Morgan Lewis

Agenda

- Introduction
  - Amendments, draft regulations, ballot initiative, and deadlines
- Amendments, including:
  - The new one-year exemption for employee data
  - The new one-year exemption for B2B communications
- Selected draft regulations
  - Requests to know, delete and opt-out; verifying requests; and notice of financial incentive
  - Businesses with data about 4M or more consumers; service providers; training; and record keeping
- Enforcement/Security Breach Private Right of Action
- Preparing for January 1 and July 1

INTRODUCTION

The CCPA Is a Game-Changer

- California has long been a laboratory for innovative approaches to privacy and security regulation
  - But the landmark California Consumer Privacy Act is by far the most sweeping, game-changing privacy law that the state has enacted
- There have been a number of significant new developments with regard to the CCPA in the past month alone, and we'll bring you up to date
- As the regulatory picture becomes clearer, companies now have a better sense of what they need to do to be ready for January 1, 2020 (the effective date) and July 1 (the anticipated enforcement date)

CCPA Timeline

- June 28, 2018: CCPA is signed into law by Governor Jerry Brown
- September 23, 2018: SB 1121 amends the CCPA, most notably:
  - Extending deadline for issuance of regulations to July 1, 2020
  - Enforcement will commence six months after publication of final regulations or July 1, 2020, whichever is sooner
- September 25, 2019: Alastair Mactaggart announces the filing of a new California ballot initiative intended to enhance CCPA privacy protections

CCPA Timeline (cont.)

- October 10, 2019: AG's office issues proposed CCPA regulations
  - Regs primarily address consumer privacy rights and do not address subsequent CCPA amendments, private right of action for security breaches, or enforcement
- October 11, 2019: Governor Gavin Newsom signs into law five CCPA amendment bills, which include new exceptions for employee and B2B transaction data

What Lies Ahead

- The AG's office will conduct four public hearings on the CCPA draft regulations
  - December 2 in Sacramento
  - December 3 in Los Angeles
  - December 4 in San Francisco
  - December 5 in Fresno
- December 6, 2019: Deadline for submitting written comments on the draft regulations
- Any revision to the proposed regulations will be subject to an additional 15-day comment period

What Lies Ahead (cont.)

- Following the comment period, the AG will submit the final text of the regulations, along with a final Statement of Reasons responding to every comment submitted, to the Office of Administrative Law (OAL)
- OAL has 30 working days to review the regulations and then, if approved, they go into effect
- Upshot: July 1, 2020 will be the CCPA enforcement date because that will almost certainly come sooner than 6 months after the date of final regulations

Businesses Subject to the CCPA

- A "business" subject to the CCPA must be a for-profit organization or legal entity that
  - Does business in California
  - Collects consumers' personal information, either directly or through a third party on its behalf
    - "Collects" is broadly defined to include "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means"
  - Either alone, or jointly with others, determines the purposes and means of processing of consumers' personal information
    - Resembles GDPR's "data controller" concept
- Business includes an entity that controls or is controlled by a business **if** it shares common branding with the business

Additional Criteria for Businesses

- A business must also satisfy one of three thresholds:
  (1) Annual gross revenues in excess of $25 million (does not appear to be limited to California revenues);
  (2) Annually buys, receives, sells or shares the personal information of 50,000 or more consumers, households, or devices, alone or in combination; **or**
  (3) Derives 50% or more of its annual revenue from selling consumers' personal information.
- Applies to brick-and-mortar businesses, not just the collection of personal information electronically or over the internet
- Does not apply to non-profits

CCPA Does Not Apply To ....

- Medical information and entities subject to HIPAA or the California Confidentiality of Medical Information Act
- Personal information subject to the Gramm-Leach-Bliley (GLBA) or the California Financial Privacy Act
  - Applicability to insurers subject to California's Insurance Information and Privacy Protection Act is unclear (AB 981 failed to pass)
- Sale of personal information to or from a consumer reporting agency
- Personal information information subject to the federal Driver's Privacy Protection Act
- Employee data (AB 25)
- B2B transaction data (AB 1355)
- Vehicle information (AB 1146)

AMENDMENTS

Employee Data (AB 25): One-Year Exemption

- Exempts certain personal information collected from job applicants, employees, owners, directors, staff, officers, and contractors of a business from most requirements of the CCPA for one year, until January 1, 2021.

Employee Data (AB 25): One-Year Exemption (cont.)

