Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Proposed Bill to Expand the CCPA's Private Right of Action Likely Dead For the Year

May 17, 2019

Key Points

- On May 16, 2019, the California Senate Appropriations Committee held Senate Bill 561 (SB-561) in committee, likely blocking its passage this term.
- SB-561, co-authored by the California Attorney General, would have expanded the private right of action in the California Consumer Privacy Act (CCPA) to include all violations of the law, not just in the data breach context, and would have eliminated the right of businesses to seek guidance from the Attorney General on CCPA compliance.
- The demise of SB-561 ensures that the CCPA will take effect with the governmental enforcement regime intended by the first drafters, rather than a private, class action-driven enforcement regime. This should be welcome news to businesses who will face the compliance challenges that the CCPA poses.

Background

The CCPA, which goes into effect on January 1, 2020, is by far the nation's strictest and most expansive privacy law. It grants California residents broad and purportedly inalienable rights of consent, access and deletion with regard to their personal information (PI); has an expansive, extra-territorial scope; governs the collection and sale of consumers' PI; and prohibits discrimination against consumers who exercise rights under the law. The CCPA grants consumers a private right of action ***only*** for certain violations arising in the data breach context, and otherwise places responsibility for enforcement on the California Attorney General's Office. The law, as originally drafted, contemplates a central role for the Attorney General, who is tasked initially with preparing regulations and providing opinions to guide businesses on compliance issues, and then ultimately with broad and exclusive enforcement power outside the data breach context.

In February 2019, Senator Hannah-Beth Jackson introduced SB-561, co-authored by the Attorney General, to amend the CCPA to expand the private right of action to any violation of the law and to eliminate the right of businesses to seek the Attorney General's guidance on compliance issues. SB-561 also would also have eliminated

Contact Information

If you have any questions concerning this alert, please contact:

Kathryn E. Deal
Partner
kdeal@akingump.com
Philadelphia
+1 215.965.1219

Seamus C. Duffy
Partner
sduffy@akingump.com
Philadelphia
+1 215.965.1212

Hyongsoon Kim
Partner
kimh@akingump.com
Irvine
+1 949.885.4218

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Neal Ross Marder
Partner
nmarder@akingump.com
Los Angeles
+1 310.728.3740

Michael W. McTigue Jr.
Partner
mmctigue@akingump.com
Philadelphia
+1 215.965.1265

the 30-day period businesses have to cure alleged violations prior to Attorney General enforcement. A motivating force behind the bill was apparently the Attorney General's concern over his office's lack of enforcement resources. The bill faced strong opposition from the start.

Update

On May 16, 2019, the California Senate Appropriations Committee held SB-561 for the year. This likely blocks passage of the bill for this legislative term. There is a chance the bill could be re-introduced next year, during year two of the two-year legislative term.

While SB-561 may be dead for this legislative session, businesses subject to the CCPA should be aware that the enforcement regime will likely be a subject of continued debate in California as the law becomes effective next year. For now though, businesses can rest assured that the law will go into effect with the Attorney General-driven enforcement regime originally intended by the law's drafters. This should help ensure a more sensible, consumer-focused approach to enforcement, rather than the undirected feast for lawyers SB-561 would have unleashed.

A number of other proposed amendments to the CCPA are pending that, if passed, could affect businesses' obligations under the CCPA. Proposed changes to the definition of PI and an expansion of the public records exception could help practical implementation. The potential carve out of employees from the definition of "consumer" is an important open issue. Changes related to aggregate and deidentified information could also be significant. Our team is closely monitoring CCPA amendments and can help clients make sense of the fast-changing landscape.

akingump.com

Meredith C. Slawe
Partner
mslawe@akingump.com
Philadelphia
+1 215.965.1202

Michael J. Stortz
Partner
mstortz@akingump.com
San Francisco
+1 415.765.9508

Diana E. Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

Shelly A. Kim
Associate
shelly.kim@akingump.com
Los Angeles
+1 310.728.3333

Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

California's Governor Signals Potential Threat to Businesses' Use of Consumer Data – A New Data Dividend

February 19, 2019

Key Points

- In his State of the State address, Governor Newsom proposed a "Data Dividend" that would apparently entitle Californians to compensation for the use of their data. If passed, it would be the first measure of its kind in the country.
- Businesses that are collecting and sharing personal information of California residents and are subject to the far-reaching 2018 California Consumer Privacy Act (CCPA) would be safe to assume that legislators may seek to apply the proposed Data Dividend to their entities.

In his State of the State address last week, California's new governor Gavin Newsom announced that he has directed his team to develop a "proposal for a new Data Dividend for Californians" that would apparently entitle consumers to compensation for the use of their data. (State of the State (02/12/2019).) If adopted, the Data Dividend would be the first measure of its kind and could spur other states to pass copycat legislation.

The new proposal signals that California looks set to continue its push to restrict and regulate the use of consumer data in ways that are likely to affect companies far beyond the state's borders. Businesses that are collecting and sharing personal information of California residents and are subject to the far-reaching 2018 California Consumer Privacy Act (CCPA) would be safe to assume that legislators may seek to apply the proposed Data Dividend to their entities.

Echoing the language used by privacy activists, Governor Newsom asserted that consumers' data has "value" and "belongs" to consumers. He also lambasted "companies that make billions of dollars collecting, curating and monetizing our personal data" and stressed that those companies "have a duty to protect it."

Consumer advocates have been pushing ideas similar to the Data Dividend for some time. It appears that Governor Newsom's office may be working with consumer advocates on the new proposal. Shortly after the governor's speech, the CEO of

Contact

Natasha G. Kohne
Email
San Francisco
+1 415.765.9505

Dario J. Frommer
Email
Los Angeles
+1 213.254.1270

Hyongsoon Kim
Email
Irvine
+1 949.885.4218

Diana E. Schaffner
Email
San Francisco
+1 415.765.9507

Common Sense Media—a nonprofit that helped push passage of the CCPA—reportedly stated that his organization is working on draft legislation to implement the Data Dividend proposal. (TechCrunch(02/12/2019).)

The proposal also drew support from key legislative players active in the fight to pass the CCPA. State Senate Majority Leader Bob Hertzberg (D–Van Nuys), who helped shepherd passage of the CCPA, called the Data Dividend proposal the “most intriguing part” of the governor’s address. “This is the next frontier of the online data and privacy conversation, and I’m looking forward to hearing what a plan could entail,” Hertzberg said. (Hertzberg Press Release(02/12/2019).)

It is unclear how the governor plans to model the Data Dividend. Some observers have suggested enacting a tax on profits derived from the collection and sharing of California residents’ personal information and then distributing a share of the proceeds of that tax to all residents. Under California law, such a tax would require a two-thirds vote of the Legislature or approval by voters at a statewide election. Another model would base payment on the actual value of the data. It is an open question how the value would be calculated. One suggestion is to take the total number of California residents from whom a company collects data, divide the profit earned by that number, and then provide each California customer a portion of the result.

