law, or risk significant financial penalties.

The focus of this report is not so much on the legal steps for how to comply with the CCPA. The goal is to clear away some of the fog around the law's uncertain future, to illuminate how California's privacy efforts are driving national action on data protection, and to show how the nascent law is already having an impact beyond the United States.

After a short overview of the privacy and data security requirements for business that CCPA will impose, we discuss how the landmark law could be superseded by federal legislation, ruled unconstitutional in the courts or replaced by an even more sweeping privacy law by California voters. Things could also go a different direction, with the California law sparking action by other states that could pass comprehensive privacy laws of their own.

This report will also discuss likely scenarios for private class-action litigation after the law takes effect in January, and for enforcement of the law's privacy provisions by the California Department of Justice from July.

We trust you enjoy reading this original MLex special report and find it a useful guide to a complex, evolving issue. The reporting here is a brief example of the insight and predictive analysis that MLex brings subscribers to our data privacy and security service every day. To ask about a trial subscription, see the contact details on page 2. ■

CHAPTERS IN THIS REPORT

mlex market insight
a LexisNexis® company

1 Overview: The working parts of a landmark new law in the US

The California Consumer Privacy Act of 2018 runs to well over 10,000 words. It is a groundbreaking piece of legislation that under political pressure passed through the state legislature in a matter of days, before being signed into law by the then California Governor, Jerry Brown, on June 28, 2018 — the very last day that proponents could withdraw a ballot initiative that would have provided very similar privacy rights.

California has always been a leader in data protection. The state passed the first US data-breach notification law back in 2003, and the state constitution already guarantees its residents a right to privacy. But the new law is California's most audacious play on privacy.

THE CCPA'S FOUR BASIC RIGHTS

Right to Know
Consumers get rights of transparency to know what personal information is collected about them and how it is used, shared or sold.

Right to Opt Out
Consumers can, by clicking on a link on a company's website or even through a browser setting, block the sale of their personal information to a third party.

Right to Delete
Consumers can demand that companies erase personal data held on them.

Right to Non-Discrimination
Businesses can't discriminate on price or service when a consumer exercises a CCPA-given privacy right.

The CCPA bestows on the state's nearly 40 million residents four key new data-privacy rights unprecedented in the United States — as outlined in the box at left.

Businesses cannot ignore a request by a consumer to view, delete or opt out of the sharing of that information. Businesses also have the responsibility to verify the identity of consumers making that request. Additionally, CCPA prohibits businesses from selling the personal information of a consumer under 16 years of age without opt-in consent. That consent must come from a parent or guardian if the child is under 13.

The law was initially pitched by its proponents as being aimed at large and mid-sized companies, allowing small businesses relief from its significant regulatory burdens. CCPA applies to businesses with annual revenues of at least $25 million; or that buy, receive or sell the personal information of 50,000 or more consumers, households or devices; or that derive more than half of their annual revenue from the sale of personal information.

However, the regulatory impact of the law will be both deep and broad, with the state's own fiscal analysis saying

THE CCPA'S TARGETS AND PENALTIES

Who does it apply to?
Companies have CCPA obligations if they do business in California **AND** they:

Make revenue of more than $25 million a year
OR
Collect data from more than 50,000 individuals a year
OR
Make more than half their annual revenue by selling personal information.

That's been estimated at half a million companies in the US alone, with potentially tens of thousands more overseas.

What are the penalties?
For noncompliance, the penalties per violation are $2,500 if unintentional or $7,500 if intentional.

For data breaches that expose personal information, consumers can sue for $100-$750 per violation, or greater if the actual damages exceed $750.

Privacy incidents can affect thousands or tens of thousands of consumers, in which case these fines could easily reach millions of dollars.

compliance costs will range between $467 million and $16.5 billion for the decade of 2020 to 2030.

Small businesses will be hit particularly hard, the state assessment found, a conclusion based on the experience of Europe's General Data Protection Regulation, or GDPR.

The initial compliance cost for a small business would be $25,000, and about $1,500 in subsequent years, while the initial cost for a "typical" business of around median size would be $75,000 in the first year, and then $2,500 annually.

CCPA carries a broad definition for what comprises "personal information" considered to be protected, including not only biometric information such as fingerprints, voice prints and facial recognition templates, but even data less frequently thought of as identifying an individual, including how people type, walk and even sleep. The CCPA's definition for biometric data includes "keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health or exercise data that contain identifying information."

It would be a mistake the think of the CCPA as "the California GDPR," because its aim is different to the European regulation. Unlike the GDPR, the California law wasn't intended to govern the collection of personal information, but to give consumers tools to limit its sharing, should they choose to use those tools. If consumers take no action, under CCPA, there are no restrictions on how businesses use their data.

But there are cross-connections between the EU and California law. Many of the compliance steps required to comply with the GDPR, such as mapping the collection and flow of the data, are also prerequisites for complying with the CCPA.

Path to privacy: The CCPA's bumpy ride

2017

November Real-estate magnate Alastair Mactaggart, founder of Californians for Consumer Privacy, finalizes plan to put consumer Internet privacy initiative on state ballot in November 2018. Over the next six months, state lawmakers negotiate a deal to enact consumer privacy legislation instead.