- Information includes: (1) personal information collected about a person as a job applicant, employee, owner, director, officer, medical staff member, or contractor of that business; (2) personal information collected and used solely for the purpose of maintaining emergency contact information; and (3) personal information collected and used solely to administer benefits to an individual's dependents.
- This information is exempted from most of the CCPA's requirements, including the requirements that businesses offer consumers opt-out, access, and deletion rights. But, businesses must provide these individuals with a CCPA-compliant privacy notice.
- These individuals also have the right to bring a private civil action for data breaches.
- CA to consider more comprehensive employee privacy legislation before the employee exemptions expire on January 1, 2021.

Employee Data: Privacy Notice

- AB 25 requires that employees receive a "notice at collection."
- AG's proposed regulations released on October 10 provide that a "notice at collection" must:
  - Use plain, straightforward language and avoid technical or legal jargon.
  - Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.
  - List the categories of personal information to be collected.
  - For each category of personal information, the business or commercial purpose(s) for which it will be used.
  - If the business sells personal information, the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info."
  - A link to the business's privacy policy, or in the case of offline notices, the web address of the business's privacy policy

AB 25: Also Addresses Consumer Requests

- AB 25 also adds language regarding consumer requests:
  - A business "may require authentication of the consumer that is reasonable in light of the nature of the personal information requested," without requiring "the consumer to create an account with the business in order to make a verifiable consumer request."
  - However, "[i]f the consumer maintains an account with the business, the business may require the consumer to submit the request through that account."

Definitions of "Personal Information" and "Publicly Available Information" (AB 874)

- Clarifies the definitions of "personal information" and "publicly available information."
- Removes from the definition of "publicly available information" a carve-out for information "used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained."
- Substantially broadens the scope of information considered publicly available, such that "publicly available information" is now defined as information that "is lawfully made available from federal, state, or local government records."
- Clarifies that "personal information" includes information "that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."
- Reasonableness standard now applies both to information that "is **reasonably capable of being associated** with . . . a particular consumer or household" and to information that "could **reasonably be linked**, directly or indirectly, with a particular consumer or household."

Vehicle Information (AB 1146)

- Exempts from the definition of "personal information" vehicle information and vehicle ownership information that is retained or shared by dealers and vehicle manufacturers for purposes of a warranty repair or recall-related vehicle repair. The dealer or vehicle manufacturer receiving such information cannot sell, share, or use that information for any other purpose.
- The amendment also adds definitions for "vehicle information" and "ownership information."
- "Vehicle information" includes "the vehicle information number, make, model, year, and odometer reading."
- "Ownership information" is defined as "the name or names of the registered owner or owners and the contact information for the owner or owners."

Business-To-Business Communications (AB 1355): One-Year Exemption

- Creates a one-year exemption for certain business-to-business (B2B) communications or transactions.
- Similar to the employee personal information exemption, this exemption sunsets on January 1, 2021, with the expectation that the California legislature will determine a more permanent approach next year.
- Personal information about an employee, owner, director, officer, or contractor of a business or government agency collected by a business within the context of the business conducting due diligence or providing or receiving a product or service is exempt from certain CCPA requirements.
- Amendment clarifies that a business is not required to "collect personal information that it would not otherwise collect in the ordinary course of its business" or to "retain personal information for longer than it would otherwise retain such information in the ordinary course of its business."

AB 1355: Other Amendments

- FCRA Exemption: Broadens the existing Fair Credit Reporting Act (FCRA) exemption, clarifying that the exemption applies to any FCRA "activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living."
- Additional PI Exclusion: Clarifies that "deidentified or aggregate consumer information" is excluded from the definition of "personal information."
- Private Right of Action: Amends the CCPA private right of action to apply only to "personal information" that is "nonencrypted and nonredacted," narrowing the scope of the consumer private right of action.
- Previously, the consumer private right of action applied to "nonencrypted or nonredacted" personal information that "is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."

PROPOSED REGULATIONS

Morgan Lewis

Selected Draft Regulations

- Requests to Know, Delete, and Opt-Out
- Verifying Requests
- Notice of Financial Incentive
- Training and Record-Keeping
- Service providers
- Businesses with Data About 4M or More Consumers

Requests to Know, Delete, and Opt-Out

- Draft regulations address notices required under the CCPA, including:
  - Notice at collection of PI
  - Notice of right to opt-out of sale of PI
  - Privacy policy requirements
- Notices and policies: easy to read and understandable to average consumer
  - Plain, straightforward language and avoid technical or legal jargon
  - Format that draws attention to the notice and makes it readable, even on small screens
  - Language that the business uses in the ordinary course
  - Accessible to consumers with disabilities (access in alternative formats)
  - Each type of notice also has additional, specific requirements

