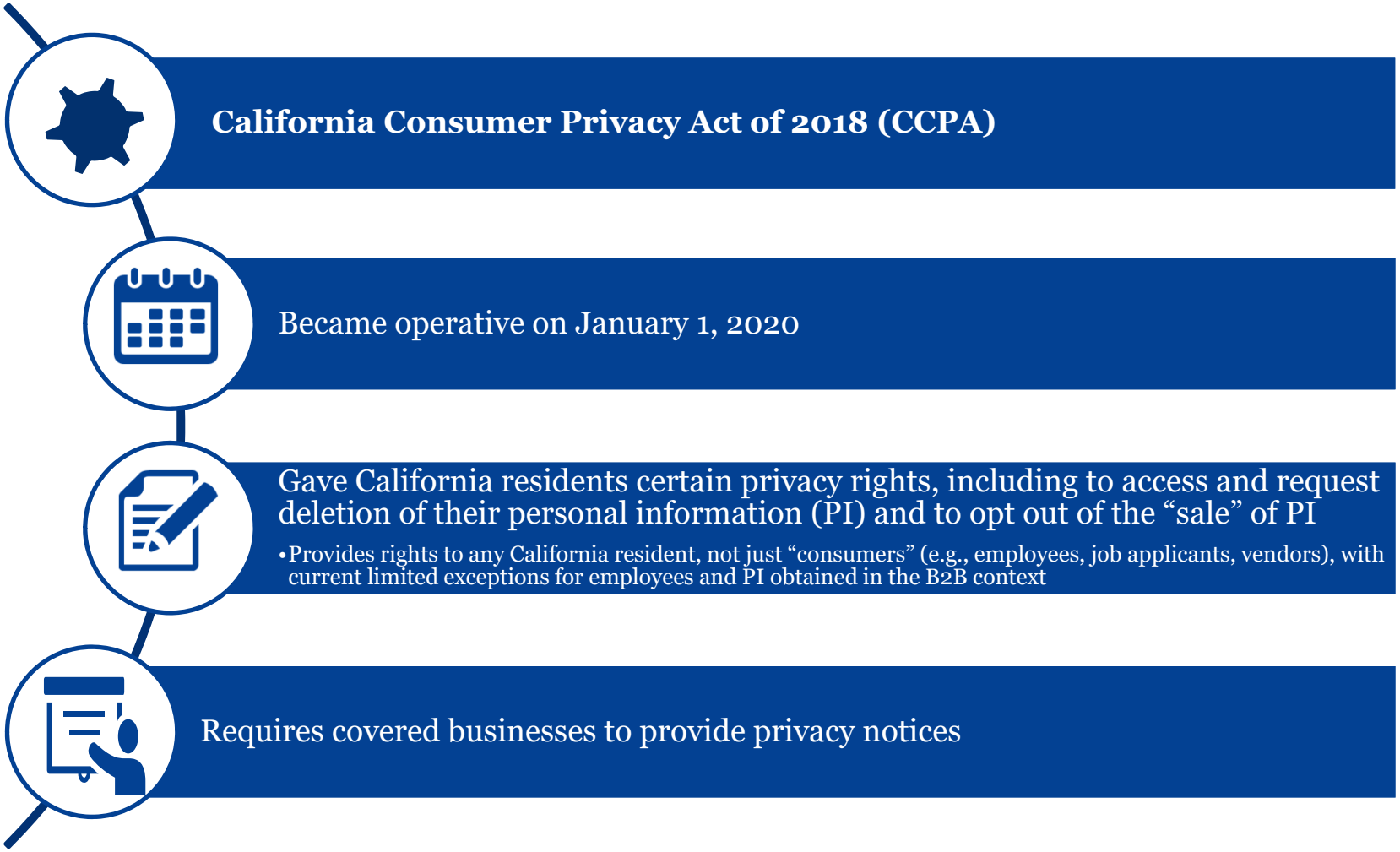
MORRISON FOERSTER

NEW STATE PRIVACY LAWS TO ADD TO THE MIX: CPRA AND VA CDPA – WHAT DO THEY ADD TO THE CCPA?