2018

May 3 Mactaggart collects 366,000 valid petition signatures from supporters in California to qualify for ballot initiative.

Late June Mactaggart makes deal with legislators to withdraw ballot initiative if they pass state law, agreeing to forfeit private right of action for privacy (but not data breach) violations.

June 28 California Governor Jerry Brown signs California Consumer Privacy Act into law.

Aug. 24 California Attorney General Xavier Becerra warns that he lacks resources to implement and enforce CCPA.

2019

Jan. 1 "Lookback" period begins: when CCPA enters force on Jan. 1, 2020, it will require disclosures based on companies' collection, use and sharing of data over the previous 12 months.

Sept. 24 Mactaggart announces plan for 2020 ballot initiative to overhaul CCPA. The "California Privacy Rights Act" would create new standalone state privacy enforcement agency.

Oct. 10 Publication of proposed implementing regulations for CCPA to provide practical guidance to consumers and businesses subject to the law. Public comment period begins.

Nov. 13 Mactaggart files papers to begin process of putting proposed California Privacy Rights Act on the November 2020 ballot.

Dec. 6 Public comment on CCPA implementing regulations closes. The attorney general may revise the regulations based on comments. If so, there will be a further 15-day public comment period, then the text will go to the Office of Administrative Law for review of up to 30 working days. If approved, the rules will go into effect.

2020

Jan. 1 CCPA enters force. Consumers can request to know where their data have been sold or disclosed over the past 12 months. Private litigation can be filed over data breaches.

May 7 Last day for California Secretary of State to determine whether Mactaggart's new ballot initiative petition meets the minimum signature requirement to qualify for ballot.

June 25 Last day for California Secretary of State to determine that initiative qualifies for the ballot or to pull it.

July 1 Deadline for Attorney General's Office to adopt CCPA implementing regulations; date that its enforcement begins for privacy violations, such as failing to honor a request to opt out of data sharing.

Nov 3 If California Privacy Rights Act measure is on the ballot, California voters would decide whether it becomes law.

2 The door opens to litigation on Jan. 1, and many companies won't be ready

While the CCPA takes effect on New Year's Day, with a one-year look-back period that holds companies responsible for their actions since Jan. 1, 2019, companies have another six months before enforcement begins by the California Department of Justice of the four new privacy rights in the law.

Given that extra time for compliance, many companies have taken a wait-and-see approach. A tiny two percent of the businesses surveyed this spring and summer by the International Association of Privacy Professionals and OneTrust said they were fully compliant with the CCPA.

The CCPA is complex and potentially evolving, which presents additional compliance challenges, companies told the IAPP. Adding to the confusion is the fact that the regulations that will guide its enforcement —for example, giving an exact description of how a company must verify a consumer's identity, for example — are not yet finished, with the California DOJ not expecting to finalize them until July.

The biggest obstacles, according to the IAPP surveys? Not surprisingly, a lack of time and resources. Some companies have been making progress on compliance, albeit incrementally. About 25 percent of the companies surveyed in April said they were aiming to be compliant by the time enforcement begins on July 1 next year. By this summer, that number had crept up to 33 percent. A more recent survey, released in November by Osterman Research and Egress Software Technologies, did have some better news but still found that only 48 percent of companies said they would be compliant by the end of this year.

Companies that are already compliant with GDPR do have an advantage, according to the IAPP survey, which found that one in three organizations were able to leverage their GDPR compliance to get ready for the CCPA.

A more basic form of compliance is the requirement that companies maintain "reasonable" cybersecurity. Companies that fail to do that, and then suffer a data breach, run the risk of having to defend costly private litigation that will also expose them to the risk of potentially large statutory damages.

Some California-based technology companies, including Snap, Adobe and Uber

Companies already compliant with GDPR do have an advantage, according to the IAPP survey, which found that one in three organizations were able to leverage their GDPR compliance to get ready for the CCPA.

GDPR similarities

- Comprehensive data-protection regulation with ex-ante rules.
- Significant financial penalties for violations (GDPR up to 4 percent of global turnover, CCPA up to $7,500 per violation).
- Largely relies on existing regulators for enforcement.
- Broad definition of personal data.

GDPR differences

- GDPR has requirement to opt in to data collection, unlike CCPA.
- Ability to opt out of sale of private information to third parties, unlike GDPR.
- Does not apply to small businesses.
- GDPR has a "right to be forgotten," CCPA does not.

Technologies, are already warning their shareholders that CCPA may trigger a wave of data-breach litigation after Jan. 1.

The CCPA's inclusion of a private right of action for data breaches, coupled with statutory damages, is likely to increase both the likelihood and cost of litigation, with effects that could be "far reaching," Snap told investors in a quarterly securities filing in October.

The CCPA carries statutory damages of up to $750 per violation for a company that suffers a data breach resulting from a failure to maintain "reasonable" security measures. For a tech company that could have several million users in California, a data breach by a company that fails to prove that it had taken steps to maintain strong security could easily face a theoretical liability in the tens of millions or even hundreds of millions of dollars.

A prophylactic defense is for companies to bolster their cybersecurity protections now, document the improvements they are making to comply with security standards and prepare a response plan in the event they are breached.