Responding to Requests to Know or Delete—Requirements Include:

- Confirm receipt of request within 10 days and explain how it will be processed
- Respond within 45 days, or 90 days if provide notice explaining why delayed
- Regulations address whether and how to respond to requests for specific information or categories of information about the consumer
  - Reasonable security measures must be used to transmit the PI to the consumer
  - May provide through the consumer's PW protected account
  - Must provide individualized responses, not just refer to generalized practices, providing details regarding each category of information
- Disclosure prohibited if it would create an unreasonable risk
- Disclosure prohibited for certain types of sensitive information, including SSNs, driver's license, financial account info, health insurance or medical ID number, etc.
- Denial of requests to know or delete must be explained

Responding to Requests to Know or Delete – Requirements Include:

- For requests to delete -- if the requester's identity cannot be verified, the request may be denied and instead treated as an opt-out of sale
- Options to comply with a request to delete (inform consumer of method used):
  - Permanently and completely erase PI, except for archived and back-up systems;
  - De-identify PI; or
  - Aggregate the PI
- OK to delay compliance for data stored on archived or back-up systems until data is next accessed or used
- Inform consumer that request to delete itself will be retained
- Consumer may be given option to delete all or select portions of PI, with option to delete all data the most prominent, with two-step confirmation process

Requests to Opt-Out – Requirements Include:

- Two or more methods for submission of requests:
  - "Do Not Sell My Personal Information" or "Do Not Sell My Info" link for websites or apps
  - Toll-free number, email address, in-person submission of a form, mailed form, etc.
- Consider methods regularly used for interacting with the consumer
- Browser plug-ins and privacy settings to be treated as a valid opt-out request for that browser or device or, if known, for the consumer
- May present choice to opt-out for all or certain categories, so long as global option is more prominent
- Respond ASAP, but no longer than 15 days from receipt
- Notify third parties to whom PI was sold within the last 90 days, and inform the consumer
- Authorized agent of the consumer may submit the request
- Request need not be verifiable; may be denied if believed to be fraudulent and explain

Verifying Requests

- Regulations establish rules and procedures for verifying the identity of consumers making requests to know and requests to delete
- Business must establish, document, and comply with reasonable verification method
  - Method must take into consideration:
    - The sensitivity of information
    - The risk of harm to the consumer if there is unauthorized access or deletion
- If consumers have a PW-protected account, the business may use the existing PW authentication processes if it uses reasonable security methods to detect fraud

Verifying Requests (cont.)

- For non-accountholders – verification standards vary by type of request
  - Requests for disclosure of categories of PI must be verified to a reasonable degree of certainty
    - Match at least two data points provided by the consumer to information maintained by the business
  - Requests for specific pieces of PI must be verified to a reasonably high degree of certainty
    - Match at least three pieces of PI provided by the consumer with info maintained by the business and a signed declaration under penalty of perjury
  - Requests to delete must be verified by a standard that varies depending upon the sensitivity of the PI and the risk of harm to the consumer if unauthorized deletion

Special Rules for Minors

- Business cannot sell PI of minors under age 16, unless they have opted in to the sale of their PI
  - Regulations establish rules and procedures to obtain affirmative authorization for the sale of PI of minors under age 16
    - Two-step process: consumer clearly requests opt-in and confirms opt-in choice
- If the minor is under age 13 years, a parent or guardian must opt-in on behalf of the child
  - Regulations address methods by which a business can verify that the person affirmatively authorizing the sale of PI of a child under 13 is the parent or guardian of the child

Notice of Financial Incentive

- Purpose: Allow consumers to make an informed decision about what financial incentives or price or service differences are offered in exchange for the retention or sale of PI

Notice of Financial Incentive (cont.)

- Notice must include:
  - Succinct summary of the financial incentive or price/service difference offered
  - Material terms, including categories of PI implicated
  - How the consumer can opt-in
  - Explanation regarding the right to withdraw at any time and how to exercise the right to withdraw
  - Explanation of why the financial incentive or price/service difference is permissible:
    - Good-faith estimate of the value of the consumer's data that forms the basis for the financial incentive or price/service difference; and
    - Method used by the business to calculate the value of the consumer data.

Training

- CCPA requires regulated businesses to have training for "individuals responsible for **[1]** handling consumer inquiries about the business's privacy practices or **[2]** the business's compliance."
- Regulation broader than CCPA:
  - Clarifies training applies to "**all the requirements** in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations."
- Implement and document training.