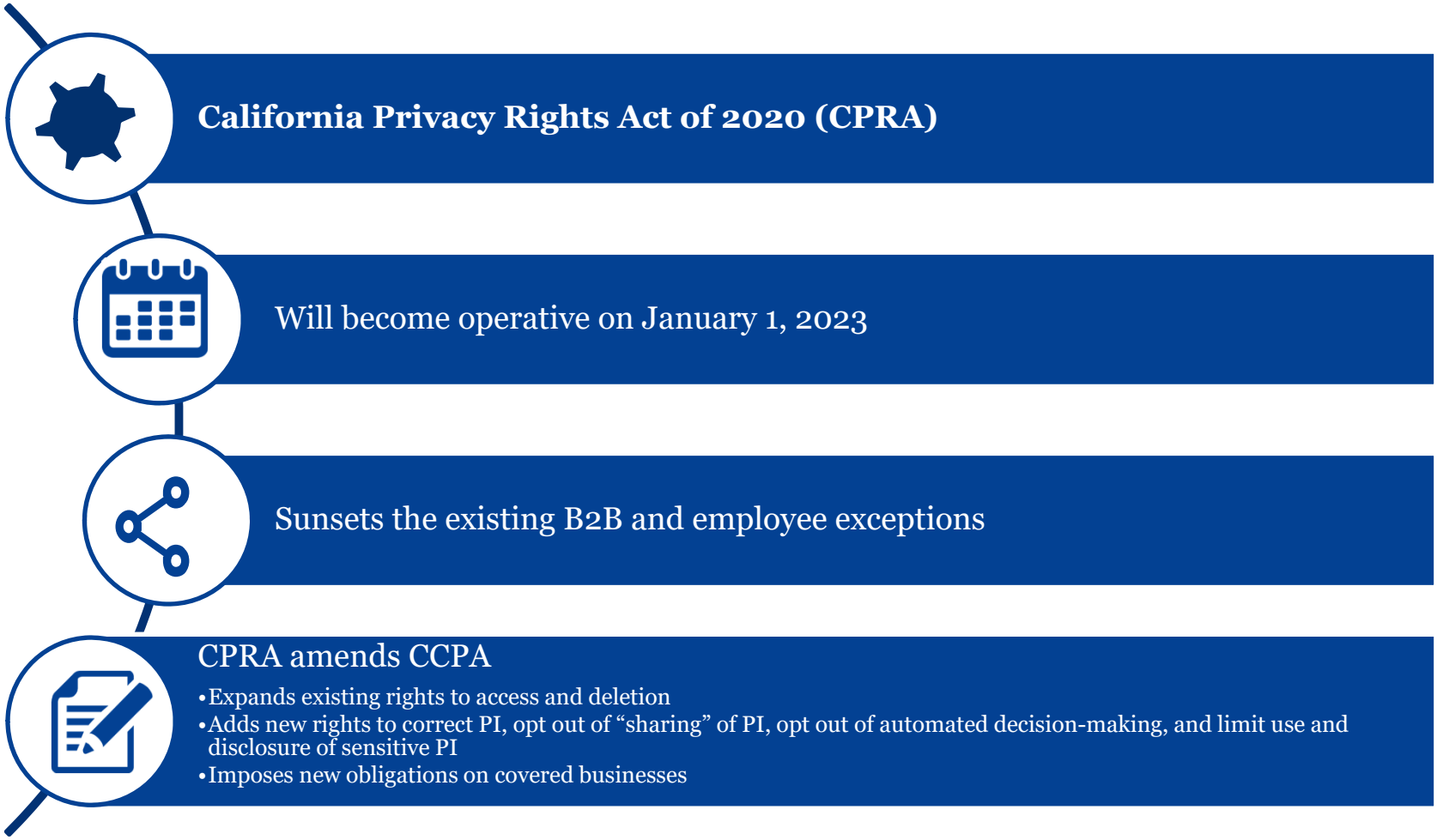
Kristen J. Mathews, Morrison & Foerster
Courtney Barton, Marriott

May 25, 2021

A Refresher on the CCPA



The New CPRA


California Privacy Rights Act of 2020 (CPRA)
Will become operative on January 1, 2023
Sunsets the existing B2B and employee exceptions
CPRA amends CCPA
•Expands existing rights to access and deletion
•Adds new rights to correct PI, opt out of "sharing" of PI, opt out of automated decision-making, and limit use and disclosure of sensitive PI
•Imposes new obligations on covered businesses

CPRA Overview: What's New?