Many companies are hurrying to create data-breach response plans. They are also making sure their security is aligned with relevant standards such as the voluntary cybersecurity framework developed by the National Institute of Standards and Technology, or NIST.

Even companies that successfully defend CCPA data-breach suits will likely face significant litigation costs, however, and a surge in litigation could have secondary effects such as making data-breach insurance more expensive and difficult to obtain. The experience of privacy laws that carry statutory damages — the Telephone Consumer Protection Act of 1991 is one good example — suggests it is highly likely that there will be some CCPA data-breach litigation filed in the California state courts after Jan. 1, even if there remains significant uncertainty over how much.

3 Enforcement: How California's new privacy cops are preparing

CCPA enters its second phase next July, when official enforcement begins of consumers' new rights to transparency, deletion, opt-out of the sale of their data, and non-discrimination in services if they exercise those rights. As the authority tasked to police those privacy rights, the California Department of Justice is preparing to take its place beside the Federal Trade Commission as a US privacy enforcer with the personnel, budget and enabling law to give it a national regulatory footprint. Absent the CCPA being superseded by a federal law or replaced in a 2020 ballot initiative, companies should expect the California Attorney General's Office, which oversees the California DOJ, to exercise its new powers.

Attorney General Xavier Becerra has begun a four-fold expansion of the department's privacy enforcement team. It is in the process of hiring lawyers and legal analysts and is budgeting money for technology experts who will help it not only enforce CCPA but also to defend the fledgling law from an anticipated wave of court challenges.

Becerra asked the state legislature for funds and has received $4.5 million for ongoing enforcement and defense of the CCPA, funding that will support 23 additional positions, including eight deputy attorneys general, eight legal analysts, six clerical staffers and $250,000 a year for expert consultants.

The enhanced enforcement team will be headed by two well-regarded, veteran lawyers on the attorney general's staff: Nicklas A. Akers, a senior assistant attorney general; and Stacey D. Schesser, a supervising deputy attorney general who Becerra described as "quite honestly, the point person" for CCPA enforcement. Another key figure on the team is Eleanor Blume, a special assistant attorney general who joined the agency in 2017 from the Consumer Financial Protection Bureau, where she was a counsel for five years, joining in the early years of that regulator.

The Privacy Unit of the California DOJ's Consumer Law Section estimates bringing at least two lawsuits annually and devoting about 15,000 hours a year starting in the 2020-21 fiscal year to investigations and prosecutions under the CCPA, according to budget documents, but the agency also noted to lawmakers that "these estimates may reflect a minimum."

Unlike the FTC, Becerra's team won't just have to enforce the new law; they will also have to defend it from what the California DOJ expects will be multiple court challenges that could

California Attorney General Xavier Becerra introduces senior members of his new privacy enforcement team team tasked with policing the CCPA.
Photo: Mike Swift/MLex

limit enforcement, as well as challenges to the forthcoming set of regulations that would direct its enforcement. A series of court challenges to the law could certainly suck bandwidth away from enforcement efforts.

The Attorney General's Civil Law Division believes it will have to defend something like four lawsuits through the 2023-24 fiscal year, including state and federal lawsuits that would challenge the CCPA, and two other state lawsuits challenging the CCPA regulations and amendments to the regulations.

Since the CCPA was "only recently passed, no lawsuits have yet been filed, and the number of lawsuits that will be filed is uncertain. Nonetheless, given the economic and privacy interests at stake, litigation is probable," Becerra's office told lawmakers.

Indeed, it's already possible to see the form that a challenge to the CCPA will likely take. A new paper by a scholar at George Mason University's Mercatus Center argues that state and local data-privacy laws such as CCPA could violate the constitution in three ways. First, state privacy laws could violate the Dormant Commerce Clause, which says states can't discriminate against interstate commerce; second, they could violate First Amendment guarantees to free speech; and, third, they could conflict with existing federal law.

4 A US state law that threatens to have international impact

From Japanese manufacturers to European data brokers, multinational companies have joined American businesses in a scramble to comply with California's new privacy law. But, if anything, there is even more uncertainty for non-US companies about whether CCPA applies to them, because of the complexity and ambiguity of some aspects of the law, and because the California law lacks the pre-implementation period that was in place before the 2018 effective date of Europe's GDPR.

Among Japanese companies, an increasing number have been rushing to boost their compliance, with some multinational businesses well prepared, while others are still unaware of potential risks. But while Japanese lawyers who practice international data-protection law believe the CCPA's extraterritorial reach is quite broad, some feel its sanctions and impact are harder to determine than the GDPR.

Among Japanese companies, an increasing number have been rushing to boost their compliance, with some multinational businesses well prepared.

Some Japanese multinationals, such as automaker Subaru and e-commerce giant Rakuten — two companies with a significant presence in California — seem well prepared for implementation of the CCPA, while other companies have left the task to their US subsidiaries.

"[CCPA] rules require continuous measures, so we will continually take steady measures, stage by stage," a Rakuten spokesman said in an e-mail response to a question by MLex about whether the company will be ready to comply by Jan. 1.

One reason for the slow start by some companies is that CCPA's enabling regulations weren't proposed until October, and they won't be finalized for months following the close of a public consultation period on Dec. 6. This has left many Japanese companies waiting for details, especially auto-parts makers, which do businesses with other US companies rather than directly with consumers.