[Cal. Civil Code § 1798.130(a)(6), CCPA Regulation § 999.317(a)]

Record-Keeping

- New proposed requirements
- Businesses to maintain records of CCPA consumer requests for "**at least 24 months.**"
- May be maintained in a ticket or log format
  - Must include the date of the request, the nature of the request, the manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of any request that is denied.
- Record-keeping information "shall not be used for any other purpose."

Service Providers

- "Service Provider"
  - Company or legal entity processing information on behalf of a business
  - Business that discloses a consumer's personal information for a business purpose pursuant to a written contract
    - Contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business
    - Or as otherwise permitted under the CCPA
      - including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

Service Providers (cont.)

- Under proposed regulations, a consumer may make certain requests directly to a service provider, and the service provider can either comply with the request or deny it and inform the consumer to submit the request directly to the business
- Service provider shall not use personal information received from a consumer or a business it services for the purpose of providing services to another person or entity
  - Except to combine personal information to detect data security incidents or protect against fraudulent or illegal activity

Businesses Maintaining Personal Information of 4 Million or More Consumers

For Businesses that annually buy, share, or receive for commercial purposes, or sell the information of, 4 million or more California consumers

- Must compile metrics for the previous calendar year:
  - Number of requests to know that the business received, complied with in whole or in part, and denied
  - Number of requests to delete that the business received, complied with in whole or in part, and denied
  - Number of requests to opt-out that the business received, complied with in whole or in part, and denied
  - Median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out
- Must include information in privacy policy or posted on website and accessible from a link included in their privacy policy
- Must also implement and document training for all individuals responsible for handling consumer requests or compliance with the CCPA

ENFORCEMENT / PRIVATE RIGHT OF ACTION

Enforcement Avenues

- California Attorney General Enforcement
- Limited Private Right of Action

Attorney General Enforcement

- **Scope**: Civil enforcement for **any violation** of CCPA against a "business, service provider, or other person."
- **Opportunity to Cure**: Applies to violation after business "fails to cure any alleged violation within 30 days after being notified of alleged noncompliance."
- **Civil Enforcement Damages**:
    - Injunctive relief
    - $2,500 for each violation
    - $7,500 for each intentional violation of the CCPA

Attorney General Enforcement (cont.)

- **Enforcement Delayed**:
  - "[U]ntil six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner."
- **New Consumer Privacy Fund**:
  - Civil enforcement penalties to be deposited in the Consumer Privacy Fund
  - Intended "to fully offset any costs incurred by the state courts and the Attorney General" in enforcement.

Attorney General Opinion

- "Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title."

Limited Consumer Private Right of Action

- **Significant Potential Consequences**
  - One of most significant aspects of CCPA
- **Opportunity to Cure**
  - Statutory damages
- **Remedies**
  - Damages
  - Injunctive or declaratory relief
  - "Any other relief the court deems proper"

Key Elements

(1) Nonencrypted and nonredacted personal information*
(2) "subject to an unauthorized access and exfiltration, theft, or disclosure
(3) as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information"

* Narrower definition of personal information

[Cal. Civil Code § 1798.150(a)(1)]

Limited Consumer Private Right of Action (cont.)

Opportunity to Cure

- **Actual Pecuniary Damages**
  - **No notice** required to initiate individual or class action

- **Statutory Damages**
  - Before "initiating any action" for "statutory damages" by individual or class action
  - Consumer **30 days' written notice** "identifying the specific provisions" of alleged violation
  - If cured within 30 days and business "provides the consumer an **express written statement** that the violations have been cured and that no further violations shall occur," no action for statutory damages or class-wide statutory damages may be initiated
  - For any continued CCPA violation "in breach of the express written statement", consumer may "**enforce the written statement** and may pursue statutory damages for each breach of the express written statement" along with any other CCPA violation after the written statement

Limited Consumer Private Right of Action (cont.)

- **What Personal Information?**
  - Not broad CCPA personal information definition
  - Limited to definition under "reasonable security" statute

Key Elements

(1) Nonencrypted and nonredacted **personal information***
(2) "subject to an unauthorized access and exfiltration, theft, or disclosure
(3) as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information"

* Narrower definition of personal information

[Cal. Civil Code § 1798.150(a)(1)]

CCPA Broad Definition of Personal Information

Personal information includes any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

1) Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, or passport number
2) Categories of PI described in California's customer records destruction law
3) Characteristics of protected classifications under CA or federal law
4) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies
5) Biometric information
6) Geolocation data
7) Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
8) Audio, electronic, visual, thermal, olfactory, or similar information
9) Professional or employment-related information
10) Education information that is subject to the Family Educational Rights and Privacy Act
11) Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

[Cal. Civil Code § 1798.140(o)]

Limited Consumer Private Right of Action

- **"Personal Information"**
  - Not encrypted or redacted

    (A) First name or first initial and his or her last name, plus another data element
    - **Social security number**
    - **Driver's license number or California identification card number**
    - **Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account**
    - **Medical information**
    - **Health insurance information**

    (B) A **username or email address** in combination with a **password or security question and answer** that would permit access to an online account.

