California Consumer Privacy Act
Countdown to Compliance

Usama Kahf
ukahf@fisherphillips.com
(949) 798-2118

www.fisherphillips.com
“Cyberweapons and sophisticated hacking pose a greater threat to the United States than the risk of physical attacks.”

Kirstjen Nielsen
Secretary of Homeland Security
in a speech at GW University
September 5, 2018
How did this Bill Come to be Law?

• Alastair Mactaggart, a rich real estate developer, self-funded a ballot measure that would have implemented an even tougher law than the one that was passed.
How did this Bill Come to be Law?

Bill History

• Because the legislature would have become irrelevant regarding privacy if the measure passed, and it looked like it would, the legislature had two choices:
  ▪ (a) take their chances with a ballot measure that would be nearly impossible to change; or
  ▪ (b) pass AB375, which had been in the works for over a year, which they could change later

• They blinked and the ballot measure went away. FOR NOW!
How did this Bill Come to be Law?

Bill History

• According to the legislature’s website, this bill was not a last-minute decision, as is often incorrectly stated. In fact, it was introduced in February 2017, 16 months before it was ultimately passed.

https://leginfo.legislature.ca.gov/faces/billHistoryClient.xhtml?bill_id=201720180AB375
Whom Does the Law Protect?

Applies To

• All California residents, including:
  ▪ Customers
  ▪ Employees
  ▪ Visitors to a company internet site or building
  ▪ Contractors and independent contractors
  ▪ Vendors

It’s not just your “customer’s” data.
Whom Does the Law Apply To?

Applies To

All companies that collect California residents data and:

• Have annual gross revenues in excess of $25,000,000
  -OR-

• Annually buy, receive, sell or share for commercial purposes, alone or in combination, the personal information of 50,000 or more California consumers, households or devices
  -OR-

• Derives 50 percent or more of its annual revenues from selling consumers’ personal information.
Whom Does the Law Apply To?

This includes:

- Companies directing that others collect the information on their behalf
- “Controlled” Affiliates
- Companies that share common branding
What Types of Information Does the Law Apply To?

Applies To

• “Personal Information” of California Residents

• Online AND offline –
  ▪ “not limited to information collected electronically or over the Internet, but [the law applies] to the collection and sale of all personal information collected by a business from consumers.”
What is Personal Information?

• Much broader than typical “Personally Identifiable Information” as used in most state data breach statutes

• Essentially, most information that could identify an individual OR be used in conjunction with other information to identify an individual
What is Personal Information?

- Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following:
Examples of Personal Information:

- Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, Social Security number, driver’s license number, passport number or other similar identifiers

- Characteristics of protected classifications under California or federal law
Personal Information

• Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies

• Biometric information

• Internet or other electronic network activity information, including, but not limited to, browsing history, search history and information regarding a consumer’s interaction with an internet website, application or advertisement
• Geolocation data
• Audio, electronic, visual, thermal, olfactory or similar information
• Professional or employment-related information
• Education information (defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act)
• Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.
Limited Exemptions from Personal Information:

- Publicly available information or information that is lawfully made available from federal, state or local government records (like land title records), so long as it is used in a manner consistent with the purpose for which it was collected

- Certain types of “regulated” information
What rights does this law confer?

- Right to know
- Purpose limitation
- Right to deletion
- Right to opt out of sale*
- Right to be free of discrimination
- Regulatory enforcement
- Private right of action (limited)
Right to Know

- Companies must be able to provide employees with:
  - What information the company collected/holds about the employee
  - Purposes for which the information was collected
  - Where the company got that information
  - How that information is being used
  - Whether the information is being disclosed or sold
  - To whom the information is being disclosed or sold
Right to Know

**Rights**

- Businesses will have to inform employees, **at or before the point of collection**, what categories of personal information they collect and the business’s purpose in collecting that information.