European companies are also preparing for implementation of the CCPA. There's a rush by companies seeking advice on compliance that resembles what occurred before the GDPR took effect in May 2018. But many businesses remain unclear about how the new law will

affect them. European businesses especially aren't used to the idea of facing potential liability from lawsuits, which presents another area of uncertainty for them. Enforcement in Europe is through data-protection authorities, not civil litigation.

European companies that are involved in a data-driven business, such as data brokers — which buy and sell data — will have to comply with the California law, allowing citizens of the state to opt out of the sale of their personal information. But for other companies that have third-party cookies on their websites, there remains much uncertainty — it's unclear whether the CCPA will consider that as a "sale" of data, uncertainty that will linger until the regulations are finalized toward the middle of 2020.

European businesses especially aren't used to the idea of facing potential liability from lawsuits, which presents another area of uncertainty for them.

Companies that completed the process of complying with the GDPR — whether they are based in Europe or somewhere else — do have an advantage in terms of compliance costs. They have already assessed what data they have and what they process. They understand where the data are held and are most likely using the same e-mail system in Europe and California.

The California attorney general disclosed in a regulatory filing this autumn that his office considered — but rejected — a proposal that GDPR-compliant companies could obtain a limited exemption from CCPA, arguing that there are "key differences between the GDPR and CCPA, especially in terms of how personal information is defined and the consumer's right to opt out of the sale of personal information."

In part for that reason, companies would be mistaken to assume that if they comply with GDPR, they would also be in good standing with the CCPA. The two laws have different definitions, requirements and objectives.

For instance, once the CCPA enabling regulations are finalized next year, they will have specific, detailed rules on how to verify a consumer's identity, and how businesses must respond when they receive consumer requests for data deletion and disclosure. Those are rules that don't exist in the GDPR.

5 CCPA leads the privacy debate, but Washington may supplant it

In Washington, the Capitol Hill crowd divide the recent history of privacy into two periods: pre-CCPA and post-CCPA. Beforehand, the prospect of a comprehensive privacy bill hadn't seemed great. Afterward looks very different. Big Tech is on a lobbying spree, privacy advocates are unusually buoyant, and members of Congress have discussed and introduced an unprecedented number of privacy bills.

In sum, the effect of the CCPA in Congress has been dramatic. It has vaulted privacy to the forefront of discussion about new legislation. The final weeks of the 2019 congressional session alone saw separate, comprehensive legislative proposals presented by the Democratic and Republican leaders of the Senate Commerce Committee as well as an exacting bill introduced by two Democrat House members who represent major chunks of Silicon Valley.

The CCPA's effect in Congress has been dramatic. It has vaulted privacy to the forefront of discussion about new legislation.

But for all the urgency the California law brought to Washington, its influence has limits. Predictions that industry would hurry lawmakers into passing a nationwide privacy standard before the CCPA could take effect have failed to materialize. Even record-setting amounts spent by companies such as Amazon and Facebook on lobbying didn't turn federal privacy proposals into reality in 2019.

Privacy advocates also say that because of the CCPA, the debate in Washington has grown more sophisticated, with sights set on a more ambitious collection of consumer rights and corporate limitations. Some note that CCPA is basically just a vehicle that lets consumers opt out of having their data shared with third parties, and that a comprehensive national law might be able to do more.

Both dueling proposals of the Senate Commerce Committee, for example, agree that consumers should need to give "prior, affirmative express consent" for processing sensitive data. The CCPA requires affirmative consent only for the sale of personal data of minors under 16. Both committee proposals contain language limiting the corporate collection of consumer data, whereas the CCPA focuses on private-sector transparency about data collection.

The Senate committee proposals also raise the problem of algorithmic bias, even if the Democrats' bill goes much farther than the Republican proposal by prohibiting companies

from using data tied to a person's ethnicity, religion, gender or other protected status to discriminate when marketing offers of housing, employment, credit or education.

By enacting the nation's first privacy law, California now also presents a conundrum to federal lawmakers: Should they let states develop and enact their own laws, or supplant the CCPA by passing their own law through "preemption," a US legal principle whereby legislation enacted through Congress overrules conflicting state laws where Congress has expressly stated an intent to do so.

In a flip of the political parties' traditional positions on states' rights, Republicans and industry clearly lean toward preemption, the stronger the better. In contrast, many progressives urge allowing states to keep passing their own privacy laws, especially since local governments may more easily respond to emerging threats than lumbering, politicized Capitol Hill. Many Democrats have been careful to tread a middle line on preemption that allows for it but without endorsing it outright. Why not use it as a negotiating ploy for extracting Republican concessions, they argue: Earn preemption with a bill worthy of supplanting the CCPA.

Lately there's been a recognition that preemption needn't be a binary proposition, either completely excluding state laws or allowing experiments to bubble in the laboratories of democracy. Preemption can be hard, or it can be soft, such as by allowing states to add requirements but not eliminate them or creating preemption exemptions for certain data. In fact, members of Congress will have to be careful in wielding preemption, since states, counties and cities have built up privacy-adjacent laws governing access to things like student records and unfair consumer practices. Sweeping them away would have significant, unintended consequences.

A similar catalog of hard and soft solutions exists for a private right of action, a measure favored heavily by Democrats and at best tolerated by Republicans.