Limited Consumer Private Right of Action (cont.)

- **Unauthorized Access**
- ***And* Exfiltration, Theft, or Disclosure**
  - o Fact specific
  - o What are the forensic facts?
  - o Legal conclusion

Key Elements

(1) Nonencrypted and nonredacted personal information*
(2) "subject to an **unauthorized access and exfiltration, theft, or disclosure**
(3) as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information"

* Narrower definition of personal information

[Cal. Civil Code § 1798.150(a)(1)]

Limited Consumer Private Right of Action (cont.)

- **Duty to implement and maintain reasonable security procedures and practices**
  - o Fact specific
  - o Nature of information
  - o Based on Reasonable Security Statute
    [Cal. Civil Code § 1798.81.5]

Key Elements

(1) Nonencrypted and nonredacted personal information*
(2) "subject to an unauthorized access and exfiltration, theft, or disclosure
(3) as a result of the business's violation of the **duty to implement and maintain reasonable security procedures and practices** appropriate to the nature of the information to protect the personal information"

Reasonable Security Statute

- "A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain **reasonable security procedures and practices** appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

- Note: Comparable statute in about half the states.

Limited Consumer Private Right of Action (cont.)

- **Remedies**
  - Statutory or actual damages (greater of)
  - Injunctive or declaratory relief
  - Any other relief the court deems proper

Key Elements

(1) Nonencrypted and nonredacted personal information*
(2) "subject to an unauthorized access and exfiltration, theft, or disclosure
(3) as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information"

* Narrower definition of personal information

[Cal. Civil Code § 1798.150(a)(1)]

Civil Damages

Statutory or Actual Damages

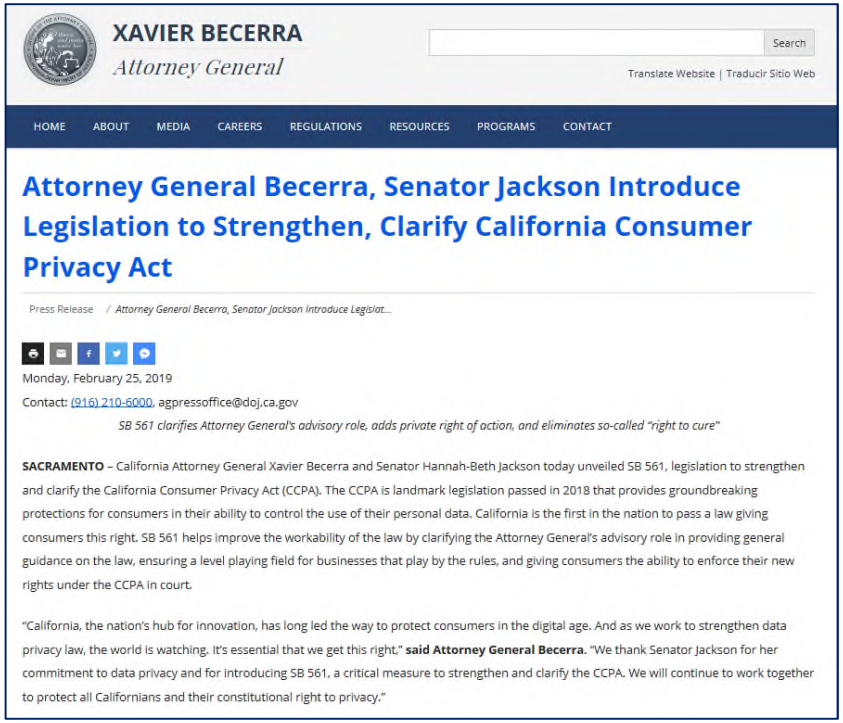
- **Greater of**:
  - not less than $100 and not greater than $750 per consumer per incident
  - or actual damages

Statutory Damages Factors

- Nature and seriousness of the misconduct
- Number of violations
- Persistence of the misconduct
- Length of time over which the misconduct occurred
- Willfulness of the defendant's misconduct
- Defendant's assets, liabilities, and net worth
- Other "relevant circumstances presented by any of the parties"

Efforts to Expand Enforcement Private Right of Action

- "SB 561 **[1]** removes requirements that the Office of the Attorney General provide, at taxpayers' expense, businesses and private parties with individual legal counsel on CCPA compliance; **[2]** removes language that allows companies a free pass to cure CCPA violations before enforcement can occur; and **[3]** adds a private right of action, allowing consumers the opportunity to seek legal remedies for themselves under the act."



