Morgan Lewis

PRACTICAL PRIVACY AND THE CCPA: BRACING FOR JANUARY 1

W. Reece Hirsch
Mark L. Krotoski
Carla B. Oakley
December 9, 2019

Agenda

- Introduction
  - Amendments, draft regulations, ballot initiative, and deadlines
- Privacy Policies
- Employee Privacy Notices
- Mitigating Litigation Exposure
- Preparing for January 1 and July 1, 2020

SECTION 01

INTRODUCTION: PRACTICAL CCPA COMPLIANCE

Preparing for January 1

- The effective date of the California Consumer Privacy Act is January 1, 2020
  - 23 days away, but there is still much uncertainty
  - Regulations are still in draft form
  - Many questions of interpretation remain open
  - The initial comment period for the regulations just ended on December 6
  - The Attorney General's office will begin enforcing the new law on July 1, 2020

- This presentation will focus on some practical steps that you can take now to position your organization for January 1 and July 1

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 conducted four public hearings on the CCPA draft regulations
- December 4 hearing in San Francisco
  - Organizations such as the Association of National Advertisers, Alliance of Automobile Manufacturers and Electronic Frontier Foundation weighed in
  - Multiple requests for an extension of effective date to 1-1-22
  - No substantive comments from AG's office representatives
- 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 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

Parent and Subsidiary Businesses

- Magnolia Corp., a retailer (Parent), owns 100% of its subsidiary Magnolia California Corp.
- Magnolia California Corp. meets the definition of "business" (including annual gross revenues > $25 million
- Magnolia Parent is included in the CCPA "business" because (1) owns more than 50% of sub's stock and (2) shares a common "Magnolia" brand
- Does Magnolia Parent actually access California personal information?
- Does Magnolia Parent have substantive CCPA compliance obligations?
- Significance of including parent in a subsidiary "business" for CCPA enforcement purposes

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
- 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)

CCPA Exemptions Are Not Blanket Exemptions

- The availability of a CCPA exception does not mean that you're home free
- Example: The "GLBA exemption" exempts personal information collected "pursuant to" the GLBA-regulated activities of a financial institution
  - But do you have a public-facing website that collects personal information of website visitors through cookies?
  - Do you acquire lists of high-net-worth individuals who are not yet your "consumers" or "customers" under GLBA?
- Consider ***all*** of the ways that you may collect personal information

Are You A Service Provider?

- A service provider is:
  - A for-profit entity
  - That processes information on behalf of a business
  - Receives personal information for a "business purpose"
  - Pursuant to a written contract that
    - Prohibits the service provider from retaining, using or disclosing the personal information for any purpose other than the specified services or as permitted by the CCPA, including using PI for a commercial purpose other than providing the contracted services
  - Under the CCPA statute, significance was primarily that disclosure to a service provider pursuant to a compliant service provider agreement was not a "sale" triggering opt-out right

Expanding Regulation of Service Providers

- The proposed regs substantially expand the regulation of service providers
  - To the extent that a person or entity provides services to a person or organization THAT IS NOT A BUSINESS, shall be deemed a service provider under the CCPA
  - Would apply to contactors to non-profits and governmental entities
- A service provider shall not use personal information received as a service provider to provide services to another person or entity
  - Exception: PI can be combined to the extent necessary to detect data security incidents or protect against fraudulent or illegal activity
  - This new rule could significantly limit the ability of vendors to aggregate data to develop AI algorithms or deliver online advertising
  - Arguably exceeds the scope of the CCPA statute

Ready by January 1 or July 1?

- As recently as a month and a half 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."
  - Suggests that non-compliance prior to July 1 may be taken into account in a post-July 1 enforcement action, and may influence civil penalty amounts
- For many businesses, this may mean accelerating CCPA compliance efforts.
- The private right of action for security breaches is available commencing January 1.

Practical CCPA Compliance Steps

- What can you reasonably accomplish by January 1?
  - Employee, applicant, director, officer and contractor privacy notices
  - Amended website privacy policy
  - Commence service provider agreement amendment/contracting process
    - Notifications versus written amendments
  - CCPA training for "individuals responsible for handling consumer inquiries"
    - Proposed regs say training should cover "all requirements" in the regs and how to direct consumers to exercise their CCPA rights
  - Update document retention policies to ensure that all CCPA consumer request records are maintained for at least 24 months

Practical CCPA Compliance Steps (cont.)

- Data mapping and forming a compliance team to resolve practical CCPA compliance issues, such as:
  - Are you engaged in "sales," as broadly defined, triggering the opt-out right?
  - Are you providing "financial incentives" to consumers in exchange for the provision of personal information that would trigger a notice of financial incentives?
  - What methods should you make available for receiving consumer requests?
    - Are toll-free number and website form sufficient, or is another method needed to "reflect the manner in which the business primarily interacts with the consumer"?

Practical CCPA Compliance Steps (cont.)

- For the right of access, what constitutes a "readily useable format" for the consumer?
- What information will you request to verify the identity of a consumer submitting a request to know or request to delete?
  - Should that verification process vary based upon the sensitivity of the information subject to the request?
- Perfect CCPA compliance on January 1 is impossible because the regulations are still a work in progress and key templates (such as the form of opt-out button) are not yet available
  - Reasonable, ongoing efforts to achieve CCPA compliance is an attainable objective
- Please see the Morgan Lewis CCPA Resource Page for our Practical Privacy series of articles on CCPA compliance

SECTION 02

PRIVACY POLICIES

Background – Current Law For Information about California Consumers

- California Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22575, requires posted privacy policies for websites and online service providers that:
  - ID categories of personally identifiable information collected and the categories of third parties with whom the PII might be shared;
  - ID the process by which consumers may review and make changes to PII, if the business has such a process;
  - ID the process by which the business will notify users of material changes to the policy;
  - The effective date;
  - Explain how the business responds to "Do Not Track" signals or similar mechanisms that track online activities; and
  - State whether other parties may collect PII over time and across different sites.
- FTC and California Attorney General guidances

CCPA Requires Many New Privacy Policy Disclosures as of January 1, 2020

- Covered businesses must disclose in online privacy policies and any California-specific description of consumers' rights several additional categories of information, including:
  - Consumers' rights to know, delete and opt out of the sale of their information, and
  - How consumers can exercise these rights.
- Proposed regulations confirm that privacy policies must describe a business's practices regarding online and offline collection, use, disclosure and sale of personal information.
- Policies must be available in an offline/in-person environment if the business conducts substantial business in such a setting.