Now is the time for businesses to engage with the governor’s office concerning sensible and fair data usage regulation, and to begin to prepare for the same. While awaiting details on the proposal, businesses would do well to review their data collection practices to limit the collection of non-essential data and to ensure collected data is properly used and secured. Our team is closely monitoring the developing California privacy landscape and can assist clients in crafting a related strategy.

Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Summary of Sacramento AGO Public Forum on CCPA Regulations

February 7, 2019

The 2018 California Consumer Privacy Act (CCPA) requires the California Attorney General's Office (AGO) to promulgate regulations related to the CCPA by July 1, 2020. The AGO is holding seven public forums and accepting written comments regarding its CCPA rulemaking. We previously provided summaries of the San Francisco forum (link) and the Riverside and Los Angeles forums (link). The AGO held its fifth public forum in Sacramento on February 5, 2019.

- The Sacramento forum was among the best attended to date, with both industry advocates and consumer activists providing detailed comments. Consumer advocates participated to a greater degree than at prior forums.
- As with prior forums, the panel of AGO staff received public comments without directly responding. The AGO has set a deadline of March 8, 2019, to receive any written comments regarding its CCPA-related rulemaking. Information on how to submit comments by email or mail can be found here.
- Unlike prior forums, consumer advocates provided comments suggesting that they are already thinking through potential methods to test compliance with the CCPA. Consumer advocates asked AGO staff to require companies to include specific, detailed information in their consumer-facing privacy policies to assist consumer advocates in, among other things, better understanding how, and with whom, companies are sharing data.
- Comments shared at the Sacramento forum tracked issues raised at earlier forums, and key themes have emerged regarding public concerns with AGO rulemaking.
  - **Industry Concerns**. Key concerns raised by industry advocates include:
    - the need to ensure that employees are clearly excluded from the definition of "consumer;"
    - the potential risks posed to consumers by including "household" data in the definition of "personal information," including the possibility that members of a household may be able to request information about other members including in sensitive situations (*e.g.*, domestic abuse);

Contact

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
jmreed@akingump.com
Dallas
+1 214.969.2713

Dario J. Frommer
Partner
dfrommer@akingump.com
Los Angeles
+1 213.254.1270

Jo-Ellyn Sakowitz Klein
Senior Counsel
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Diana E. Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

- the benefits to consumers in enabling companies to offer a range of opt out options, rather than an all-or-nothing approach;
- the need to enable companies to tell consumers what types of specific pieces of information that they have on consumers, without having to risk privacy violations by providing the actual information back to consumers (*e.g.*, telling the consumer that they have his or her social security number without providing that number); and
- the need for the AGO to provide guidance on how companies should verify consumer requests, and the benefit to offering companies a safe harbor from liability if they comply with the AGO verification process.

– **Consumer Advocate Concerns**. Key concerns raised by consumer advocates include:

- that the fee that companies are permitted to charge to consumers who opt out of the sale of their data be truly reasonable and that the companies be required to submit reporting to support the reasonableness of their fees; and
- that companies be forced to adopt a streamlined and easily understood opt-out process, including by working toward a global opt-out option.

The AGO will hold the next public forum in Fresno on February 13, and the last public forum at Stanford is scheduled for March 5. Information about the upcoming hearings can be found here.

Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Summary of Riverside and Los Angeles AGO Public Forums on CCPA-Related Regulations

January 29, 2019

The 2018 California Consumer Privacy Act (CCPA) requires the California Attorney General's Office (AGO) to promulgate regulations related to the CCPA by July 1, 2020. The AGO is holding a series of public forums and accepting written comments regarding its CCPA rulemaking. A seventh public forum was recently added to the schedule and will be held at Stanford Law School on March 5, 2019.

The AGO held its third and fourth public forums in Riverside on January 24 and Los Angeles on January 25, respectively. The following is an overview of points of interest that arose from the most recent forums. A summary of the first AGO forum can be found here.

- As with the prior forums, panels of AGO staff received public comments without directly responding to them.
- Attendance ranged from approximately 30 people at the Riverside forum (with five people speaking) to more than 120 people at the Los Angeles forum (with 20 people speaking).
- At this point, AGO staff anticipate releasing CCPA-related regulations in the fall of 2019. A period of public comment with additional public forums will follow the release of the rules. Updates on CCPA rulemaking can be found here.
- The following points of interest, among others, were raised by speakers at the forums:

Personal Information

- Consumer advocates suggested that any data collected by a company should be subject to the CCPA's disclosure requirements, whether or not defined as personal information under the CCPA. They also asked that IP addresses alone (without additional information) and fingerprints be explicitly listed as unique identifiers.
- Industry advocates questioned whether recorded telephone calls constitute personal information under the CCPA.

Contact

Natasha G. Kohne
Email
San Francisco
+1 415.765.9505

Michelle Reed
Email
Washington, D.C.
+1 214.969.2713

Dario Frommer
Email
Los Angeles
+1 213.254.1270

Diana E. Schaffner
Email
San Francisco
+1 415.765.9507

Annie Banks
Email
Los Angeles
+1 310.229.1082

Brett Manisco
Email
Los Angeles
+1 310.229.1086

Nicholas Joseph Schuchert
Email
Irvine
+1 949.885.4223

- Attorney commentators suggested that identifiers should be separated into two categories—sensitive and nonsensitive information—with the former being the only type that is subject to the CCPA. They recommended that "sensitive" identifiers be limited to information that could expose a consumer to identity theft or other particularly sensitive data (e.g., medical information, fingerprints and other biometric information).

Nondiscrimination Clause

- Consumer advocates claimed that permitting fees to be charged in lieu of sharing data would disproportionately affect low-income consumers. One advocate recommended that companies that charge fees be required to publicly disclose revenue reporting at least annually to establish that the fees charged are directly related to the value of the data collected.
- Industry advocates emphasized the need for companies to be able to charge a reasonable fee and requested clarification on exactly how the AGO would determine the reasonableness of fees.

Employee Data

- Industry advocates and attorney commentators recommended that there be a specific exemption for employee data.

Need for Safe Harbors

- Industry advocates and attorney commentators noted the importance of establishing safe harbors from both AGO enforcement and private rights of action for companies that seek to comply with the CCPA.
- Industry advocates asked that template language, forms or mechanisms be provided to enable companies that adopt those templates to fall within a safe harbor (e.g., consumer request verifications, minimum security standards).
- Industry advocates asked that a process be created to enable companies to be certified as in compliance with CCPA requirements.

Opt-Out Logo/Process

- Consumer advocates asked that the opt-out process be limited to a short, one- to two-click system. They stressed that the logo should appear on each webpage of a company and not be limited to only a company's homepage.
- Industry advocates asked that businesses be required to post the opt-out logo on their homepages only. They also recommended that the opt-out logo follow a similar model to the existing self-regulatory program AdChoices.