XAVIER BECERRA
Attorney General

Search

Translate Website | Traducir Sitio Web

HOME ABOUT MEDIA CAREERS REGULATIONS RESOURCES PROGRAMS CONTACT

Attorney General Becerra, Senator Jackson Introduce Legislation to Strengthen, Clarify California Consumer Privacy Act

Press Release / *Attorney General Becerra, Senator Jackson Introduce Legislat...*

Monday, February 25, 2019

Contact: (916) 210-6000, agpressoffice@doj.ca.gov

SB 561 clarifies Attorney General's advisory role, adds private right of action, and eliminates so-called "right to cure"

SACRAMENTO – California Attorney General Xavier Becerra and Senator Hannah-Beth Jackson today unveiled SB 561, legislation to strengthen and clarify the California Consumer Privacy Act (CCPA). The CCPA is landmark legislation passed in 2018 that provides groundbreaking protections for consumers in their ability to control the use of their personal data. California is the first in the nation to pass a law giving consumers this right. SB 561 helps improve the workability of the law by clarifying the Attorney General's advisory role in providing general guidance on the law, ensuring a level playing field for businesses that play by the rules, and giving consumers the ability to enforce their new rights under the CCPA in court.

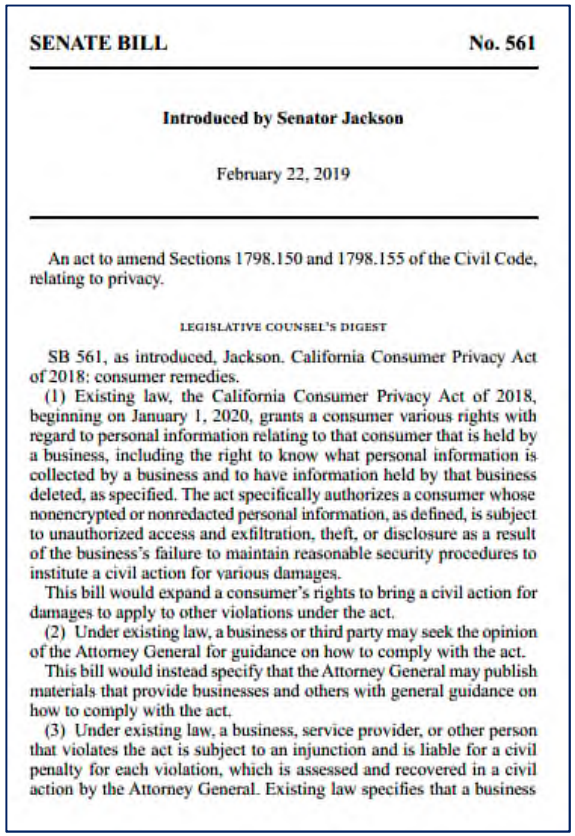
"California, the nation's hub for innovation, has long led the way to protect consumers in the digital age. And as we work to strengthen data privacy law, the world is watching. It's essential that we get this right," **said Attorney General Becerra.** "We thank Senator Jackson for her commitment to data privacy and for introducing SB 561, a critical measure to strengthen and clarify the CCPA. We will continue to work together to protect all Californians and their constitutional right to privacy."

https://oag.ca.gov/news/press-releases/attorney-general-becerra-senator-jackson-introduce-legislation-strengthen

Efforts to Expand Enforcement Private Right of Action (cont.)

- On **May 16**, the California Senate Appropriations Committee blocked SB 561.

- **SB 561** proposed to:
  1) Expand private right of action to all CCPA violations, not limited to security breaches;
  2) Eliminate 30 days to cure a violation before a private action may be filed; and
  3) Remove provision to request "the opinion of the Attorney General for guidance on how to comply with the provisions of this title";
     - Instead allows the Attorney General to "publish materials that provide businesses and others with general guidance on how to comply with the provisions of this title."



SENATE BILL **No. 561**

Introduced by Senator Jackson

February 22, 2019

An act to amend Sections 1798.150 and 1798.155 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 561, as introduced, Jackson. California Consumer Privacy Act of 2018: consumer remedies.