Privacy Policy Format Requirements

- Use plain language and avoid technical or legal jargon
- Be readable, including on smaller screens (mobile phones)
- Be available in all languages in which the business ordinarily communicates with consumers
- Be accessible to those with disabilities, including to inform persons with disabilities how they may access the policy in an alternative format
- Be available in a printable format
- Be posted online through a conspicuous link using the word "privacy" on the business's website homepage or the download or landing page of a mobile app

Policy Content Requirements: Right to Know

- Explain that a consumer has the right to request that a business tell the consumer what categories or specific pieces of PI the business collects, uses, discloses and sells
- Explain how consumers can submit verifiable requests
- Include links to online request forms or a portal for making requests
- List the categories of information the business has collected in the preceding 12 months and, for each category, provide the source from which it was collected, the purpose for collection, and categories of third parties with whom the business shares the PI
- State whether the business has disclosed or sold any PI in the preceding 12 months and, if yes, the categories of information disclosed or sold
- State whether the business sells PI of minors under age 16 without affirmative authorization

Policy Content Requirements: Right to Delete

- Explain that consumers have the right to request the deletion of their personal information
- Explain how consumers can submit verifiable requests, and how the verification process works
- Include links to online request forms or a portal for making requests

Policy Content Requirements: Right to Opt Out of Sale

- Explain that a consumer has the right to opt out of the sale of the consumer's personal information
- Include the contents of the right to opt out notice or a link to it via the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage or landing page of a mobile app

Policy Content Requirements: Nondiscrimination

- Explain that the business cannot discriminate against consumers if they exercise their privacy rights
  - Financial incentives or price/service differences are discriminatory if a business treats a consumer differently because the consumer exercises rights under the CCPA or regulations (Proposed Regulation, § 999.336)
  - Businesses may offer a price or service difference if reasonably related to the value of the consumer's data, for example:
    - Music streaming business offers a free service and a premium service for $5 per month. If only those who pay are allowed to opt out of the sale of their PI, then the practice is discriminatory unless the $5 payment is reasonably related to the value of the consumer's data to the business
    - A retailer offers discounted prices to those to are on the mailing list. If the consumers on the list can continue to receive discounted prices even after they exercise their rights to know, delete or request to opt out, the price difference is not discriminatory
- Proposed regulations include notice requirements regarding financial incentives, but do not require that these types of notices be included in a privacy policy (although may satisfy notice requirement by linking to disclosure in the privacy policy)

Policy Content Requirements: Authorized Agents

- Explain that consumers may designate authorized agents to make requests on their behalf
  - An "authorized agent" is a person or business that is registered with the Secretary of State and has been authorized by a consumer to act on the consumer's behalf, subject to Proposed Regulation § 999.326
  - For consumers who use authorized agents, the business may require that the consumer:
    - Provide the authorized agent written permission; and
    - Verify the consumer's own identity directly with the business.
  - Businesses may deny a request from an agent that does not submit proof that the person or business has been authorized by the consumer to act on the consumer's behalf

Policy Content Requirements: Contact and Date

- Provide contact information so that consumers can contact the business to raise questions or concerns about the business's privacy policy or practices
- Contact methods should be those that the business ordinarily uses for interactions with consumers
- Provide the date when the privacy policy was last updated (as required under California's current online privacy policy statute)

Policy Content Requirements: Large Data Sales

- Businesses that obtain, sell, or share the personal information of 4 million or more consumers who are California residents must disclose in the privacy policy the metrics they are required to compile under Section 999.317(g)(1) of the proposed regulations:
  - Disclose the number of requests to know, delete or opt out that the business received for the previous calendar year
  - Disclose the median number of days it took the business to respond to the requests

Personal Information of Minors

- Explain special procedures for opting in to the sale of personal information for minors under 16 years old
  - Businesses that have actual knowledge that they collect or maintain personal information of children under age 16, but at least 13 years of age, must have a process for those minors to opt in to the sale of their personal information
  - Businesses must explain how the minor in this age group can opt out after having provided affirmative authorization
- Explain special procedures for opting in to the sale of personal information for minors under 13 years old
  - Businesses that have actual knowledge that they collect or maintain personal information of children under age 13 must determine that a parent or guardian of the child has affirmatively authorized the sale of the personal information of the child
    - Proposed regulations detail six methods for reasonably determining that the person providing consent is the parent or guardian
  - Businesses must explain how the parent or guardian can opt out after having provided affirmative authorization

Recommendations

- Content requirements of the CCPA augment the requirements of Section 22575 of the Business and Professions Code
- ID types of PI the business collects, uses and/or shares about California residents
- Consider whether there is a reasonable business purpose for the collection of consumers' information
- Update existing privacy policies by January 1, 2020, complying with the terms of any existing policy regarding how amendments are implemented and communicated
- Policies are likely to be more granular and detailed due to the requirements to provide the source, purpose and third-party sharing information
- Be prepared to implement the CCPA requirements described in the policy
- Train personnel

SECTION 03

NOTICE REQUIREMENTS FOR EMPLOYERS

CCPA Covers Employees, Owners, Job Applicants, Officers, Directors and Independent Contractors

- "Consumer" is defined as "a natural person who is a California resident"
  - No requirement that the individual is buying or using for personal, family or household purposes
  - Definition necessarily includes individuals in the employment context, but the CCPA did not otherwise acknowledge the unique issues
- AB 25, signed by Governor Newsom October 11, put a one-year hold on all but two provisions in the CCPA for employees, owners, job applicants, officers, directors and independent contractors:
  - The notice requirement in Section 1798.100(b); and
  - The private right of action for breaches of nonencrypted and nonredacted personal information.
- AB 1355, signed by Governor Newsom on October 11, put a one-year hold on the CCPA for certain business-to-business communications

Employers' Notice Requirements for January 1, 2020

- CCPA requires businesses to provide notice to California residents regarding:
  - The categories of personal information they are collecting; and
  - The purposes for which each category of information will be used.
- CCPA and proposed regulations do not provide any guidance specific to the employment context
- Notices are to be provided "at or before the point of collection"
- Businesses may not collect additional categories of information or use the information for different purposes without providing a new notice
- The law does not expressly provide for notice regarding information collected prior to the CCPA's effective date of January 1, 2020
  - Consider including given the law's key goal of transparency

Employers' Notice Requirements (cont.)