Internal Inconsistencies/Clarification of Terms

- Industry advocates commented on how inconsistent and undefined terminology in the CCPA makes it difficult for businesses to determine the CCPA's applicability. They asked for clarification on the following points, among others:
  - That companies are not required to collect or store more information than they would otherwise in order to comply with the CCPA.
  - Whether the term "technically feasible" applies to a company's internal abilities or, instead, implies a duty to use third-party capabilities where a company does not have the internal capacity.
  - Whether carveouts for the definition of "selling" exist where ongoing business requires the transfer of personal information (e.g., with financial institutions) or where an entire business is sold (e.g., a merger).
  - What "household" means and how the inclusion of "household" data affects the scope of the CCPA.
- Attorney commentators recommended changes to sections of the CCPA that appear inconsistent with other sections. Among others, they highlighted the apparent discord between sections that empower consumers to request and receive (if their request is verified) specific pieces of information that a company collects about them, and those sections that obligate businesses to identify only the categories of information that they collect about consumers.

Aligning the CCPA with other Regulatory Regimes

- Industry advocates and attorney commentators recommended aligning the CCPA's regulatory regime with existing regimes to facilitate compliance, including the European Union's General Data Protection Regulation (GDPR). One advocate asked that companies that are able to establish their compliance with the GDPR be exempted from the obligations of the CCPA.

The AGO will hold three additional public forums over the coming months: February 5 in Sacramento, February 13 in Fresno and March 5 at Stanford. Information on those forums is available at this link.

Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Summary of First AGO Hearing re CCPA-Related Regulations

January 15, 2019

The 2018 California Consumer Privacy Act (CCPA) requires the California Attorney General's Office (AGO) to promulgate regulations related to the CCPA by July 1, 2020. The AGO is holding a series of six public forums and accepting written comments regarding its CCPA rulemaking. The AGO held its first public forum in San Francisco on January 8, 2019. The following is a high-level overview of points of interest:

- A panel of AGO staff received public comments. The AGO staff did not directly respond to comments or provide additional information regarding the AGO rulemaking process.
- Nearly 200 people attended the forum, although fewer than 20 people spoke. Contrary to expectations, there was not a significant activist presence. The short notice regarding the timing of the forum and post-holiday schedules may have contributed.
- The following points of interest, among others, were raised by speakers at the forum:
  - Speakers from both a business and consumer standpoint highlighted the need to identify a relevant standard of care with regard to businesses' conduct.
  - Speakers from both a business and consumer standpoint commented on the definition of personal information, recommending respectively that the definition be limited in various ways (removal of IP addresses, etc.) or that it remain as is.
  - Multiple speakers noted the adverse effect that the CCPA may have on businesses that support themselves through advertising. Speakers recommended that businesses be able to charge a reasonable fee to consumers who elect to use their services, but choose to opt out of the sale of their data.
  - Industry advocates raised concerns that the CCPA may incentivize or require companies to collect or retain more information on consumers than they would otherwise in order to comply with consumer requests. There was also concern that the CCPA could be interpreted to require companies to link currently anonymized data to specific consumers in order to respond to consumer requests.

Contact

Natasha G. Kohne
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
mreed@akingump.com
Dallas
+1 214.969.2713

Dario J. Frommer
dfrommer@akingump.com
Los Angeles
+1 213.254.1270

Elizabeth Marie Dulong Scott
edscott@akingump.com
Dallas
+1 214.969.4297

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Diana E. Schaffner
dschaffner@akingump.com
San Francisco
+1 415.765.9507

  - Industry advocates suggested that loyalty programs be explicitly exempted from certain provisions of the CCPA.
  - Industry advocates recommended that businesses be required to post the “Do Not Sell My Information” button on their homepages only to balance the burden.
  - Attorney commentators noted the importance of establishing safe harbors for companies that seek to comply with the CCPA, including companies that comply with consumer requests.
  - Attorney commentators recommended aligning the CCPA’s regulatory regime with existing regimes, including the European Union’s General Data Protection Regulation, to facilitate compliance.
- The AGO will hold additional public forums over the coming weeks. Information on those forums is available at this link.
- Industry advocates and activists continue to push for revisions to the CCPA in Sacramento even as the AGO pushes forward on its rulemaking mandate. At this time, we understand that bills aimed at exempting loyalty programs and permitting targeted advertising will be submitted this session.

Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

California Governor Signs Into Law Amendments to CCPA

September 27, 2018

This week, Governor Brown signed into law various amendments to the 2018 California Consumer Privacy Act (CCPA) passed by the California Legislature at the end of August. We discussed those amendments in detail in an earlier alert, posted here.

Key amendments to the CCPA signed into law include: (1) an extended deadline of July 1, 2020 for the California Attorney General's Office (AGO) to publish CCPA-related regulations; (2) a change in the date that the AGO can begin enforcing the CCPA to the earlier of either six months from the date the AGO publishes its CCPA-related regulations or July 1, 2020; (3) immediate application of the statewide preemption provision to avoid the potential effects of similar measures passed by California counties or cities; (4) revisions to the provision exempting information covered by the Gramm-Leach-Bliley Act (GLBA) or information covered by the California Financial Information Privacy Act (CFIPA); (5) a removal of the requirement that individuals wishing to bring a private right of action, must first notify and wait for a response from the California AGO before proceeding with their claim; and (6) clarification and expansion of exemptions relating to medical information.

There is a chance that further efforts to amend or modify the CCPA will take place when the California Legislature returns to session in December 2018. We will continue to provide updates on any such efforts.

Contact

Natasha G. Kohne
Email
San Francisco
+1 415.765.9505

Michelle A. Reed
Email
Dallas
+1 214.969.2713

Dario J. Frommer
Email
Los Angeles
+1 213.254.1270

Jo-Ellyn Sakowitz Klein
Email
Washington, D.C.
+1 202.887.4220

Diana E. Schaffner
Email
San Francisco
+1 415.765.9507

Elizabeth Marie Dulong Scott
Email
Dallas
+1 214.969.4297

Kelsey Stapler Morris
Email
Irvine
+1 949.885.4226

Tylor S. Dominguez
Practice Attorney
Email
San Francisco
+1 415.765.9543

Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

The Significance to Businesses of the California Legislature's Last-Minute Revisions to the 2018 California Consumer Privacy Act

September 7, 2018

Key Points

- The California Legislature passed SB 1121 to revise certain sections of the CCPA – the nation's strictest privacy protection statute which provides Californians with a right to learn what personal information certain businesses collect about them, to stop the sale of their personal information to third parties and to sue over data breaches if companies fail to adequately protect their information. The Governor has until September 30 to sign the bill.
- Key changes in SB 1121 include (1) extending the deadline for the AGO to publish CCPA-related regulations to July 1, 2020; (2) changing the date that the AGO can begin enforcing the CCPA to the earlier of either six months from the date that the AGO publishes its CCPA-related regulations or July 1, 2020; (3) making the statewide preemption provision effective immediately to avoid the potential effects of similar measures passed by counties or cities; (4) revising the provision exempting information covered by the GLBA; and (5) clarifying and expanding exemptions relating to medical information.
- The AGO, business groups and privacy activists may continue to press for additional revisions to the CCPA when the Legislature returns in December. It remains to be seen whether those efforts will take place or be successful and whether, and how, the CCPA may be amended further before it goes into force on January 1, 2020.