New rights

- Right to limit use and disclosure of Sensitive Personal Information
- Right to opt out of Sharing PI (for cross-context behavioral advertising)
- Right to correct PI

New requirements

- Purpose limitation and data minimization obligations
- Contractual provisions for agreements with third parties with whom businesses share PI
- Implement reasonable security procedures and practices
- Businesses whose processing poses "significant risk to consumers' privacy or security" must perform an annual, independent cybersecurity audit, and submit privacy risk assessment to newly formed enforcement agency

Modified requirements

- Service providers
- Behavioral advertising
- Enhanced notice obligations

New or modified exceptions

- De-identified data
- Publicly available data
- Physical items
- Small business

And more…

CPRA Timeline

2022

The **regulations** under the CPRA are required to be finalized by July 1, 2022.

2023

With some exceptions, the CPRA will become **operative** on January 1, 2023.

Enforcement powers will begin on July 1, 2023, and will not be retroactive.

Generally (except with respect to access requests), the CPRA will only apply to personal information (PI) that is collected after January 1, 2022.

The New Virginia Consumer Data Protection Act (VCDPA)

Effective January 1, 2023

- Same as operative date of CPRA

No regulations are called for

- However, there is a work group that will review the provisions of the act and submit findings, best practices, and recommendations to the legislature by November 1, 2021.

Will be enforced exclusively by Virginia Attorney General

Substantively, a mix of the CCPA, CPRA, and GDPR

Scope

	CPRA	VCDPA
Covered Entities	For-profit entities that collect consumers' PI, do business in California, and: • Have annual gross revenues in excess of **$25,000,000;** • Alone or in combination annually buy, sell, or share the PI of **100,000 or more consumers or households**; or • Derive **50% or more of annual revenue** from selling or sharing consumers' PI.	Entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents and that: • Control or process personal data of at least **100,000 consumers** who are VA residents in a calendar year; or • Control or process the personal data of at least **25,000 consumers** who are VA residents *and* derive over **50% of gross revenue** from the sale of personal data.
Employee/B2B Exception	Sunsets January 1, 2023.	Yes.
Non-Profits Exempted	Yes.	Yes (also exempts institutions of higher education and utilities).
HIPAA / GLBA Exemptions	Apply to **data.**	Apply to **entities.**
Other Key Exemptions	PI bearing on a consumer's creditworthiness (as defined in FCRA); information collected as part of a clinical trial; PI collected, processed, sold, or disclosed pursuant to the DPPA; vehicle information to effectuate warranty or recall.	Personal data created or maintained for purposes of select federal laws, including FCRA, FERPA, and DPPA.

What Is Personal Information/Data?

VCDPA's "Personal data" definition is similar to CCPA/CPRA, except it only includes data that is identifiable to a natural person (i.e., does not also extend to a household or device)

VCDPA excludes personal data of employees, applicants, and representatives of a business when they are acting in that capacity

- Unlike CPRA, this exception does not expire on January 1, 2023

CPRA and VCDPA both exclude publicly available information

VCDPA Consumer Rights

As under the CPRA, consumers have the right to:

- Find out whether the controller is processing their personal data
- Access the personal data the controller is processing
- Correct inaccuracies in the personal data
- Delete personal data provided by or obtained about the consumer
  - The specific deletion exceptions in CCPA/CPRA are not present in VCDPA
- Obtain a copy of the personal data that the consumer previously provided to the controller…
  - in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit the data to another controller without hindrance, where the processing is carried out by automated means

Conundrum:
Can a consumer obtain a copy of data that is not processed by automated means?

VCDPA Consumer Right to Opt Out of Sale

Consumers can opt out of:

- "Sale" of personal data
  - Unlike under CCPA/CPRA, "sale" only includes exchange of data for monetary consideration (not other things of value)
  - Excludes disclosure of personal data that the consumer intentionally made publicly available without restricting its audience
  - Also excludes sharing personal data with an affiliate (and "affiliate" is broadly defined to include other entities that share a brand)

CPRA New Right: Opt Out of "Sharing"

Introduces "Sharing" as a new term

- Disclosing PI to third parties for cross-context behavioral advertising (CCBA) purposes
- No monetary or other valuable consideration required
  - Doesn't matter whether anything of value is shared back in return for the PI
- In contrast with "sale" under CCPA