- Plain, straightforward language without technical or legal jargon
  - Each category of information, and each purpose for which the information is used, must be identified in a manner that can be readily understood
- Format must draw attention to the notice and make the notice readable (including on small screens, which may be particularly applicable for businesses that collect job applications online or through mobile apps)
- Use the language that the business typically uses
- Be accessible to persons with disabilities
- Be visible or accessible where it will be seen before personal information is collected

Considerations for Employer Notices

- "Personal information" is broadly defined and includes nearly all types of publicly available information, including information obtained from social media sites
- In the employment context, this includes email addresses, account numbers, biometric information (including those collected for security and authentication procedures), GPS information, protected class information, performance records, computer usage monitoring record, and so on
- "Personal information" does not include deidentified or aggregated information
- Consider creating different notices for different categories of individuals given the different information collected, different uses, and likely different means for communicating with each category of individual

Timing and Enforcement for Employer Notices

- Notice provision is effective January 1, 2020
- Enforceable only by the California Attorney General
  - AG to provide notice and a 30-day opportunity to cure
- Violations can give rise to injunctions and civil penalties
- Enforcement actions cannot be brought until July 1, 2020
  - Non-compliance notices could be issued earlier
  - Failure to comply or at least take steps to compliance by January 1, 2020, may influence later enforcement for this and other CCPA provisions, as well as civil penalties

Recommendations for Employer Notices

- Identify all categories of personal information that have been and will be collected (regardless of source) regarding employees, owners, officers, directors, job applicants and independent contractors
- Identify all past and anticipated uses of each category of information, having in mind differences for employees, owners, officers, directors, job applicants and contractors
- Create clear and concise notices that are accessible to those with disabilities
- Provide the notices on or before January 1, 2020, having in mind the requirement that notices must be visible and seen in advance of collection
  - Consider separate notices, handbooks, website links with online job applications
  - Consider acknowledgements if possible to consistently obtain and document receipt
- Provide notices as new people join the company or are otherwise engaged

Additional Considerations for Employers

- The one-year delay also covers personal information of emergency contacts or benefits beneficiaries
  - There is no indication that businesses are required to send notices to these individuals, although use of the information should be limited to purpose for which it was collected
- Former employees, etc. – there is no indication that businesses are required to locate and send notices to these individuals
- The one-year delay applies only to information collected and used in the employment context, and does not extend to information collected from these same individuals in their roles as retail customers or otherwise
- Evaluate whether the business has the need to collect, retain and use all of the personal information traditionally collected and used
- Evaluate security measures and options to encrypt, redact, deidentify, aggregate, or destroy data as appropriate
- Monitor proposed regulations and new legislation tailored to the employment context, understanding that all of the CCPA may otherwise come into force January 1, 2021

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."

SECTION 04

MITIGATING LITIGATION EXPOSURE

Overview

- Compare Standards Before CCPA
- CCPA New Era in Class Action and Civil Data Breach Litigation
- Mitigation Steps

BEFORE CCPA

Before CCPA

- Cybersecurity or data breach damages have required proof of actual injury
- Constitutional bar: Article III standing "Cases" and "Controversies"
  - Plaintiff burden to show:
    - "The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. _, 136 S. Ct. 1540, 1547 (2016)
    - First element:
      - Plaintiff must "show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"
  - Motions to dismiss for lack of Article III

- Even assuming an injury could be shown, what damages can be proved?

Antman v. Uber (NDCA) (May 10, 2018)

- **Case Example**
- Uber drivers class-action "after an unknown hacker downloaded drivers' personally identifiable information ("PII") from Uber's computer system in May 2014"
- Dismissed with prejudice after three tries to amend complaint; failure to show standing
- Failure to "allege a disclosure about their PII that plausibly suggests an immediate, credible risk of harm. **The name, driver's license, and (for Mr. Antman) his bank account and routing information do not plausibly risk fraud or identity theft** for the reasons in the court's earlier orders."
- "By contrast, fraud and identity theft are plausible risks with the account numbers and passwords disclosed in *Zappos*, the credit-card numbers and Social Security numbers in *Attias*, or the names, addresses, and Social Security numbers in *Krottner*. "

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

SASHA ANTMAN and GUSTAVE LINK, individually and on behalf of others similarly situated,

Plaintiffs,

v.

UBER TECHNOLOGIES, INC. and Does 1–50,

Defendants.

Case No. 15-cv-01175-LB

ORDER GRANTING MOTION TO DISMISS

Re: ECF No. 182

INTRODUCTION

The plaintiffs are former Uber drivers who filed this class-action lawsuit against the defendant Uber Technologies — which operates a smart-phone application connecting drivers and passengers — after an unknown hacker downloaded drivers' personally identifiable information ("PII") from Uber's computer system in May 2014, an event that Uber disclosed in February 2015.[1] In October 2015, the court dismissed the First Amended Complaint ("FAC") — brought only by Mr. Antman — for lack of standing. *Antman v. Uber Techs., Inc.*, No. 3:15-cv-01175-LB,

Antman v. Uber Technologies Inc., No. 3:15-cv-01175 (NDCA)

Before CCPA

- Trend to apply "reasonable security" standard
- Standard in about half of the states including California

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."

New York SHIELD Act

- New reasonable security requirement for companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of" private information of New York residents.
- Effective March 21, 2019.
- Reasonable safeguards include
  - Risk assessments, employee training, selecting vendors capable of maintaining appropriate safeguards and implementing contractual obligations for those vendors, and disposal of private information within a reasonable time.

FTC v. Wyndham Worldwide Corp.