I. Introduction

The California Consumer Privacy Act (CCPA), the nation's broadest privacy protection statute, was enacted by the California Legislature in June 2018 as part of a last-minute deal to stop a proposed statewide ballot measure that could have ushered in an even stricter privacy law. We have written about the CCPA's passage in earlier alerts.

Contact

Natasha G. Kohne
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
mreed@akingump.com
Dallas
+1 214.969.2713

Dario J. Frommer
dfrommer@akingump.com
Los Angeles
+1 213.254.1270

Elizabeth Marie Dulong Scott
edscott@akingump.com
Dallas
+1 214.969.4297

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Tylor S. Dominguez
Practice Attorney
tdominguez@akingump.com
San Francisco
+1 415.765.9543

Diana E. Schaffner
dschaffner@akingump.com
San Francisco
+1 415.765.9507

Kelsey Stapler Morris
kmorris@akingump.com
Irvine
+1 949.885.4226

Sponsored by San Francisco real estate magnate Alastair Mctaggart and privacy advocacy groups, the ballot measure was strongly opposed by business groups and tech interests. Racing to beat a statutory deadline for the Mctaggart measure to be placed on the ballot, the Legislature hastily passed the CCPA in June while promising to introduce cleanup legislation after the summer recess.

Efforts to substantively revise the CCPA began nearly immediately after its passage, with the AGO (the chief enforcement agency for the CCPA), business groups, and privacy activists pressing for focused changes. Those efforts coalesced around Senate Bill 1121 (SB 1121) in August.

At the beginning of August, Sen. Bill Dodd (D-Napa) amended SB 1121 to correct various technical and drafting errors contained in the CCPA (AB 375 Chapter XX Statutes of 2018). After intense lobbying from business groups, banks, tech interests and California Attorney General Xavier Becerra, additional substantive amendments were adopted.

On August 22, Attorney General Becerra sent a letter to the co-authors of the CCPA outlining five key complaints that he had with the CCPA and asking for corresponding revisions to the CCPA. (X. Becerra Ltr. (Aug. 22, 2018.) Becerra opined that (1) businesses' and third parties' rights to seek Attorney General Office (AGO) opinions as to CCPA compliance issues would unduly burden the AGO and could lead to a conflict with its enforcement role; (2) the civil penalties included in the CCPA are likely unconstitutional, since they purport to amend and modify the California Unfair Competition Law's (Cal. Bus. and Prof. Code §§ et seq.) civil penalty provision as applied to CCPA violations; (3) consumers should not have to provide notice to the AGO prior to filing and pursuing their private rights of action related to data breaches; (4) the AGO needs additional time and resources to draft CCPA regulations; and (5) consumers should be able to bring a private right of action for any violation of the CCPA, not only for violations tied to a data breach.

Various business groups also lobbied for substantive changes to the CCPA, including (1) adding a defense to consumers' private rights of action where a business implemented an information security framework and documented its compliance with the same; (2) expanding the Gramm-Leech Bliley Act (GLBA) exemption; (3) expanding the exemption relating to medical information to cover business associates; (4) narrowing the definition of "personal information" to apply to information linked or linkable to a specific individual and excluding household information; (5) extending the compliance deadline to 12 months after the AGO enacts its final CCPA-related regulations; (6) ensuring that the statewide preemption goes into effect immediately; and (7) clarifying the definition of "consumer" to exclude employees, contractors and those involved in business-to-business interactions.

On August 31, SB 1121 passed both houses of the California Legislature. (SB 1121) The Governor now has until September 30 to sign it into law. We detail the key substantive changes included in SB 1121 below.

II. Overview of Changes to CCPA in SB 1121

The revisions included in SB 1121 fall into two categories: (1) technical or grammatical revisions adopted to fix drafting errors, revise internal inconsistencies, etc.; and

(2) substantive revisions that change the enforcement of the CCPA itself. This alert will focus on the latter category. SB 1121 makes the following important changes to the CCPA:

- **Extends Time for the AGO to Adopt Regulations (Section 1798.185(a)):** The deadline by which the AGO has to adopt CCPA-related regulations was extended by six months from January 1 to July 1, 2020. Attorney General Becerra requested additional time to draft and pass regulations in his August 22 letter.
- **Postpones Enforcement to the Earlier of Six Months from the Date the AGO Adopts its Regulations or July 1, 2020 (Section 1798.185(c))**: In a corresponding change to that noted above, SB 1121 also extends the date on which the AGO can begin enforcing the CCPA by the **earlier** of either six months from the date that the AGO adopts its final CCPA-related regulations or July 1, 2020. Should the AGO adopt its final regulations on July 1, 2020, it appears that businesses may be faced with having to comply with those regulations on the first day that they are promulgated.
- **Makes Statewide Preemption Provision Effective Immediately (Section 1798.199):** The revisions speed up enforcement of the statewide preemption provision to ensure that it takes effect immediately upon the Governor signing SB 1121 into law. This revision is a direct response to local privacy protection efforts, including a ballot initiative set to go before San Francisco voters this November. The San Francisco initiative could result in a "Privacy First Policy" to which the city, its contractors and its permit holders would have to adhere. The Policy is made up of 11 principles that effectively give city residents and certain guests greater control over how their personal information is collected, stored and shared. If the initiative is passed, the city government would have to consider the Policy when drafting and proposing a privacy ordinance containing more detailed rules. SB 1121 would undercut this local effort by ensuring that the CCPA's requirements preempt certain local laws statewide.
- **Removes Various Prerequisites to a Consumer Pursuing a Private Right of Action (Section 1798.150(b)(2), (3))**: SB 1121 removes Subsection 1798.150(b)(2) and (3) from the CCPA, which required consumers to notify the AGO within 30 days of filing a private right of action and then outlined the potential responses of the AGO to that notice. Some of the AGO responses under Subsection 1798.150(b)(2) appeared to limit consumers' ability to pursue their private rights of action if the AGO responded in a certain manner. In his August 22 letter, Attorney Gmaeneral Becerra complained of the onus that these provisions would put on the AGO and requested that they be eliminated. Should this revision be adopted, the only prerequisite a consumer will have prior to pursuing a private right of action is providing a business 30 days' notice of an alleged violation and a chance to cure.
- **Modifies the GLBA Exemption (Section 1798.145(e))**: The revised GLBA exemption eliminates the original requirement that it would apply only if the CCPA was in conflict with the GLBA (it would now apply even if there was no conflict). It also expands its protection to include personal information covered by the California Financial Information Privacy Act (Cal. Fin. Code § 4050 *et seq.*). However, SB 1121 adds language explicitly excluding Section 1798.150, which grants a consumer a private right of action, from the exemption. Business groups sought to revise this section in an effort to simplify compliance for companies that have already undertaken significant work and expense to ensure compliance with the

GLBA. It is not clear if that goal was entirely achieved, given the exclusion of the private right of action provision from the exemption.