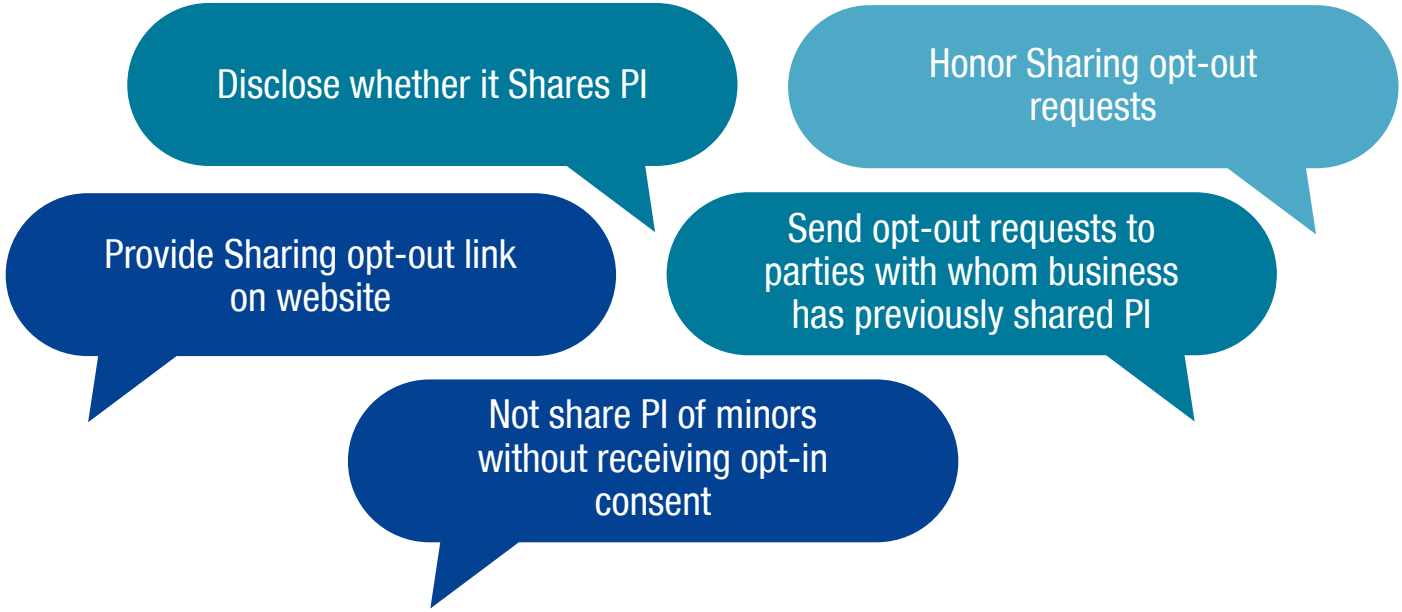
What is cross-context behavioral advertising (CCBA)?

- "Targeting of advertising to a consumer based on the consumer's PI obtained from the consumer's activity across businesses, distinctly-branded websites, applications or services, *other than the business, distinctly-branded website, application or service with which the consumer intentionally interacts*"
- This definition is focused on sources that are *not* first-party data (e.g., third-party data)

CPRA New Right: Opt Out of "Sharing"

Consumers have the right to opt out of a business's Sharing of PI, just as they do from the sale of PI

- Sharing requirements mirror CCPA's existing requirements for sales. A business must:



VCDPA Right to Opt Out of Targeted Ads

Consumers can opt out of:

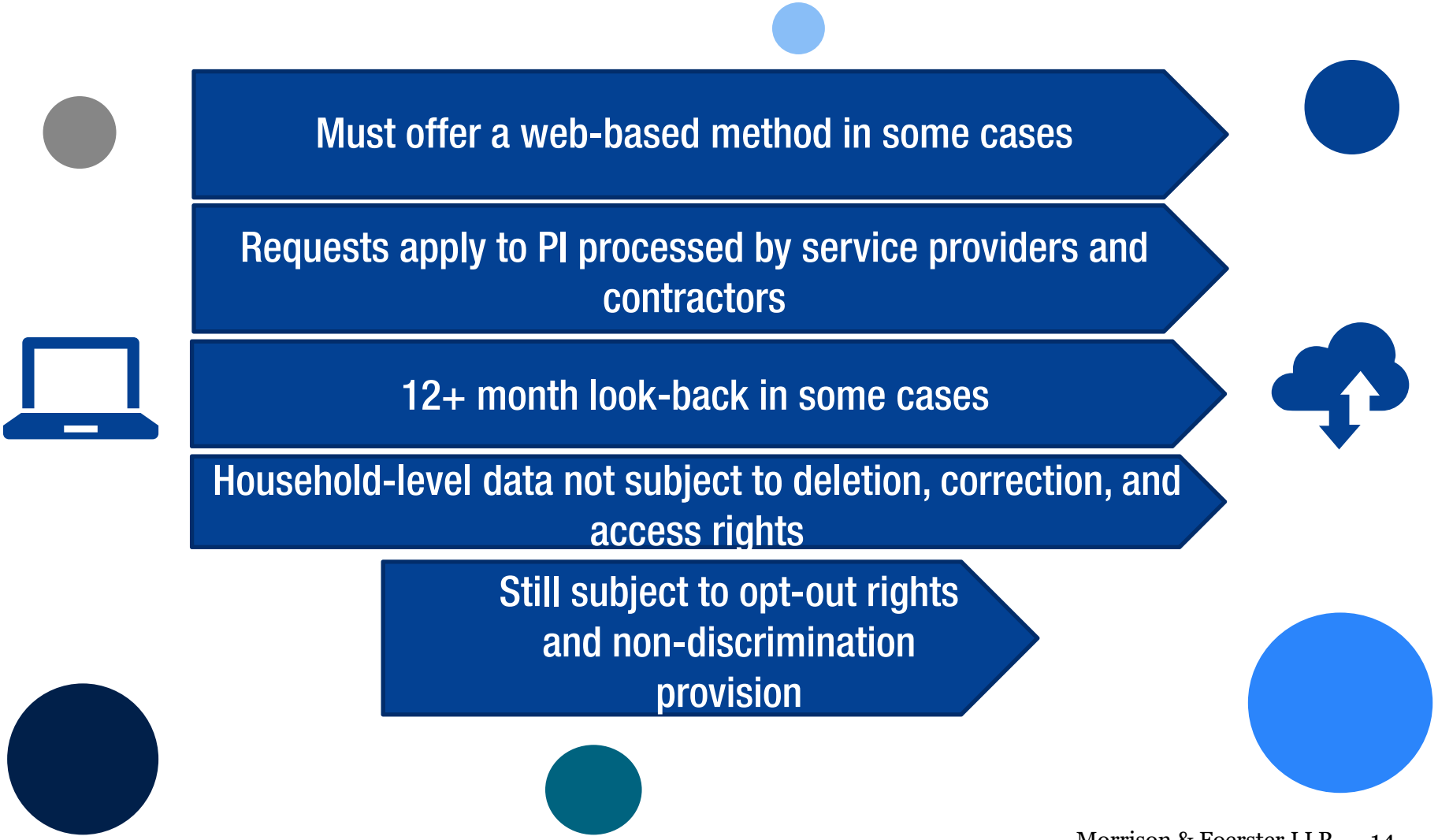
- Processing of personal data for the purpose of targeted advertising
- "Targeted advertising" is displaying advertisements that are selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests. Targeted advertising does *not* include:
  - First party tracking
  - Contextual advertising
  - Ads in response to consumer request for info
  - Measuring, reporting ad performance, reach, or frequency

Conundrum:
If personal data only includes data identifiable to a natural person, not a device, how broad is the opt-out for use of personal data for targeted advertising?

CPRA and VCDPA Right to Opt Out of Auto Decisions

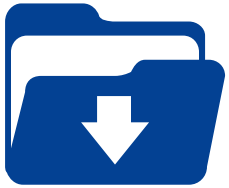
- VCDPA: Automated profiling (as defined) in furtherance of decisions that produce legal or similarly significant effects concerning the consumer (i.e., financial, lending, housing, insurance, education, criminal justice, employment, health care, or basic necessities)
- CPRA: Regulations will detail this consumer right

CPRA Consumer Requests



CPRA Access Requests

- For access requests (other than requests for "specific pieces"), a business's Privacy Policy is deemed to be compliance if the Privacy Policy contains information that satisfies the request
  - The Privacy Policy does not have to be specific for the individual. It has to be accurate as to consumers generally.
- Categories of PI must be described using specific terms of PI and SPI definitions
- **Format/portability**: when "specific pieces" are requested, they must be provided in a portable format
  - Structured, commonly used, machine-readable format