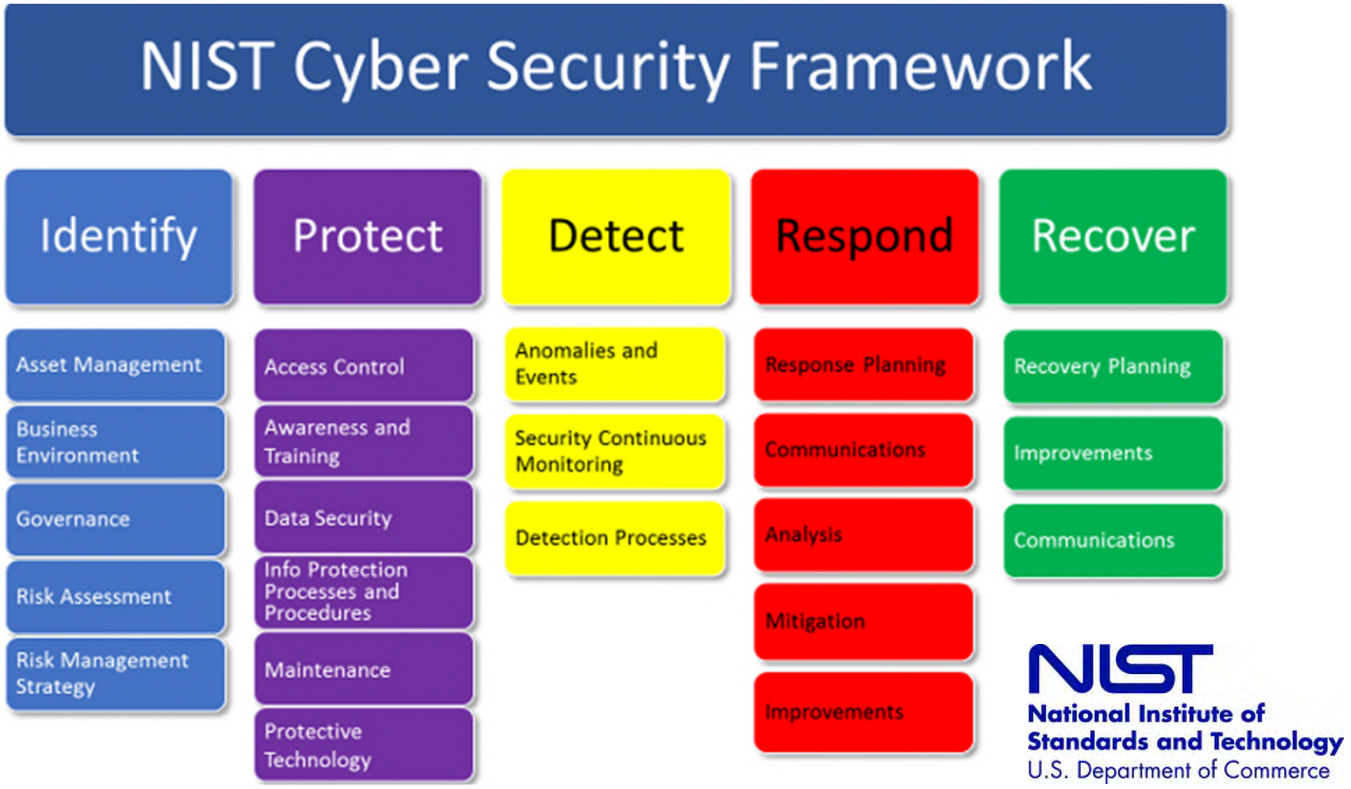
"Today's Third Circuit Court of Appeals decision reaffirms the **FTC's authority to hold companies accountable for failing to safeguard consumer data**. It is not only appropriate, but critical, that the FTC has the ability to take action on behalf of consumers **when companies fail to take reasonable steps to secure sensitive consumer information**."

https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect

Before CCPA

- Responding to enforcement actions and in civil litigation
- Record of reasonable cyber security program tailored to your information and risks
- Proactive in developing a strong, tailored cybersecurity program based on risk assessments, designed to safeguard vital or sensitive information and addressing any unique circumstances
- What is your Cyber Security Framework?

NIST Cyber Security Framework



CIS Critical Security Controls

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capabilities

Foundational CIS Controls

11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational CIS Controls

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

https://www.cisecurity.org/controls/cis-controls-list/

Central Role of Attorney Client Privilege

- For the purpose of seeking or providing legal advice
  - Aids in the careful evaluation of any threats/intrusions and responsive action for investigation, legal obligations, and litigation
  - Early in the process
  - Risks if not properly used/protected
- Company counsel working with outside counsel
- Role of counsel with vendors
  - At the direction of counsel
- Cases concluding failure to protect communications under privilege or work product doctrine

CCPA NEW ERA IN DATA BREACH LITIGATION

CCPA New Era in Data Breach Litigation

- **Key Questions**
  - What measures are in place to protect personal information?
  - Can you redact and encrypt where possible?
  - Can you demonstrate there are reasonable security procedures and practices appropriate to the nature of the information to protect the personal information?
  - Are you prepared to respond to an incident?

CCPA New Era in Data Breach Litigation

- No actual harm is required
- Court imposes the **greater** of **statutory or actual damages**
- Statutory damage range
  - Statutory damages are "not less than" $100 and "not greater than" $750 "per consumer per incident"
- Other remedies
  - Injunctive or declaratory relief
  - "Any other relief the court deems proper"

Staggering Statutory Damages

Per Consumer Per Incident	Low End of Statutory Range [$100]	High End of Statutory Range [$750]
1,000	$100,000	$750,000
10,000	$1 million	$7.5 million
100,000	$10 million	$75 million
1,000,000	$100 million	$750 million
10,000,000	$1 billion	$7.5 billion
100,000,000	$10 billion	$75 billion

When End of the Statutory Damages Range?

- **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"

Limited Consumer Private Right of Action

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"

[Cal. Civil Code § 1798.150(a)(1)]

MITIGATION STEPS

Limited Consumer Private Right of Action

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"

[Cal. Civil Code § 1798.150(a)(1)]

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."