- **Modifies Medical Information Exemptions to Expand Coverage (Section 1798.145(c))**: While the CCPA included an exemption aimed at limiting its applicability where privacy protection already existed under the California Confidentiality of Medical Information Act (CMIA) (Cal. Civ. Code Part § 56 et seq.) or the Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act of 2009 (together with their implementing regulations, HIPAA), the provision was poorly crafted and unduly narrow. SB 1121 overhauls this provision, making important improvements. "Medical information" as defined under and governed by CMIA is exempted. "Protected health information" as defined under HIPAA that is collected by a HIPAA-covered entity (such as a hospital or a health plan) or business associate (such as a vendor providing services for the hospital or a health plan that involve processing protected health information) is also exempted. "Providers of health care" as defined under CMIA and HIPAA-covered entities are exempted to the extent that they maintain patient information in the same manner as medical information or protected health information in accordance with CMIA and HIPAA, as applicable. Questions remain as to whether a company offering a mobile health app that collects information directly from individuals, without the involvement of a licensed health care professional, may take advantage of these exemptions. In addition, SB 1121 adds a new exemption for information collected as part of clinical trials, as long as the study was subject to certain human-research, subject-protection requirements.
- **Emphasizes the Broad Definition of Personal Information (Section 1798.140(o)(1))**: Revisions to the existing definition of "personal information" in SB 1121 emphasize that the term was intended to apply broadly by adding additional language stating that personal information includes the various examples listed in the CCPA if "it identifies, relates to, describes, is capable of being associated with or could be reasonably linked, directly or indirectly, with a particular consumer or household." This reemphasis contrasts with requests from business groups to narrow the definition to exclude household information and to limit the definition to information that is actually linkable to a specific individual.
- **Continues Requirement for Intentional Conduct to Trigger Highest Penalty (Section 1798.155(b))**: At least one of the various iterations of SB 1121 (as amended on August 24) would have amended the CCPA to permit the AGO to seek the highest civil penalty ($7,500) for any violation of the CCPA, intentional or otherwise. However, the final version of SB 1121 reimposed the original limits in the CCPA, including a $2,500 cap for the amount that the AGO can seek for general violations and a $7,500 cap for the amount that the AGO can seek for intentional violations.

III. Conclusion

The CCPA goes into effect on January 1, 2020. It remains to be seen whether the business community will continue to push for further CCPA amendments when the Legislature returns in December. These efforts may intensify as more businesses nationwide realize the CCPA's far-reaching scope. Indeed, some estimates suggest

that as many as 500,000 companies may fall under the statute. With Democrats expected to increase their large majorities in both houses of the Legislature in November, there may be little appetite to scale back CCPA consumer protections. Gov. Jerry Brown (D), who was instrumental in brokering the compromise to keep the Mctaggart measure off the ballot, is also set to leave office at the end of his current term. In addition, there is a likelihood that the CCPA may further embolden other state and local governments outside of California to adopt similar measures. Getting ahead of some of these privacy issues now, before they go into full force in California, may provide businesses with the best means of driving policy development in an area that is sure to affect business practices and costs for years to come.

Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

California Passes Landmark Consumer Privacy CCPA—What it Means for Businesses

July 9, 2018

Key Points

- California recently passed the landmark California Consumer Privacy Act that goes into effect in 2020, which grants California residents new privacy rights.
- The CCPA creates a private right of action for California residents and grants new enforcement power to the Attorney General with high damages recoverable.
- Hastily passed by the Legislature after only a week of debate, the CCPA contains provisions that require further clarification and that may prompt additional revisions.

I. Background

On June 28, 2018, Governor Brown signed into law one of the strictest and farthest-reaching consumer privacy laws in the country, the California Consumer Privacy Act of 2018 (the "CCPA"). (*See* AB-375.) The CCPA is a response to a growing concern that consumers need stronger means to protect their personal information in light of, among other things, recent data breaches and related privacy incidents that have affected millions of Americans (*e.g.*, Target, Equifax and Cambridge Analytica). The CCPA imposes a range of new requirements on businesses to further its goal of ensuring that consumers enjoy choice and transparency in the treatment of their personal information.

The hastily-passed CCPA is part of a deal brokered by the Legislature and Governor Brown to avert a costly fight over a proposed ballot initiative championed by privacy activists that would have put even more stringent measures before voters this November. Legislators and the proponents of the ballot initiative reached an agreement whereby the proponents would remove the initiative from the ballot if the CCPA was signed into law by the deadline for such removal.

The CCPA grants California residents the right: (1) to know what personal information is being collected about them; (2) to know whether their personal information is sold or otherwise disclosed and to whom; (3) to say no to the sale of their personal

Contact

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco/Abu Dhabi
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Dario J. Frommer
Partner
dfrommer@akingump.com
Los Angeles
+1 213.254.1270

Hyongsoon Kim
Partner
kimh@akingump.com
Irvine
+1 949.885.4218

Anthony T. Pierce
Partner
apierce@akingump.com
Washington, D.C.
+1 202.887.4411

Jo-Ellyn Sakowitz Klein
Senior Counsel
jsklein@akingump.com
Washington, D.C.
+1 202.887.4220

Diana E. Schaffner
Counsel
dschaffner@akingump.com
San Francisco
+1 415.765.9507

information; (4) to access their personal information and request deletion under certain circumstances; and (5) to receive equal service and price, even if they exercise their privacy rights.

It also creates a private right of action for California residents if their unencrypted or unredacted personal information is subject to certain security incidents as a result of a business's failure to implement reasonable security. Plaintiffs may seek the greater of their actual damages or set damages of between $100 and $750 per consumer per incident. The CCPA also empowers the Attorney General to pursue cases against businesses for damages of up to $7,500 per violation for intentional violations.

There is already talk about amending the CCPA to revise and clarify certain provisions. Businesses should carefully monitor future amendments to the law and the adoption of corresponding regulations, which will likely affect the CCPA's impact on day-to-day business.

II. Key Provisions

A. Whose Information is Regulated?

The CCPA places restrictions on certain businesses as a means of protecting consumers' personal information. Importantly, "consumer" for the purposes of the CCPA means any natural person who is a resident of California as "resident" is defined in tax provisions. Thus, under this broad definition, "consumer" includes: (1) every individual who is in California for other than a temporary or transitory purpose, and (2) every individual who is domiciled in California who is outside of California for a temporary or transitory purpose. Given this definition, the CCPA may arguably apply to covered entities that process even a single California resident's personal information no matter where that entity is located.