CPRA Deletion Requests

- CPRA expands a business's obligations in response to deletion requests: business **must notify all third parties** to which it has sold or Shared PI (not just service providers) **to delete PI**
  - Unless impossible or disproportionate effort
  - **Potentially very broad implications**
    - A radical interpretation:
      - Is a business's "sale" or "sharing" of PI encumbered by consumers' future deletion right?
      - Would this effectively make a sale or sharing of PI merely a license that can later be revoked?
    - Unclear how narrowly or broadly this should be interpreted

CPRA Deletion Requests (cont'd)

CPRA changes certain exceptions to the deletion right

- The "catchall" exception is eliminated
- Other new exceptions are added

Service providers have a direct duty under CPRA to delete and to direct sub-processors to delete

VCDPA Consumer Rights

Controller must establish and inform consumers of an appeals process if it declines a consumer request.

Moreover, if the controller declines the request after the appeal, it must give the consumer a method to contact the Virginia Attorney General to submit a complaint.

Sensitive Personal Information/Data

CPRA

*Overlapping elements are **bolded***

Sensitive personal information (PI)

- Social security, driver's license, state identification card, or passport number.
- Account log-in, financial account, debit card, or credit card number in combination with security or access code, password, or credentials allowing access to an account.
- **Precise geolocation.**
- **Racial or ethnic origin, religious** or philosophical beliefs, or union membership.
- Contents of consumer's mail, email, or texts, unless the business is the intended recipient.
- **Genetic data.**
- **Biometric information, processed for the purpose of uniquely identifying a consumer.**
- PI collected and analyzed concerning a consumer's health.
- PI collected and analyzed concerning a consumer's sex life or sexual orientation.

VCDPA

Sensitive personal data

- **Racial or ethnic origin or religious beliefs.**
- **Mental or physical health diagnosis.**
- **Sexual orientation.**
- Citizenship or immigration status.
- **Genetic or biometric data processed for the purpose of uniquely identifying an individual.**
- Personal data collected from a known child (under age 13).
- **Precise geolocation.**

CPRA: Using or Disclosing SPI *Beyond* Limited Purposes Triggers Heightened Obligations

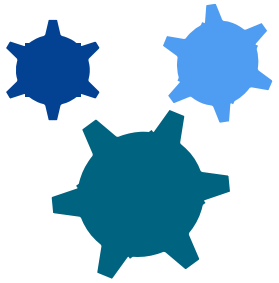
- What are the **limited purposes**?
  - To **perform the services** set forth in subsections **2, 4, 5, and 8 of the "business purpose" definition**
    - (2) Helping to ensure security and integrity,
    - (4) Short-term, transient use,
    - (5) Performing services on behalf of the business (e.g., maintaining accounts, fulfilling orders and transactions), and
    - (8) Maintaining quality of, or improving, the business's service or device; **and**
  - As authorized by **regulations**

- If a business uses or discloses SPI ***beyond*** the limited purposes:
  - Must provide **additional notice**
  - Must provide a clear and conspicuous **link** on its website that enables a consumer to limit the use or disclosure of SPI (or respect an opt-out preference signal)
  - **Upon consumer request:**
    - **Business** must **limit** (a) its own **use** and (b) **disclosure** of SPI to service providers and contractors
    - After receiving instructions from business, **service providers and contractors** cannot use SPI for any other purpose

SPI Exemption

- If SPI is collected/processed **without the purpose of inferring characteristics** about a consumer, then such SPI qualifies for an exemption

- May be difficult for a business to **draw the line** as to when SPI is collected/processed for purposes of inferring characteristics vs. when it's not
  - Regulations to shed light on this
    - 1798.185(a)(19)(C): "issuing regulations…to govern the use or disclosure of a consumer's [SPI]…including:…(iv) ensuring that the exemption…applies to information that is **collected or processed incidentally**, or **without the purpose of inferring characteristics about a consumer**, while ensuring that businesses do not use the exemption for the purpose of evading [consumers' SPI rights]"



VCDPA Sensitive Data: What Are the Rules?