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"

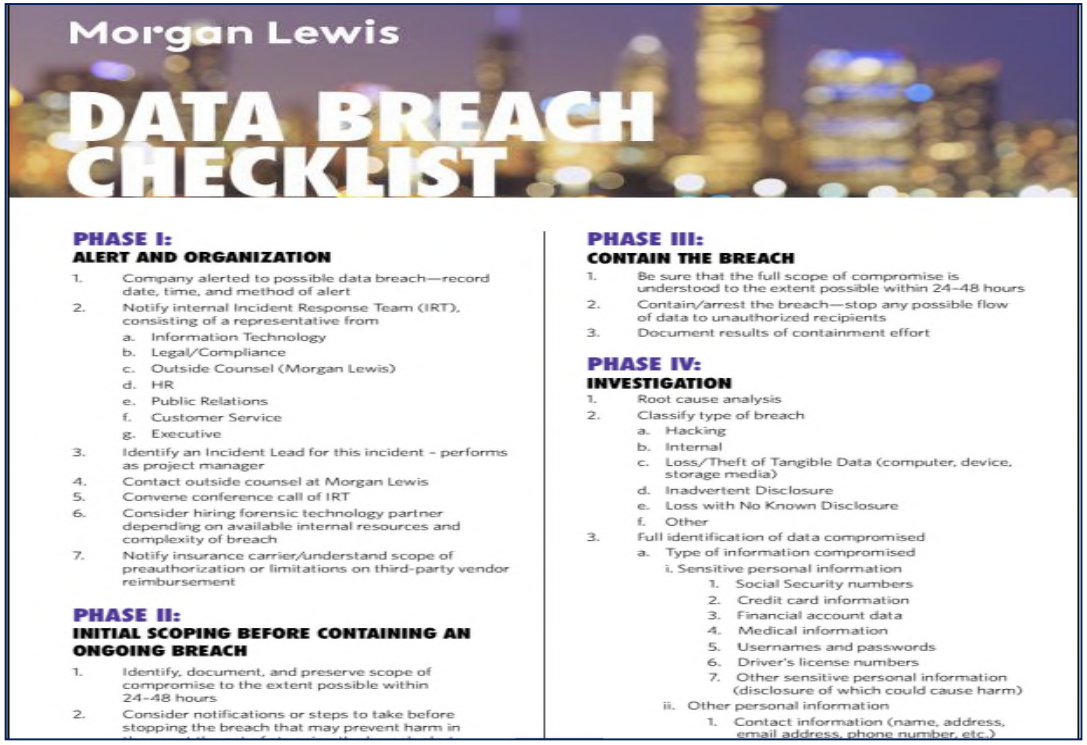
Reasonable Security Procedures and Practices

- **Demonstrate Reasonable Security Procedures and Practices**
  - Cyber Security Framework
    - Risk assessments designed to safeguard vital or sensitive information and address any unique circumstances
    - Mechanisms in place to prevent and detect incidents and respond and mitigate appropriately
  - Training
    - On cyber risk matters that may impact company
    - Also required under the CCPA
- **Policies and Controls**
  - Cybersecurity policies and controls based on key security areas
- **Role of Attorney Client Privilege and Work Product Doctrine**
  - At key stages in the cybersecurity process in which legal advice may be needed including for the establishment of appropriate policies to incident response and anticipated litigation
- **Governance**
  - Board's role in managing cyber risk and establishing a culture of cyber security

Reasonable Security Procedures and Practices

- **Third Party Vendors**
  - Vendor management processes in place to address risk issues
  - Due diligence in the selection of the vendor, contract provisions and measures to safeguard the information
- **Cyber Security Insurance**
  - Does the policy cover penalties to the extent permitted by law?
  - Does a "Claim" include a "regulatory proceeding" under the CCPA?
- **Incident Response Plan**
  - Tested and current plan to know that it will work when needed
  - Ensure that the incident response plan is updated for new issues including the CCPA
- **Responding to Cybersecurity Investigations**
  - Determining and assessing "unauthorized access and exfiltration, theft, or disclosure"
  - Managing multiple issues in determining scope of any incident
  - Preserving relevant records and anticipating downstream inquiries

Data Breach Checklist



Morgan Lewis

DATA BREACH CHECKLIST

PHASE I:
ALERT AND ORGANIZATION

1. Company alerted to possible data breach—record date, time, and method of alert
2. Notify internal Incident Response Team (IRT), consisting of a representative from
   a. Information Technology
   b. Legal/Compliance
   c. Outside Counsel (Morgan Lewis)
   d. HR
   e. Public Relations
   f. Customer Service
   g. Executive
3. Identify an Incident Lead for this incident – performs as project manager
4. Contact outside counsel at Morgan Lewis
5. Convene conference call of IRT
6. Consider hiring forensic technology partner depending on available internal resources and complexity of breach
7. Notify insurance carrier/understand scope of preauthorization or limitations on third-party vendor reimbursement

PHASE II:
INITIAL SCOPING BEFORE CONTAINING AN ONGOING BREACH

1. Identify, document, and preserve scope of compromise to the extent possible within 24–48 hours
2. Consider notifications or steps to take before stopping the breach that may prevent harm in

PHASE III:
CONTAIN THE BREACH

1. Be sure that the full scope of compromise is understood to the extent possible within 24–48 hours
2. Contain/arrest the breach—stop any possible flow of data to unauthorized recipients
3. Document results of containment effort

PHASE IV:
INVESTIGATION

1. Root cause analysis
2. Classify type of breach
   a. Hacking
   b. Internal
   c. Loss/Theft of Tangible Data (computer, device, storage media)
   d. Inadvertent Disclosure
   e. Loss with No Known Disclosure
   f. Other
3. Full identification of data compromised
   a. Type of information compromised
      i. Sensitive personal information
         1. Social Security numbers
         2. Credit card information
         3. Financial account data
         4. Medical information
         5. Usernames and passwords
         6. Driver's license numbers
         7. Other sensitive personal information (disclosure of which could cause harm)
      ii. Other personal information
         1. Contact information (name, address, email address, phone number, etc.)

Other Litigation Issues

- Is a class action waiver in favor of arbitration an option?
- "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."

Federal Arbitration Act (FAA)

- FAA, Section 2
  - "A written provision in any maritime transaction or **a contract evidencing a transaction involving commerce to settle by arbitration a controversy thereafter arising out of such contract or transaction**, or the refusal to perform the whole or any part thereof, or an agreement in writing to submit to arbitration an existing controversy arising out of such a contract, transaction, or refusal, **shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract**."