B. What Information is Regulated?

The CCPA expands the definition of "personal information" to include any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked with a particular consumer or household. This includes information like a consumer's name, postal address, social security number, education information, inferences drawn to create a profile about the consumer, consumer preferences, etc. The definition both encompasses and is broader than the definition of "personal information" used in California's data breach statute. For example, it includes biometric information (*e.g.*, imagery of the fingerprint, face, palm, etc.) collected without a consumer's knowledge.

Businesses may find that they collect information that may be considered sensitive under the CCPA even though other regulations or statutes may not classify it as such. The CCPA, moreover, contemplates that the Attorney General will adopt regulations to revise various subcomponents of the definition of personal information that, depending on the regulation adopted, could further expand the definition beyond its already broad terms. Because of the breadth of this definition, businesses in California and beyond that previously did not consider themselves to be maintaining regulated personal information may find that this is no longer the case once the CCPA takes effect, even if their data practices have not changed.

Notably, certain categories of information are apparently excluded from the reach of the Act, including: (1) publicly available information, which appears to generally mean information that is lawfully made available from government records; (2) deidentified information, which means information that cannot reasonably identify, relate to, describe, etc. a particular consumer provided the businesses takes certain safeguards (*e.g.*, protect against reidentification); and (3) aggregate consumer information, which means information that relates to a group or category of consumers from which individual consumer identities have been removed and that is not linked or reasonably linkable to a particular consumer or household. Information is not considered to be publicly available if it is used for a purpose other than the purpose for which it is maintained and made available in government records, or for which it is publicly maintained. The sections of the CCPA discussing deidentified and aggregate consumer information are somewhat opaque and businesses relying upon information in these categories should further explore the applicability of the CCPA to some uses of these types of information.

C. What Entities are Regulated?

The CCPA governs businesses (meaning for-profit entities) that (1) collect consumers' personal information, or on whose behalf such information is collected, and that determine the purposes and means of processing that information, and that (2) meet one of three criteria: (a) have annual gross revenue above $25 million; (b) alone or in combination annually buy, receive for commercial purposes, sell, etc. the personal information of 50,000 or more consumers, households, or devices; or (c) derive 50 percent or more of its annual revenue from selling consumers' personal information. Entities that either control or are controlled by such businesses are also covered by the Act. Commercial conduct that takes place wholly outside of California is not covered by the Act.

The CCPA also places restrictions on how a business should share consumers' personal information with its service providers as well as with third parties. "Service provider" means a for-profit entity that processes information on behalf of a business and to which the business discloses consumers' personal information for a business purpose pursuant to a written contract. Such contract must prohibit the service provider from, among other things, selling, retaining, using, or disclosing the personal information it receives for any commercial purpose other than the services specific in that contract. Any entity that is not a business or a service provider – as those terms are defined in the CCPA – is considered a third party. The CCPA treats service providers and third parties differently in a number of ways, including that it: (1) limits a business's liability for service provider misconduct if certain conditions are met (*see infra* Section L), but does not offer the same protection when a business sells, share, or discloses personal information to third parties; and (2) limits a business's ability to sell, share, or disclose consumers' personal information to third parties without providing consumers prior notice and the option to opt out of the sale (*see infra* Sections D and G(2)), but does not place the same requirements on sharing information with service providers.

The collection and use of consumers' personal information by California state and local government entities is **not** covered by the Act. This omission has been soundly criticized by privacy advocates and marks a departure from other privacy-focused

statutes. There is already discussion of passing additional legislation during the next session to apply similar controls to California government entities.

D. What Notices and Disclosures Must be Provided to Consumers?

Businesses are required to provide consumers certain notices and disclosures in materials posted on their websites and through other means. This includes notice of: (1) at or before the point of collection, the categories of personal information the business collects about consumers and the purposes for which they will be used; (2) consumers' rights to request that the business delete their personal information; and (3) if the business intends to sell personal information to third parties, consumers' right to opt out from that sale. In addition, businesses have to include in their online privacy policies, in California-specific descriptions of rights online, or in their websites generally information to help consumers understand and exercise their rights, including a description of consumers' rights under the CCPA (*e.g.*, to request information on what personal information has been collected, sold or disclosed about them, to have such information deleted, or to opt out of the sale of information, etc.), how to submit related requests, and lists of the categories of personal information the business has collected, sold and disclosed about consumers generally in the prior 12-month period.

E. What Information Must be Provided to Consumers Upon Request?

Consumers have a right to request and receive (if they provide a verifiable request) the following information from businesses: (1) the categories and specific pieces of personal information the business has collected about the consumer; (2) the categories of sources from which the personal information is collected; (3) the business purposes for which the personal information is collected; (4) the categories of third parties with whom the business shares consumers' personal information; and (5) the categories of personal information that the business sold or disclosed about the consumer for a business purpose. Subject to certain potential extensions, businesses have to respond to consumers' requests within 45 days. The response must cover the 12-month period prior to the consumer's request and include the required information in a transferrable format if provided electronically. In effect, businesses should be prepared operationally by December 31, 2019 (the day before the CCPA takes effect) to practically respond to consumer requests, which requires tracking the collection of personal information, as well as tracking the sources of information and any third parties that receive the information.

The CCPA does not specify whether businesses will be expected to provide information for the 12 months preceding the date the Act takes effect (January 1, 2020), or if the requirement to track and provide the various categories of covered information begins as of that date. Until this point is clarified, businesses may need to be prepared operationally as of January 1, 2019 (12 months before the CCPA takes effect) to track the various categories of information that they may need to practically respond to consumer requests as of January 1, 2020. This is yet another issue that should be clarified before the CCPA goes into force.

There are certain qualifiers that suggest the actual information that need be provided to consumers under the CCPA is more limited than may appear upon first reading. Businesses are only required to provide the "categories" of sources from which personal information is collected or the categories of third parties with which personal information is shared. It appears business could respond to consumer requests for information on these points with a general list, rather than with information specific to the particular consumer making the request. An exception to this is the requirement that businesses inform consumers of both the categories and specific pieces of personal information it has collected about the requesting consumer. Even then, the CCPA is not clear what is meant by "specific pieces" of information. It may be sufficient for a businesses to inform the consumer which of its general list of categories of personal information it actually collected about the consumer, rather than provide the consumer all of the personal information collected about the consumer in the prior 12-month period.

F. Are There Limits on a Business's Obligation to Respond to Requests?

The CCPA includes a few protections for businesses in the form of limitations on the number of responses that have to be provided to consumers within a single year (two responses per year only are required), potential extensions of the time to respond to consumer requests (can be extended by an additional 90 days), and the possibility of refusing to CCPA on requests or charging a reasonable fee where requests are unfounded or excessive. With regard to the last point, businesses bear the burden of demonstrating that the requests were unfounded or excessive should they refuse to respond or charge a fee for this reason.