(1) Existing law, the California Consumer Privacy Act of 2018, beginning on January 1, 2020, grants a consumer various rights with regard to personal information relating to that consumer that is held by a business, including the right to know what personal information is collected by a business and to have information held by that business deleted, as specified. The act specifically authorizes a consumer whose nonencrypted or nonredacted personal information, as defined, is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's failure to maintain reasonable security procedures to institute a civil action for various damages.

This bill would expand a consumer's rights to bring a civil action for damages to apply to other violations under the act.

(2) Under existing law, a business or third party may seek the opinion of the Attorney General for guidance on how to comply with the act.

This bill would instead specify that the Attorney General may publish materials that provide businesses and others with general guidance on how to comply with the act.

(3) Under existing law, a business, service provider, or other person that violates the act is subject to an injunction and is liable for a civil penalty for each violation, which is assessed and recovered in a civil action by the Attorney General. Existing law specifies that a business

PREPARING FOR JANUARY 1 AND JULY 1, 2020

Morgan Lewis

The CCPA Beyond 2020

- Businessman Alastair Mactaggart, who sponsored the California ballot measure that was the impetus for the CCPA, announced the filing of a new ballot measure on Sept. 25 – the California Privacy Rights and Enforcement Act of 2020.
- With enough signatures, it will appear on the November 2020 California ballot.
- The new ballot measure would "substantially" raise the bar for CCPA compliance, including:
  - requiring consumers to expressly opt in to sate of sensitive information, such as health, financial, racial, and geolocation data;
  - tripling fines for violations of children's privacy; and
  - establish a new agency to replace the AG as the primary enforcer of the CCPA.

Ready by January 1 or July 1?

- As recently as a few weeks ago, many businesses were uncertain about how to implement CCPA by January 1, 2020.
- Now that amendments have been enacted and proposed regulations have been issued, the picture is (somewhat) clearer.
- AG Xavier Becerra stated that companies should not view the gap between the law's effective date and enforcement date as any sort of safe harbor.
  - "If that were [the case], then you could murder someone today and if we couldn't figure out who did it for a month, would that mean that you go scot-free? I don't think so. The law's the law."
- For many businesses, this may mean accelerating CCPA compliance efforts.
- The private right of action for security breaches is available commencing January 1.

Next Steps

- Assess what "personal information" is collected based on the CCPA's broad definition
- Review and update privacy policies
- Revise website home pages
- Prepare consumer notifications
- Consider how to verify consumer requests
- Consider safeguarding personal information, including encryption and redaction
- Review and assess "reasonable security procedures" in place to protect personal information

Next Steps (cont.)

- Issue employee privacy notices
- Comply with training requirements
- Review recordkeeping policies and requirements
- If a business collects personal information of minors, special rules apply
- Review non-discrimination issues to provide consumers with the right to equal service and price
- Review and update incident response plans

The CCPA – A Moving Target, But Still A Target

- Despite many remaining ambiguities and regulations that are still a work in progress, the CCPA's January 1 effective date is fast approaching
- Reasonable efforts to comply prior to the July 1 enforcement date should provide some measure of protection from potential enforcement
- Recent enactment of statutory amendments and issuance of proposed regulations means that the race to comply with the CCPA begins in earnest now

W. Reece Hirsch

W. Reece Hirsch
San Francisco
reece.hirsch@morganlewis.com
+1.415.442.1422

Reece Hirsch is a partner in the San Francisco office of Morgan Lewis and co-head of the firm's Privacy and Cybersecurity practice. He advises clients on a wide range of privacy and cybersecurity matters, and has special expertise in California and healthcare privacy laws, including HIPAA. Reece edited and contributed to Bloomberg Law's California Privacy Law Profile.

Reece has been listed in *Chambers USA: America's Best Lawyers for Business* since 2005, and has served on two advisory groups to the California Office of Privacy Protection and Department of Justice that developed recommended practices for security breach response and medical identity theft prevention. He is a Certified Information Privacy Professional, and is a member of the editorial advisory boards of *Bloomberg Health Law News, Healthcare Informatics*, and *Briefings on HIPAA*.

Mark L. Krotoski

Mark L. Krotoski
Silicon Valley | Washington, DC
mark.krotoski@morganlewis.com
+1.650.843.7212
+1.202.739.5024

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues
- Advises clients on mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Experience handling complex and novel cyber investigations and high-profile cases
  - At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
  - Served as the National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, in addition to other DOJ leadership positions.