Must obtain consent to process Sensitive Data

- Recall GDPR-like high bar for consent
- Must comply with COPPA to process personal data of a child under 13 years old

Must conduct data protection assessments of processing of Sensitive Data

Conundrum:
How can a business comply with COPPA when data is collected offline and, therefore, not covered by COPPA?

CPRA Consent Is Not…

- Acceptance of a **general or broad terms of use** or a similar document that contains descriptions of PI processing along with other, unrelated information
- **Hovering over, muting, pausing,** or **closing** a given piece of content
- Agreement obtained through use of **dark patterns**
  - "Dark pattern" is a user interface designed or manipulated with the substantial effect of subverting or importing user autonomy, decision-making, or choice, as further defined by regulations

CPRA Notice at Collection…

- Is the duty of the controller of the collection
- Must include (in addition to what's required under CCPA):

- Whether PI is sold or Shared
- What categories of SPI are collected, the purposes for which they are processed, and whether they are sold or Shared
- The retention period for each category of PI or the criteria for the retention period

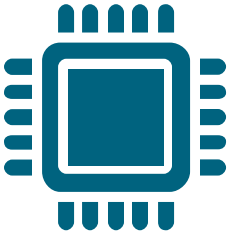
VCDPA Privacy Notice

- Like CCPA Privacy Notice
- Categories of personal data processed
- Purposes for processing
- Categories of personal data shared (excludes processors)
- Categories of third parties with which personal data are shared (excludes processors)
- Whether controller sells personal data, or uses it for targeted advertising, and if so, how to opt out
- How consumers can exercise their consumer rights afforded by VCDPA
- How consumers can appeal when the controller declines to honor a request

Data Minimization, Proportionality, and Purpose Limitation

	CPRA	VCDPA
Limiting Collection	Business may not collect additional categories of PI, or use PI collected for additional purposes that are incompatible with the disclosed purpose at collection, without providing the consumer with notice.	Controller must limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.
Proportionate Processing	Business's collection, use, retention, and sharing of PI must be reasonably necessary and proportionate to achieve the purposes for which the PI was collected or processed, or for another disclosed, compatible purpose.	Controller may not process personal data for purposes that are neither reasonably necessary to nor compatible with the disclosed purposes for which the data are processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.
Retention	Business may not retain PI or sensitive PI for each disclosed purpose for longer than reasonably necessary for that disclosed purpose.	No specific requirements.

CPRA Retention



Retention policy
Practically speaking, businesses will need a retention policy to comply with the retention-related notice requirements (as well as the data minimization requirement)

Privacy notice must include the **retention period** or **retention criteria** for each category of PI collected

A business is **prohibited** from retaining PI or SPI for each disclosed purpose for which it was collected for **longer than is reasonably necessary** for that disclosed purpose

Cybersecurity

CPRA and VCDPA: Businesses must have reasonable security procedures and practices

- In CCPA, this duty wasn't actually *in* CCPA; the private right of action re: data breaches cross-referenced the CA Customer Records Act
- Due to the CPRA, this duty now appears in CCPA itself, which (a) now **covers more PI** and (b) broadens the scope of CPRA enforcement powers

CPRA Private right of action following data breaches

- CPRA adds **username/password** combinations as triggers
- Compliance with Customer Records Act following a data breach is **not a "cure"** for the data breach

CPRA Regulations to require annual cybersecurity **audits** and periodic **risk assessments** for some businesses

- Risk assessments will have to be sent to the new agency CPPA

VCDPA Data Protection Assessments

Controllers must perform data protection assessments if they:

- Use personal data for targeted advertising
- Sell personal data
- Use personal data for automated profiling (re: economic situation, health, personal preferences, interests, reliability, behavior, location, movements) that presents a reasonably foreseeable risk of:
  - Unfair or deceptive treatment of, or unlawful disparate impact on, consumers
  - Financial, physical, or reputational injury
  - Offensive intrusion upon solitude or seclusion, or privacy affairs or concerns
  - Other substantial injury
- Process sensitive data
- Engage in other processing involving personal data that presents heightened risk of harm to consumers

VCDPA Data Protection Assessments

VCDPA assessments are like GDPR impact assessments	VCDPA allows piggy-backing on other laws' assessments
Upon request under a CID, must share assessment with Attorney General	This will not waive the attorney client privilege
Assessments are only required for processing "created or generated" after January 1, 2023	