G. What Rights Does a Consumer Have Beyond Requesting Information?

1. The Right to Delete Personal Information

A consumer has a right to request that a business delete his or her personal information from its records and direct any service providers to do the same. Businesses must comply with verifiable consumer requests. The CCPA does not specify how information is to be deleted or provide a specific means of testing the proper outcome.

There are nine exemptions to the deletion requirement that permit a business to avoid deleting a consumer's personal information, including: (1) to complete the transaction or service for which the information was collected; (2) to detect security incidents, protect against malicious, deceptive/fraudulent, or illegal activity, or prosecute those responsible for that activity; (3) to debug or identify errors; (4) to exercise free speech; (5) to comply with certain sections of the California Electronic Communications Privacy Act; (6) to engage in certain types of research if the consumer has provided informed consent; (7) to enable solely internal uses that are reasonably aligned with the consumer's expectations (based on his or her relationship with the business); (8) to comply with legal obligations; or (9) to use internally in a lawful manner consistent with the context in which the information was provided. The breadth of these exemptions suggests the right to delete may be fairly limited in certain circumstances, although even a limited deletion right could present material challenges for businesses.

Although akin to the GDPR's "right to erasure," California's "right to delete" appears to be narrower in application. Under the GDPR, personal data must be erased immediately as long as the data are no longer needed for their original processing purpose, the impacted person has withdrawn his or her consent and there is no other reason for justification, the impacted person has objected and there is no preferential justified reason for the processing, or erasure is required to fulfill a statutory obligation under EU law or the right of the Member States. The GDPR, as with the Act, does not specify how data should be erased in individual cases. The key result is that it is no longer possible to see the data without disproportionate expense.

2. The Right to Opt Out of the Sale of Personal Information

Consumers must be provided the option to opt out of the sale of their personal information to third parties at any time. Once consumers have opted out, their information cannot be sold unless they later provide authorization. The CCPA restricts businesses from requesting reauthorization from a consumer for 12 months after the consumer opts out. The right to opt out only covers the sale of personal information to third parties.

To facilitate the opt-out process, businesses are required to provide a "Do Not Sell My Personal Information" link on their websites' homepages that link to a form enabling consumers to opt out of the sale of their personal information and providing related information. Consumers must be permitted to opt out of the sale of their data without creating an account with the business. The CCPA also contemplates the eventual development of a standard "Do Not Sell My Personal Information" link that will have a similar appearance and function across different entities. Development of that common icon will take place sometime in the future.

There are special authorization or "opt-in" rights provided to minors. Businesses may not sell the personal information of a consumer if they have "actual knowledge" that the consumer is younger than 16 and have not received specific authorization. Children age 13 to 16 can provide authorization for the sale of their own personal information, while only the guardians of children under 13 can provide such authorization. Businesses that "willfully disregard" a child's age will be considered to have "actual knowledge" of the child's age. The CCPA does not provide guidance on what constitutes "willful disregard" in this context.

The CCPA does not appear to regulate the access that companies provide to advertisers regarding targeted individuals where that access is granted without providing specific information from individual users. In this manner, some large companies that maintain they do not sell consumers' data (*e.g.*, Facebook) appear to fall outside the reach of those portions of the CCPA that govern sale-specific issues. It remains to be seen if or how the Attorney General may seek to apply the CCPA to such a context. Unless the CCPA were revised to clarify its applicable to this use of consumer information, or the Attorney General were to issue a regulation or guidance related to the same, it is not clear how consumers would opt out of having their information shared with third-party advertisers.

H. Are There Limits Placed on the Collection of Information?

The CCPA does not appear to place limits on businesses' ability to collect personal information on consumers, although, as noted above, it does require that businesses provide consumers certain notices and disclosures related to the collection of that information. In this way the CCPA may be a continuation of the status quo with some additional disclosure protections layered on top of the existing data-collection framework. The GDPR, in contrast, requires that companies obtain a data subject's permission before they collect data on that data subject.

I. Can a Business Treat Consumers Differently if They Exercise Their Rights?

Businesses are generally prohibited from discriminating against consumers who choose to exercise their rights under the Act, including by opting out of the sale or disclosure of their personal information to third parties. This includes through actions like increasing fees, slowing services, etc. Businesses *are* allowed to differentiate among consumers in terms of prices charged or level of services provided if the difference is reasonably related to the value provided to the consumer by the consumer's data. In addition, businesses may offer financial incentives for the collection, sale, or deletion of consumers' data, if the business provides notice of the incentive to consumers.

Some commentators have remarked that by permitting differentiation among consumers linked to the value provided by the consumer's data, the CCPA effectively permits businesses to charge more or offer lesser services to consumers who elect to exercise their rights to greater privacy. A few lawmakers expressed concern with the CCPA for this reason suggesting it was setting California on a path toward a "pay-for-privacy" regime. (Sacramento Bee (07/05/18), quoting Sen. Hannah Beth-Jackson.) Other commentators have suggested that this permits businesses to effectively market services where consumers would prefer to provide information rather than pay for a service.

J. Are Businesses Required to Implement Certain Security Measures?

To help minimize the risk of a consumer action, businesses must implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information that is to protected. What constitutes "reasonable security" is not discussed in the Act. Indeed, California has not codified what is meant by "reasonable security" although it requires businesses that own, license or maintain personal information about California residents to provide reasonable security for that information both in the CCPA and in other state privacy-related statutes. (*See* Cal. Civ. Code § 1798.81.5(a).)

In the absence of codified standards, industry best practices suggest ensuring security policies and practices are in line with one of the several internationally-recognized information security frameworks. These include, among others, the Center for Internet Security's ("CIS") 20 Critical Security Controls, the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework and related NIST standards (*e.g.*,

NIST SP 800-171), or the International Standards Organization's (ISO) various series governing information security management (*e.g.*, ISO/IEC 27001). Adoption of these or equivalent information security frameworks and incorporation of the same into internal policies and practices would likely assist a business in establishing its good-faith effort to implement and maintain reasonable security measures. Guidance from the California Attorney General's Office in its 2016 Data Breach Report, suggests that businesses that abide by CIS's Critical Security Controls would likely meet the reasonable security requirement. (*See* CA 2016 Data Breach Report, p. v.) The guidance does not rule out the ability for businesses to follow equivalent, industry-recognized information security frameworks to achieve the same goal.

K. Are there Limits on the Re-Sale of Personal Information?

A third party that purchases consumers' personal information from a business cannot in turn sell that information to another without providing the consumers explicit notice and the opportunity to opt out. The CCPA does not specify how that notice or opt-out option should be provided to consumers. Once the CCPA goes into force, businesses may want to take precautionary measures like automatically providing options to opt out of the sale of personal information prior to any collection to easily enable the sale of such information down the line, segregating all personal information from California residents and not selling the same, or seeking guidance from the Attorney General as to how best to comply prior to re-sale.