- "The FAA was enacted in 1925 in response to widespread judicial hostility to arbitration agreements. We have described this provision as reflecting both a '**liberal federal policy favoring arbitration**,' and the "fundamental principle that **arbitration is a matter of contract**.'" *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 339 (2011) (citations omitted).

Federal Arbitration Preemption Argument

- Class action waivers in arbitration provisions are enforceable
  - "When state law prohibits outright the arbitration of a particular type of claim, the analysis is straightforward: The conflicting rule is displaced by the FAA." *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 341 (2011)
  - *DirecTV Inc. v. Imburgia*, 577 U.S. _, 136 S. Ct. 463 (2015)
  - *Kindred Nursing Centers L.P. v. Clark*, 137 S. Ct. 1421 (2017), FAA supersedes state laws that undermine the goals of the act pursuant to implied preemption.
- Consider arbitration agreement and class action waiver
  - Requires affirmative consent
- Strong federal preemption argument that the FAA preempts CCPA
  - However likely to be litigated

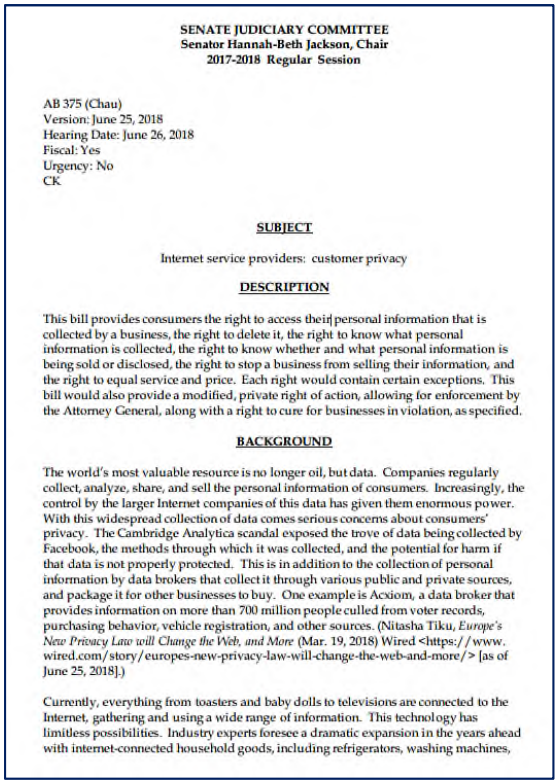
Other Litigation Issues

- What about using violations of the CCPA to support other claims such as the Unfair Competition Law?
- Unfair Competition Law (UCL)
  - Prohibits businesses from engaging in business practices that are "unlawful, unfair or fraudulent." Cal. Bus. & Prof. Code § 17200 *et seq*.
  - UCL may be used to establish "unlawful" practices based on violations of other laws.
    - *See, e.g., Cel-Tech Communications, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999) ("By proscribing 'any unlawful' business practice, 'section 17200 'borrows' violations of other laws and treats them as unlawful practices" that the unfair competition law makes independently actionable.'")

AB 375 – Senate Judiciary Report

- In addition, a recent amendment to the bill would add the following subdivision to the section providing the private right of action: "**Nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law.** This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution."

- "It appears that **this provision would eliminate the ability of consumers to bring claims for violations of the Act under statutes such as the Unfair Competition Law, Business and Professions Code Section 17200** et seq. It also makes clear that the Act does not relieve any parties from having to follow the Constitution. This latter provision is likely unnecessary."



SENATE JUDICIARY COMMITTEE
Senator Hannah-Beth Jackson, Chair
2017-2018 Regular Session

AB 375 (Chau)
Version: June 25, 2018
Hearing Date: June 26, 2018
Fiscal: Yes
Urgency: No
CK

SUBJECT

Internet service providers: customer privacy

DESCRIPTION

This bill provides consumers the right to access their personal information that is collected by a business, the right to delete it, the right to know what personal information is collected, the right to know whether and what personal information is being sold or disclosed, the right to stop a business from selling their information, and the right to equal service and price. Each right would contain certain exceptions. This bill would also provide a modified, private right of action, allowing for enforcement by the Attorney General, along with a right to cure for businesses in violation, as specified.

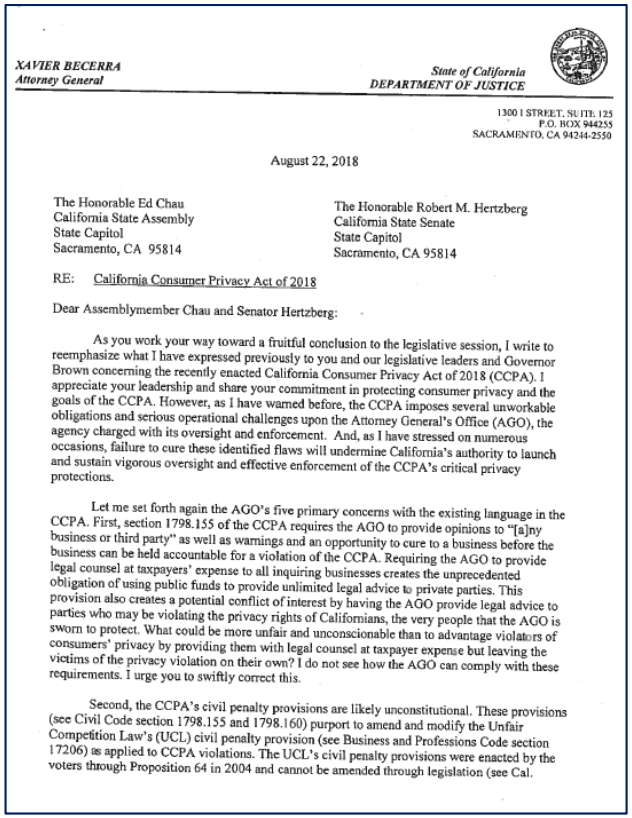
BACKGROUND

The world's most valuable resource is no longer oil, but data. Companies regularly collect, analyze, share, and sell the personal information of consumers. Increasingly, the control by the larger Internet companies of this data has given them enormous power. With this widespread collection of data comes serious concerns about consumers' privacy. The Cambridge Analytica scandal exposed the trove of data being collected by Facebook, the methods through which it was collected, and the potential for harm if that data is not properly protected. This is in addition to the collection of personal information by data brokers that collect it through various public and private sources, and package it for other businesses to buy. One example is Acxiom, a data broker that provides information on more than 700 million people culled from voter records, purchasing behavior, vehicle registration, and other sources. (Nitasha Tiku, *Europe's New Privacy Law will Change the Web, and More* (Mar. 19, 2018) Wired <https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/> [as of June 25, 2018].)