Carla B. Oakley

Carla B. Oakley
San Francisco | Silicon Valley
carla.oakley@morganlewis.com
+1.415.442.1304
+1.650.843.7299

Carla B. Oakley is a partner in the San Francisco and Silicon Valley offices. She focuses on intellectual property and advertising, from inception and global protection through trial. Carla's litigation experience includes cases involving advertising, unfair competition, trademarks, domain names, trade secrets, copyrights, product design and trade dress claims, rights of publicity, patents, and false patent marking claims, as well as IP license disputes, database protection issues and enforcement of online terms of service.

She also advises clients on how to minimize risks of conducting business online and how to comply with privacy laws (including website privacy policies), effective website terms of use, advertising regulations (including social media and email marketing), Federal Trade Commission and Attorney General guidelines, and laws pertaining to sweepstakes and skills contests.

Kristin M. Hadgis

Kristin M. Hadgis
Philadelphia
+1.215.963.5563
kristin.hadgis@morganlewis.com

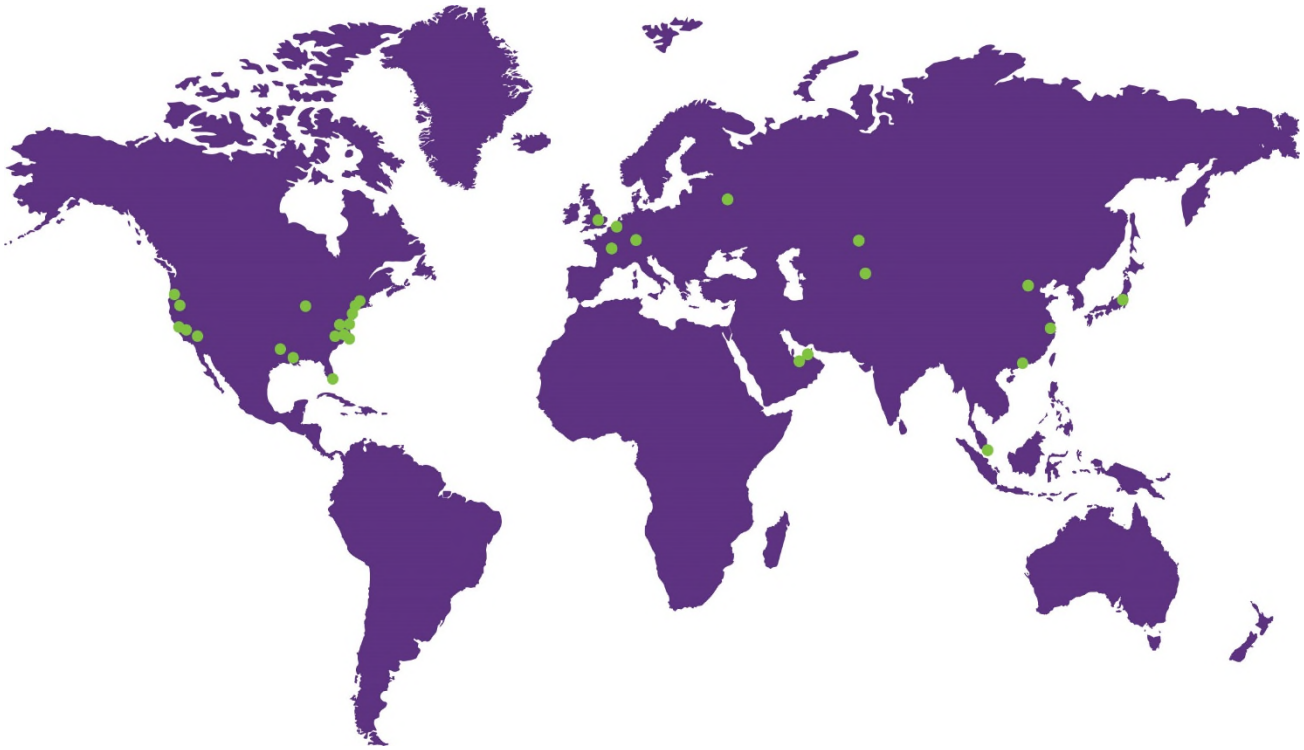
Kristin has represented companies faced with class actions and government investigations, and has advised hundreds of companies in connection with data breaches and privacy and cybersecurity compliance issues such as privacy policies, information security policies, incident response plans, and protocols for data collection, storage, and transfer. Her experience includes the General Data Protection Regulation (GDPR), state data security laws, the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transactions Act (FACTA), US federal and state CAN-SPAM laws, the Telephone Consumer Protection Act (TCPA), Federal Trade Commission (FTC) rules, the Securities and Exchange Commission privacy regulations (Reg. S-P), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA).

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.