Having failed to pass a bill before the CCPA goes into effect, Congress might feel a slight, if temporary, lessening of industry pressure to approve legislation after Jan. 1. But that may depend on how many Golden State residents decide to exercise their new right to opt out of the sale of their data and on how aggressively state attorneys and private litigators go to court against tech companies. Those data points will take time to accrue.

Congress is unlikely to be in a bill-passing mood in 2020, anyhow. Impeachment proceedings plus additional possible standoffs with President Donald Trump are set to dominate Washington for now. Even if those faceoffs were to subside by the first few months of the coming year, 2020 will see a presidential campaign that promises to squeeze out consideration of other matters. A federal privacy law will likely have to wait until 2021, at the earliest.

6 California's wrangle isn't over yet. Voters could overhaul CCPA in 2020

Even in California, the political struggle over CCPA is far from finished even as the law takes effect. Indeed, its greatest backer has launched a new political campaign to expand and buttress the law and even create a bespoke privacy watchdog.

In September, Bay Area housing developer Alastair Mactaggart, who launched the campaign that ultimately led to the CCPA, proposed a new privacy initiative that would expand the CCPA by establishing new privacy rights protecting "sensitive personal information" on health, finances, race and ethnicity, and an individual's location. It would also create the first single-purpose data-protection authority in the US, a "California Privacy Protection Agency."

If Mactaggart can collect enough signatures from California voters to get his new proposal listed as a ballot initiative — the powerful direct democracy tool in many US states that lets citizens put a legislative idea to a public vote — then the next major battle over privacy in the Golden State would be next November, in a campaign that would play out in parallel to the US presidential election.

After spending $3.5 million of his own fortune on his first privacy campaign in 2018, Mactaggart opted for a compromise to ensure that the bulk of his proposal would become law. He agreed to limit the private right of action in CCPA to data breaches and undertook to withdraw his ballot initiative so long as the rest of the law was adopted, a deal that left the elected legislature in control of privacy regulation in California.

But events since 2018, including efforts by the tech industry to pare back CCPA in the California legislature, or to push Congress to preempt CCPA with a national law, have the privacy advocate in no mood for compromise in 2020.

His new initiative would put significant new limits on the sale and use of personal health and financial information, as well as limits on the use of information on race and ethnicity, and a person's precise geolocation. Under the proposal, companies could still track people to a general location, but not to where they go specifically. Businesses would have to get permission from a parent or guardian to use a child's data, and they could be fined triple the damages if they violate a child's privacy.

There would also be expanded transparency rules around automated decision making and

Alastair Mactaggart's plan to get his extended privacy initiative onto next November's California ballot faces stiffer challenges than his original 2018 proposal.

consumer profiling, requiring companies to disclose more information about decisions that affect areas such as employment, housing, credit and politics.

And a five-member board appointed by the governor, legislative leaders and the state attorney general would oversee the proposed new California Privacy Protection Agency, which would be funded by fines collected from companies that violate residents' privacy.

Getting the proposal on the 2020 ballot, though, could be a challenge. California is one of several US states that let voters bypass their state legislatures and vote directly on proposed laws, if the sponsors can collect enough signatures to get on the ballot. But that costs money. Mactaggart has not said how much of his own money he plans to spend to gather petition signatures next year.

The minimum threshold to get a proposed law on the statewide ballot is 5 percent of the votes cast in the most recent election for state governor. In 2018, Mactaggart's group, Californians

for Consumer Privacy, collected about 366,000 signatures from eligible, registered voters to successfully place on the ballot his first initiative, which ultimately became the CCPA.

But because far more Californians voted in the 2018 gubernatorial election — about 12.6 million — than in the previous one in 2014, Mactaggart must this time gather at least 623,212 signatures. And not every signature will ultimately be an authenticated registered voter. That means sponsors must collect significantly more than the minimum threshold number of signatures to successfully qualify for a ballot initiative. Mactaggart has acknowledged that his campaign needs 1 million signatures.

Californians for Consumer Privacy expects to start gathering that mountain of signatures sometime this month, once the Office of the California Attorney General signs off on the legal summary of the initiative. Under California law, proponents have up to 180 days from the official summary date to circulate petitions, collect signatures and file those signed petitions with county election officials.

Mactaggart has said that 90 percent of the people he's polled support his latest effort and claimed that the tech industry would have to spend hundreds of millions of dollars to defeat it.

The campaign has until early May to gather enough signatures and have them certified valid by the Secretary of State of California. The deadline for Mactaggart's ballot initiative to be certified for the Nov. 3 election next year is June 25. If voters approve the ballot initiative, it would take effect on Jan. 1, 2021. Mactaggart said this time, he doesn't want the state legislature to take over.

Mactaggart agreed to withdraw his first proposed ballot initiative in June 2018, after gathering the required signatures, on the understanding that the California legislature would pass a privacy law. That deal allowed elected lawmakers, rather than the state's voters, to retain control over privacy regulation in California.

Under his latest proposal, lawmakers could amend the law by a simple majority vote, but proposed amendments would only be allowed if they were aimed at advancing privacy rights. Even if he doesn't get enough signatures to be on the ballot next year, Mactaggart said politicians won't be able to ignore the strong public support for privacy protections.