Currently, everything from toasters and baby dolls to televisions are connected to the Internet, gathering and using a wide range of information. This technology has limitless possibilities. Industry experts foresee a dramatic expansion in the years ahead with internet-connected household goods, including refrigerators, washing machines,

AG Letter

- "[T]he CCPA's civil penalty provisions are likely unconstitutional. These provisions (see Civil Code section 1798.155 and 1798.160) purport to amend and modify the Unfair Competition Law's (UCL) civil penalty provision (see Business and Professions Code section 17206) as applied to CCPA violations. The UCL's civil penalty provisions were enacted by the voters through Proposition 64 in 2004 and cannot be amended through legislation (see Cal. Const. art. II, § 10). We can and should **address this constitutional infirmity by simply replacing the CCPA's current penalty provision with a conventional stand-alone enforcement provision that does not purport to modify the UCI**. My team has offered corrective language for this purpose."



XAVIER BECERRA
Attorney General

State of California
DEPARTMENT OF JUSTICE

1300 I STREET, SUITE 125
P.O. BOX 944255
SACRAMENTO, CA 94244-2550

August 22, 2018

The Honorable Ed Chau
California State Assembly
State Capitol
Sacramento, CA 95814

The Honorable Robert M. Hertzberg
California State Senate
State Capitol
Sacramento, CA 95814

RE: California Consumer Privacy Act of 2018

Dear Assemblymember Chau and Senator Hertzberg:

As you work your way toward a fruitful conclusion to the legislative session, I write to reemphasize what I have expressed previously to you and our legislative leaders and Governor Brown concerning the recently enacted California Consumer Privacy Act of 2018 (CCPA). I appreciate your leadership and share your commitment in protecting consumer privacy and the goals of the CCPA. However, as I have warned before, the CCPA imposes several unworkable obligations and serious operational challenges upon the Attorney General's Office (AGO), the agency charged with its oversight and enforcement. And, as I have stressed on numerous occasions, failure to cure these identified flaws will undermine California's authority to launch and sustain vigorous oversight and effective enforcement of the CCPA's critical privacy protections.

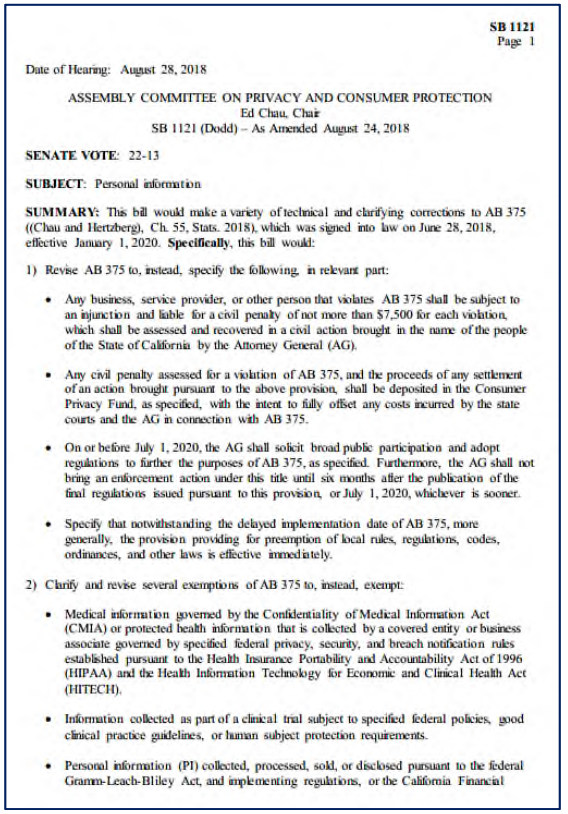
Let me set forth again the AGO's five primary concerns with the existing language in the CCPA. First, section 1798.155 of the CCPA requires the AGO to provide opinions to "[a]ny business or third party" as well as warnings and an opportunity to cure to a business before the business can be held accountable for a violation of the CCPA. Requiring the AGO to provide legal counsel at taxpayers' expense to all inquiring businesses creates the unprecedented obligation of using public funds to provide unlimited legal advice to private parties. This provision also creates a potential conflict of interest by having the AGO provide legal advice to parties who may be violating the privacy rights of Californians, the very people that the AGO is sworn to protect. What could be more unfair and unconscionable than to advantage violators of consumers' privacy by providing them with legal counsel at taxpayer expense but leaving the victims of the privacy violation on their own? I do not see how the AGO can comply with these requirements. I urge you to swiftly correct this.

Second, the CCPA's civil penalty provisions are likely unconstitutional. These provisions (see Civil Code section 1798.155 and 1798.160) purport to amend and modify the Unfair Competition Law's (UCL) civil penalty provision (see Business and Professions Code section 17206) as applied to CCPA violations. The UCL's civil penalty provisions were enacted by the voters through Proposition 64 in 2004 and cannot be amended through legislation (see Cal.

SB 1121 Amendments to CCPA

As amended August 24, 2018, SB 1121 now reflects the agreements reached between the authors of both AB 375 and SB 1121, and stakeholders on a variety of issues, consistent with the commitment of the authors when this Committee last heard SB 1121. Those issues include:

- Clarifying that the private right of action applies only to AB 375's section on data breach.
- Clarifying that the rights and obligations enumerated under AB 375 to not apply to the extent that they infringe upon any commercial activities of newsgathering entities, as specified under the California Constitution.
- Revising the AG enforcement section to ensure that there are no Proposition 64 issues by removing reference to the UCL (Section 17206 of the Business and Professions Code, specifically), and further eliminating the 80/20 split in the how civil penalties are to be allocated in the Consumer Privacy Fund, such that the penalties would, instead, *all* be deposited into the Consumer Privacy Fund with the intent to fully offset any costs incurred by the state courts and the AG in connection with this title, as otherwise specified under AB 375.