L. Are there Protections Against Liability for Service Provider Misconduct?

Businesses that share consumers' personal information are not liable under the CCPA for service provider misconduct, if, at the time the business discloses the personal information, the business did not have actual knowledge, or reason to believe, that the service provider intended to violate the Act. Businesses also must have complied with the requirements of the CCPA in terms of having a proper written contract in place that prohibits the service provider from retaining, using or disclosing the personal information for any purpose other than for performing the services specified in the contract for the business that provided the personal information, or as otherwise permitted by the Act. A service provider is similarly free of liability for the obligations of a business from which it receives personal information.

To help preserve this limit on liability, businesses should ensure that their contracts with service providers include specific provisions prohibiting the service providers from using any consumers' personal information provided in connection with the contract aside from carrying out the purposes of the contract or related administrative tasks. Businesses should also require service providers to represent that they are aware of and abide by the terms of the Act, as well as related regulations. Representations of this kind could assist businesses in establishing that they did not have actual knowledge or a reasonable basis for believing the service provider was planning to violate the CCPA at the time personal information was transferred to the service provider. It may be wise to have businesses reaffirm their awareness of and compliance with the CCPA and related regulations until both are fully adopted and in force.

M. Can Consumers Waive Applicability of Act?

The CCPA explicitly empowers courts to deem unenforceable any provision of a contract or agreement that purports to waive or limit in any way a consumer's rights under its terms. This includes any right to a remedy or specific means of enforcement. A consumer can still opt not to request information from a business or decline to take other actions under the Act.

III. Enforcement and Penalties

The CCPA contemplates two main avenues for enforcement of and recovery under the CCPA–private consumer rights of action (whether through individual or class actions), and actions brought by the Attorney General in the public interest. Both pose risks to businesses. Businesses also have the ability to seek guidance from the Attorney General on how to comply with the Act.

A. Consumer's Private Right of Action

Any consumer whosenonencrypted ornonredacted personal information is subject to an unauthorized access andexfiltration, theft or disclosure as a result of a business's failure to implement and maintain reasonable security procedures and practices may institute a private right of action for any of the following: (1) the greater of either the consumer's actual damages or damages in an amount not less than $100 and not greater than $750 per consumer per incident;[1] (2) injunctive or declaratory relief; or (3) any other relief a court deems proper. A consumer is apparently not required to establish actual harm to pursue a private right of action.

A consumer may only bring a private right of action where he or she meets two additional requirements. First, prior to initiating any action, the consumer must provide the business 30 days' written notice identifying the specific provisions of the CCPA he or she alleges have been or are being violated. If the business cures the issue within 30 days, no consumer action is permitted. If not, the consumer may proceed with filing. If a business informs a consumer that an issue is cured and it is not, that consumer is entitled to initiate an action against the business that seeks damages for each breach of the written representation as well as any other violation of the CCPA that postdates receipt of the written representation. Consumers seeking to recover only their actual, monetary damages do not have to provide such notice and may proceed directly to filing and notifying the Attorney General.

Second, the consumer must notify the Attorney General within 30 days that the action has been filed. The Attorney General then has 30 days to take one of the following three actions: (1) notify the consumer of its intention to prosecute the action; (2) refrain from acting for 30 days, thus permitting the consumer to proceed; or (3) notify the consumer that he or she shall not proceed with the action. With regard to the first option, the Attorney General has six months in which to initiate its prosecution. If the

[1] In assessing what statutory damages may be imposed, the CCPA directs courts to consider factors including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

Attorney General fails to CCPA within that period, the consumer may proceed with his or her action.

B. Attorney General Enforcement

The Attorney General has the sole right to pursue civil penalties against businesses in violation of the CCPA through a civil action in the public's name. Businesses are in violation of the CCPA if they do not cure any alleged violation within 30 days of notification of the same. Penalties of up to $2,500 for general violations could be imposed, while penalties for intentional violations could be up to $7,500 for each violation. The term "violation" is not defined in the CCPA and it is not clear how penalties might be imposed. The private right of action, in contrast, limits the collection of its set damages to a per consumer per incident basis.

The CCPA created a new Consumer Privacy Fund (the "Fund") within California's General Fund into which 20 percent of the funds recovered will be deposited, while the remaining 80 percent will go to the jurisdiction that brought the action. The Fund is intended to offset any costs incurred by state courts or the Attorney General in bringing cases connected with the Act.

C. Ability to Seek Attorney General Guidance

Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the Act. This provision may be of particular importance with regard to gaining clarity on some of the more opaque sections of the CCPA before it goes into force in 2020. This may be a particularly useful tool in some cases for groups of businesses facing the same issue that may wish to submit a joint request for an opinion on as both a means of gaining guidance and as an advocacy tool to highlight a particularly unclear section of the CCPA, although the CCPA remains silent concerning how long the Attorney General has to respond to opinion requests.

IV. Conclusion and Proactive Steps to Take Now

- Passage of the CCPA marks a watershed moment for privacy law in the United States. California's size, population and the predominance of the state's technology sector ensure that the Act's requirements will have consequences far beyond the state's borders. The best way to respond to these developing requirements is to implement strong security and privacy measures and to periodically review the same. We recommend that businesses take the following steps now to begin to protect themselves from the likely effects of the Act.
- Determine if you collect, maintain or hold California residents' personal information or if an entity you control or that controls you does so. Understanding if the CCPA actually applies to you is the first step in defense.
- If you do not already have someone in your organization responsible for following and addressing requirements relating to personal information, consider establishing a role that makes sense for your organization.
- Engage in a data mapping activity that provides information on who in your organization collects, uses and shares what personal information for what purposes, and that tells you where and how that data is stored and accessed. This

effort will assist in compliance with a range of regulatory regimes (*e.g.*, California, GDPR, etc.).

- Incorporate an internationally-recognized framework like the CIS's 20 Critical Security Controls, NIST's Cybersecurity Framework, the ISO/IEC series 27001, or an equivalent in your information security policies and practices to help ensure your company is employing reasonable security measures. Consider implementing other industry-specific best practices that may meet special needs of your business.
- Take steps now to encrypt or redact consumers' personal information when collected, stored, and transmitted as a means of helping to mitigate some of the potential litigation burden that could arise if unencrypted or unredacted personal information is the affected by a security incident.
- Draft strong written contracts with service providers and vendors with which you share consumers' personal information to ensure those contracts meet the requirements of the CCPA and will afford you the strongest protection from liability.
- Consider requesting guidance from the Attorney General before the CCPA goes into effect regarding its applicability if unclear. Official guidance could protect against consumer litigation, particularly on ambiguous sections of the Act.
- Begin considering whether it is feasible to segregate personal information you collect, maintain or hold on California consumers to enable eventual easy compliance with the Act. Consider taking similar steps to those your organization may already have taken to comply with other regulatory regimes like the GDPR or Massachusetts's Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00).