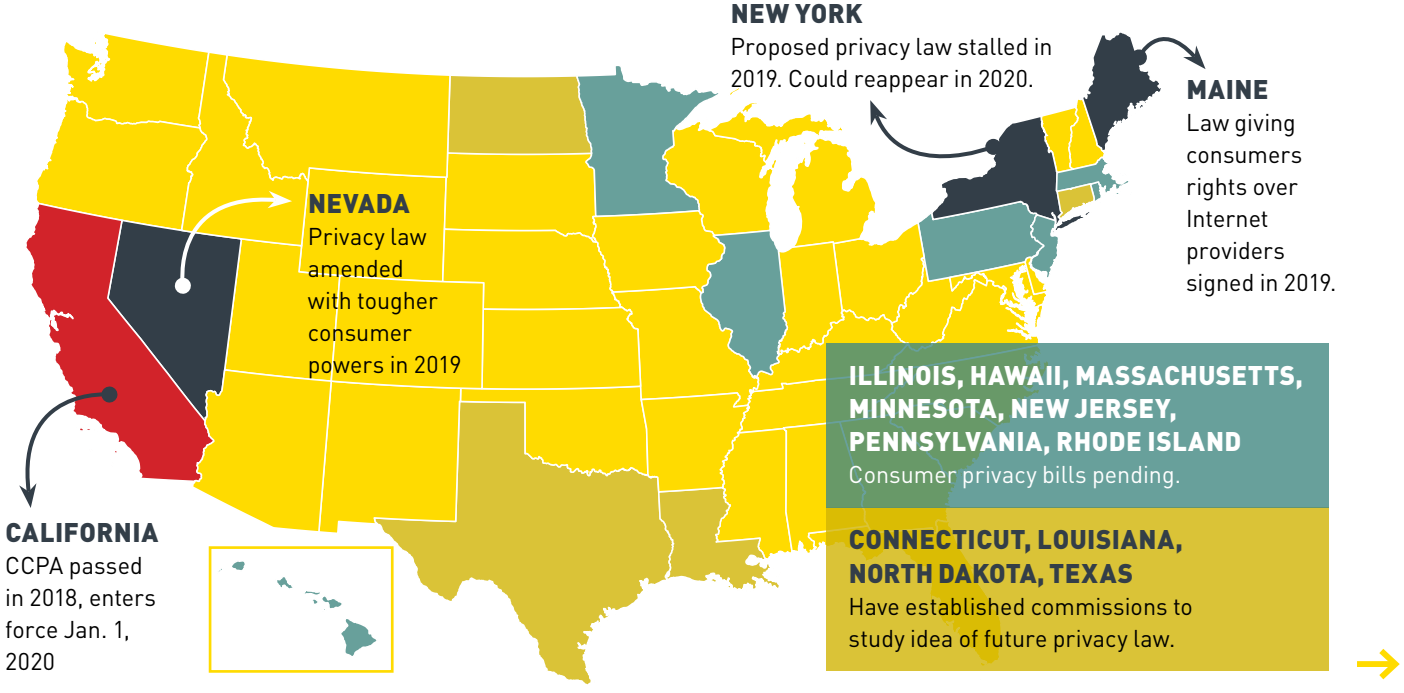
He has said that 90 percent of the people he's polled support his latest effort and claimed that the tech industry would have to spend hundreds of millions of dollars to defeat it. Back in 2018, the revelation of the Cambridge Analytica privacy scandal in the middle of Mactaggart's petition drive acted as a kind of fuel for the campaign.

7 We want better protections too! Other states pushing for privacy

As usual on privacy issues, California blazed a trail in passing a comprehensive privacy law. And as in other things, California now has imitators. Several other US states have enacted or expanded their own privacy and data security laws, and that trend could continue or even intensify.

While none of the new state laws so far have been as comprehensive as the CCPA, it is well within the bounds of possibility that other states could pass legislation in the coming year that would enact additional regulatory burdens in excess of that required by the CCPA.

New York may be the next to do that. Last May, a New York state senator from Long Island, Kevin Thomas, introduced a bill that included the concept of a "data fiduciary," the idea that companies that collect and store consumer data have the obligation to use those data in the best interests of the consumer.



The proposed New York Privacy Act, which courted controversy by including a private right of action for data-protection violations — and not just data breaches, as in California — died in committee earlier this year. But Senator Thomas expects to reintroduce the bill as soon as early January, although it is still in revision and its final form remains uncertain.

Other states have already passed privacy laws. In May this year, Nevada amended an existing law and now requires businesses to offer consumers an opt-out from the sale of their personal information, albeit with many exceptions for a wide range of companies.

But Nevada Governor Steve Sisolak signed the bill only after legislators removed a provision that would have allowed consumers to sue companies for violations. Lawmakers introduced several business-friendly exemptions and narrowed the definition of "sale" to "monetary consideration."

The more states that pass their own privacy rules, the greater the political pressure will be on Congress to pass a national bill that would preempt state privacy rules.

In June, Maine Governor Janet Mills signed legislation to limit the ability of broadband providers to trade in consumer information. From July 1, 2020, broadband providers will have to get consumers' express permission before using, disclosing, selling or permitting access to their personal information, although there are some exceptions.