- Businesses will have to provide information about the personal information they have collected from a consumer upon receipt of a **verifiable consumer request**.
A Verifiable Request

Verifying a Request

• Let’s say you collected information on me as a job applicant that you never ended up hiring.
• How do you **VERIFY** that I am me?
• Not a hacker, not an imposter and not some other John Doe with the same name.
Right to Know

Rights

Creates multiple compliance challenges

- Thorough inventory of data, including collection, storage and uses
- Policies and compliance mechanisms to
  - ensure processing consistent with purpose limitation
  - inventory processing, disclosure and sale
  - track and respond to consumer requests
Purpose Limitation

• Information must generally be used for company’s operational purposes or other notified purposes that are reasonably necessary and proportionate to the purpose for which the data was collected.

• Businesses cannot use the data for a purpose not disclosed – additional disclosure will be needed.

• Businesses cannot collect additional categories of personal information without providing notice.
Right to Deletion

Rights

• The right to have their data deleted, upon request, unless it “is necessary for the business to maintain the consumer’s personal information.”
For example:

- Comply with a legal obligation
- Find, prevent or prosecute security breaches
- “Enable solely internal uses that are reasonably aligned with the consumer’s expectations
- “Otherwise use the consumer’s personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information”
Right to Opt Out of Sale

Rights

• The right to say no to the sale of personal information.
• “Do Not Sell My Personal Information.”
• The right to equal service and price, even if they exercise their privacy rights.
Right to be Free of Discrimination

- Generally, businesses must provide equal service and pricing to consumers regardless of whether they exercise their rights under the act.
- Some provision to allow businesses to “pay” consumers who allow greater use of personal information.
You need to be able to track

- Do not sell requests
- Opt in authorizations (for under 16s)
- Deletion requests
- Access (copies) requests
- Along with your response
- To make sure that you can prove compliance
Noncompliance – Consequences

Consequences

- Civil penalties from an AG action up to $7,500 per violation
- Private right of action in case of a breach up to $750 per consumer per incident, or actual damages
- 30-day right to cure, but how do you cure a breach?
Much More to Come

AG Responsibilities

• The law authorizes the AG to “adopt regulations to further the purposes of this title.”

• Some statutory revisions have already been proposed – more revisions likely.
The News

The Good News –
• It doesn’t go into effect until 1/1/2020, so the legislature could tweak it
• Enforcement does not start until 7/1/2020

The Bad News –
• There is a LOT of work to do
First set of changes signed by the governor in Sept. 2018 (SB 1121):

- The Cal. AG is no longer a gatekeeper on private rights of action
- Extended HIPAA exemption to other personal information if protected in the same way
First set of changes signed by the governor in Sept. 2018 (SB 1121):

• Enforcement begins the earlier of 6 months after publication of guidelines or 7/1/2020, whichever is first

• Clarifies PI as must be reasonably linked, directly or indirectly, to a consumer or household

• Clarifies that private right of action must be related to a breach as a result of reasonable security practices (all breaches will be claimed to be a result of that)
AB 25 (Pending) – Amends the CCPA

• “clean-up” bill by same author of CCPA
• Originally intended to exempt employee data collected by employers for employment purposes
• After it passed the Assembly, there was late opposition from labor groups
• Compromise ➔ postpone by one year (until 1/1/20201) all requirements for employee data except 2
AB 25 (Pending) – Amends the CCPA

- If it passes, 2 requirements still go into effect 1/1/2020 with respect to employee data:
  - Reasonable security measures to protect employee data (both physical and electronic)
  - Disclosure of categories of PI collected and the business purposes for which it is collected
California Consumer Privacy Act

- Enacted in June 2018
- Effective 1/1/2020; enforcement starts 7/1/2020
- Applies to for profit businesses based on certain factors
- Disclosure requirement at or before collecting information from consumers
- Gives number of rights to consumers
California Consumer Privacy Act

• Expanded definition of “Personal Information” – applies to all paper and electronic info
• Requires adopting policies, procedures and tools to track what info is collected, deleted, requested
Planning

• Assume there will be some changes and challenges
• Start planning for implementation by 1/1/2020
• Start budgeting for the implementation
Final Questions?

Presented by:
Usama Kahf
Phone: (949) 798-2118
Email: ukahf@fisherphillips.com