SB 1121
Page 1

Date of Hearing: August 28, 2018

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
SB 1121 (Dodd) – As Amended August 24, 2018

SENATE VOTE: 22-13

SUBJECT: Personal information

SUMMARY: This bill would make a variety of technical and clarifying corrections to AB 375 ((Chau and Hertzberg), Ch. 55, Stats. 2018), which was signed into law on June 28, 2018, effective January 1, 2020. **Specifically**, this bill would:

1) Revise AB 375 to, instead, specify the following, in relevant part:

- Any business, service provider, or other person that violates AB 375 shall be subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General (AG).
- Any civil penalty assessed for a violation of AB 375, and the proceeds of any settlement of an action brought pursuant to the above provision, shall be deposited in the Consumer Privacy Fund, as specified, with the intent to fully offset any costs incurred by the state courts and the AG in connection with AB 375.
- On or before July 1, 2020, the AG shall solicit broad public participation and adopt regulations to further the purposes of AB 375, as specified. Furthermore, the AG shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this provision, or July 1, 2020, whichever is sooner.
- Specify that notwithstanding the delayed implementation date of AB 375, more generally, the provision providing for preemption of local rules, regulations, codes, ordinances, and other laws is effective immediately.

2) Clarify and revise several exemptions of AB 375 to, instead, exempt:

- Medical information governed by the Confidentiality of Medical Information Act (CMIA) or protected health information that is collected by a covered entity or business associate governed by specified federal privacy, security, and breach notification rules established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).
- Information collected as part of a clinical trial subject to specified federal policies, good clinical practice guidelines, or human subject protection requirements.
- Personal information (PI) collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act, and implementing regulations, or the California Financial

CCPA Does Not Establish Other Private Rights of Action

- "Nothing in this title shall be interpreted to serve as the basis for a **private right of action under any other law**."
  - Part of AB 375, CCPA as originally enacted

SECTION 05

PREPARING FOR JANUARY 1 AND JULY 1, 2020

CCPA Compliance Is 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 by January 1 (where feasible) and ongoing efforts to achieve full compliance by the July 1 enforcement date should provide some measure of protection from potential enforcement
- Recent enactment of statutory amendments, issuance of proposed regulations and the fast approaching January 1 effective date mean that the race to comply with the CCPA begins in earnest now

QUESTIONS

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, online database protection issues and enforcement of online terms of service. She has first chair jury trial and appellate experience, and has handled disputes in a variety of forums.

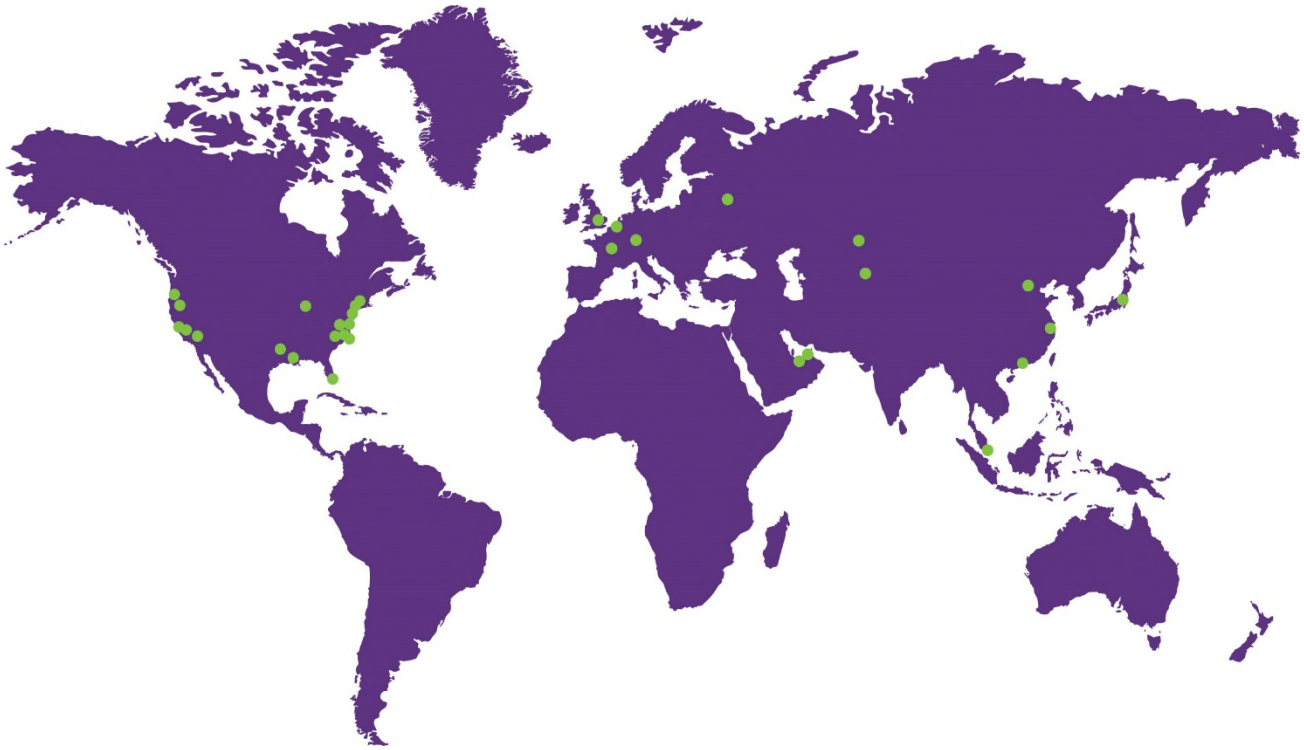
Since companies started doing business on the internet, Carla has been advising clients on how to minimize risks of conducting business online and compliance with privacy laws (including website privacy policies and other notices required under privacy laws), advertising regulations (including social media and email marketing), Federal Trade Commission and Attorney General guidelines, and laws pertaining to sweepstakes and skills contests, as well as effective website terms of use and protection on online databases.

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