In an echo of CCPA's non-discrimination right, the Maine law also prohibits broadband providers from refusing to serve a customer or charging them more if they don't consent to the use, disclosure, sale or access of their personal data.

Several state legislatures declined to pass bills modeled after the CCPA, but they did amend those proposals to establish commissions that will study the possibility of passing privacy legislation in the future. Those states include Connecticut, Louisiana, North Dakota and Texas.

Meanwhile, privacy bills are still pending in Illinois, Hawaii, Massachusetts, Minnesota, New Jersey, Pennsylvania and Rhode Island that would implement new requirements for companies doing business in their states that collect or process residents' personal information.

All the activity at state level could have a result that is very different from that which local lawmakers intend. The more states that pass their own privacy rules, the greater the political pressure will be on Congress to pass a national bill that would preempt state privacy rules precisely to avoid a checkerboard of regulatory rules based on state laws.

8 Conclusion: Some known knowns ... but a slew of known unknowns

As audacious as the California Consumer Privacy Act is, it may well emerge that that the law represents only a way station in the evolution of data-protection law in the United States.

Microsoft gave the CCPA a vote of support when the maker of Windows said it would extend the law's core rights for people to control their data to all of its customers in the US, not just in California.

The fact that it will be exceedingly difficult to segregate the personal data of Californians from the data of consumers in the other 49 US states suggests other companies will follow Microsoft's lead, although other big tech companies — including Facebook, Google, Apple and Twitter — have not yet followed with similar pledges.

While the timing remains highly uncertain for Congress to pass a federal privacy bill, it appears inevitable that it will happen within two to five years. A bigger question for companies, as they prepare for the CCPA, is whether the federal law will be written to coexist with or to preempt the California law and other state privacy laws that will be passed before Washington lawmakers finally act.

For now, perhaps the biggest regulatory risk issues for companies are how aggressive the California Department of Justice will be in its enforcement.

That question, given the political power of House Speaker Nancy Pelosi — a CCPA supporter from San Francisco — and the rest of the California congressional delegation, is impossible to answer at this time.

For now, perhaps the biggest regulatory risk issues for companies are how aggressive the California Department of Justice will be in its enforcement. Attorney General Becerra has his own doubts on that score. He has said repeatedly that a private right of action should be added to the CCPA for privacy violations, not just data-breach violations, because the California DOJ under his office lacks the resources to protect the privacy of 40 million people, and it needs the plaintiffs' bar to help achieve that goal.

Becerra has taken heat in recent months for failing to join the antitrust probes of Google

and Facebook that were joined by virtually all the other states. But criticism that the attorney general was afraid to lock horns with powerful California technology companies came before it became public that Becerra had launched an investigation of Facebook's privacy practices in 2018, less than two months after revelations of the Cambridge Analytica privacy leak.

A long-time member of Congress before becoming California's attorney general, Becerra is aware of the political potency that privacy has among voters right now.

Since then, Becerra has hit Facebook with two investigative subpoenas and sued the company in San Francisco to force it to turn over e-mail correspondence of Mark Zuckerberg and other top executives. A long-time member of Congress before becoming California's attorney general, Becerra is aware of the political potency that privacy has among voters right now.

With an enforcement budget in hand, a powerful enabling law and a newly minted enforcement team, look for Becerra's team to be aggressive in its enforcement of CCPA starting in the second half of 2020. If everything else is shrouded in uncertainty, that at least seems a good bet. ■

Contributors to this report

Mike Swift

Chief Global Digital Risk Correspondent

Formerly chief Internet reporter for the San Jose Mercury News and SiliconValley.com, Mike has covered Google, Facebook and Yahoo closely as he followed trends in search, the mobile web and online social networks. He helps coordinate MLex coverage of privacy and data security worldwide. A former John S. Knight Fellow at Stanford University, he is a graduate of Colby College. He is an award-winning journalist with expertise ranging from the business of professional sports to computer-assisted reporting.

Amy Miller

Senior Correspondent, Data Privacy & Security

Amy is responsible for the coverage of an array of regulatory and litigation issues pertaining to the Internet, including privacy, data security and antitrust. Formerly a legal reporter for the ALM media group, Miller has closely followed legal trends in Silicon Valley and covered corporate legal departments for online and print publications including The American Lawyer, Corporate Counsel, and The Recorder. Miller is a graduate of Columbia University Graduate School of Journalism and is an award-winning journalist with expertise ranging from education and legal reporting to computer-assisted reporting.

Dave Perera

Data Security & Privacy Reporter

Dave Perera joined the Washington, DC office as our new technology reporter as we built out that part of our coverage. He is a veteran cybersecurity reporter for Politico and a former editor for FierceMarkets publications. Dave studied Spanish and Italian literature at the University of Colorado, and has a Master's degree from the Columbia University School of International and Public Affairs.

Sachiko Sakamaki

Senior Correspondent, Tokyo

Sachiko covers antitrust, anti-bribery & corruption, and privacy & cyber security. She has an undergraduate degree from Waseda University in Tokyo and a master's degree in communications from United States International (now Alliant International) University in California. She previously worked as a journalist for Time magazine, the Far Eastern Economic Review, Bloomberg News, and the Washington Post in Japan.

Matthew Newman

Chief Correspondent, Brussels

Matthew writes about mergers, antitrust and cartel investigations as well as digital risk. Matthew began covering competition at the Luxembourg courts in 2004 and then moved to Brussels. After working as a spokesman for the European Commission until April 2012, he spent several months in Washington, DC writing about mergers for MLex. He spent a year studying French, history and communications in Grenoble, France and is a graduate of Boston University with degrees in history and journalism.

Built on TRUST

MLex's unique insight, analysis and commentary delivers investigative and forensic coverage of cases working their way through decision-making bodies and regulatory agencies around the world. Regulatory change is coming. Be ready. Be the first to understand how regulatory change impacts you or your clients. **Request a free trial.**

MORE THAN 2,100 USERS FROM
G7 REGULATORS
SUBSCRIBE TO MLEX

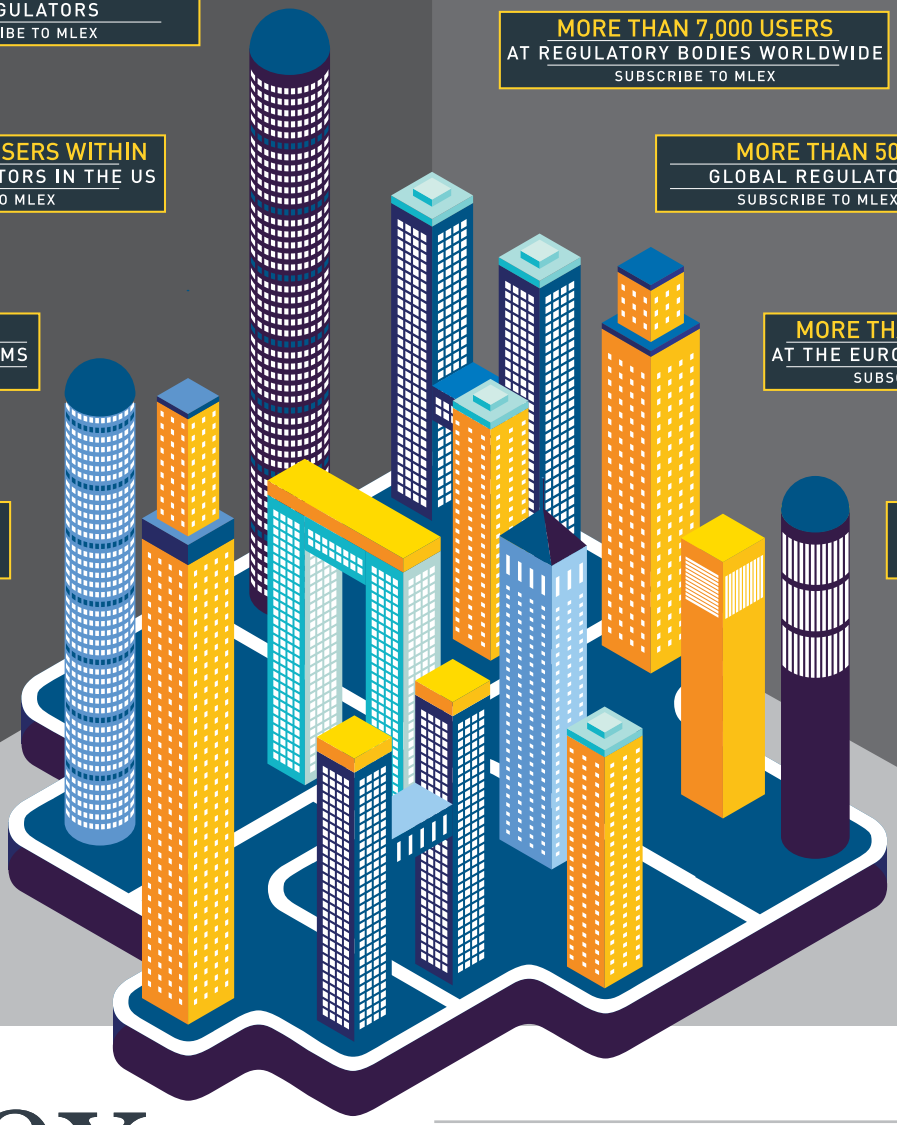
MORE THAN 7,000 USERS
AT REGULATORY BODIES WORLDWIDE
SUBSCRIBE TO MLEX

MORE THAN 800 USERS WITHIN
ANTITRUST REGULATORS IN THE US
SUBSCRIBE TO MLEX

MORE THAN 50
GLOBAL REGULATORS
SUBSCRIBE TO MLEX

9 OF THE TOP 10
GLOBAL TECHNOLOGY FIRMS
SUBSCRIBE TO MLEX

MORE THAN 2,300 USERS
AT THE EUROPEAN COMMISSION
SUBSCRIBE TO MLEX



THE TOP 10
EUROPEAN LAW FIRMS
SUBSCRIBE TO MLEX

90% OF THE TOP 50
GLOBAL LAW FIRMS
SUBSCRIBE TO MLEX

mlex
market insight
a LexisNexis® company

UK: +44 800 999 3237
US: +1 800 356 6547
Hong Kong: +852 2965 1424
www.mlexmarketinsight.com
customerservices@mlex.com