CPRA Service Providers

- CPRA may **narrow** what service providers are able to do with PI without a data transfer being considered a "sale" or "sharing" of PI

Narrows down the use of PI for service provider's own use or for benefit of others

- **Deleted** from definition of "**business purposes**"

  - References to service providers' own purposes
  - References to behavioral advertising

- Open door for **regulations** to add back to what service providers can do

CPRA Contracts with Service Providers, Contractors, And Third Parties

Content requirements for agreements to which business discloses PI:	Service providers and contractors
	Outright transferees
Some content requirements that are not in CCPA:	Compliance with CCPA
	Quasi-audit rights
	Duty to inform business if no longer able to comply
	Quasi-self-help on part of business
	Provisions on sub-processors

VCDPA Processors

Adhere to controller's instructions

Assist controller in meeting its obligations, including to respond to consumer requests, security measures, breach notification, or data protection assessments

Contracts with processors:

- Type of personal data; instructions for processing; nature, purpose, and duration
- Duty of confidentiality on each person engaged in processing
- Deletion or return of data at end of services, unless retention required by law
  - Unlike CCPA/CPRA, no exception for back-up and archival copies
- Information to demonstrate compliance
- Cooperation with controller's assessments of processor's policies and technical/organizational measures (or an independent assessment arranged by processor and reported to controller)
- Pass through obligations to sub-processors
- Prohibit processor from re-identifying de-identified data

Reasonable oversight of processor's compliance with duties regarding de-identified and pseudonymous data

Non-Discrimination and Financial Incentives

CPRA

Business may not discriminate against a consumer for exercising rights under the Act, including by:

- Denying goods or services.
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
- Providing a different level or quality of goods or services.
- Suggesting that the consumer will receive a different price, rate, level, or quality for goods or services.
- Retaliating against an employee, applicant for employment, or independent contractor.

Business may:

- ✓ Charge a different price or provide a different level or quality of goods/services if the difference is reasonably related to the value provided to the business by the consumer's data.
- ✓ Offer loyalty, rewards, premium features, discounts, or club card programs.
- ✓ Offer financial incentives, including payments as compensation, for the collection, sale, sharing, or retention of PI. Requires notice and opt-in consent.

VCDPA

Controller may not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers, or discriminate against a consumer for exercising rights under the Act, including by:

- Denying goods or services.
- Charging different prices or rates for goods or services.
- Providing a different level of quality of goods and services.

Controller may offer a different price, rate, level, quality, or selection of goods or services, including offering goods or services for no fee, if:

- ✓ The consumer has exercised his or her opt-out right.
- ✓ The offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

De-identified Personal Data

CPRA

Information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer.

De-identification standards:

- ✓ Take reasonable measures to ensure that the information cannot be associated with a consumer or household.
- ✓ Publicly commit to maintain and use the information in de-identified form and not to attempt to re-identify the information, except to determine whether its de-identification processes satisfies the requirements of the Act.
- ✓ Contractually obligate any recipients of the information to comply with all provisions of this subdivision.

VCDPA

Data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person.

De-identification standards:

- ✓ Take reasonable measures to ensure that the data cannot be associated with an individual.
- ✓ Publicly commit to maintaining and using de-identified data without attempting to re-identify the data.
- ✓ Contractually obligate any recipients of the de-identified data to comply with all provisions of the Act.

De-identified Personal Data

De-identified personal data are not covered by CPRA/VCDPA

VCDPA: Consumer requests do not apply to de-identified data as long as certain conditions are met

VCDPA: A controller that discloses de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which de-identified data is subject and shall take appropriate steps to address any breaches of those contractual commitments

VCDPA Conundrum:
The definition of personal data does not mention devices, and the requirements to maintain de-identification do not mention devices. Do devices matter?

VCDPA Pseudonymous Data

Pseudonymous data is personal data that cannot be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person

A lower standard than de-identified data

Also reduced benefits

VCDPA Pseudonymous Data

If controller can demonstrate that any information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing such information, then:

- Consumer requests (except the rights to opt-out) do not apply to pseudonymous data
- Purpose and minimization, data security, non-discrimination, consent, and privacy notice provisions of VCDPA do not apply to pseudonymous data

A controller that discloses pseudonymous data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which pseudonymous data is subject and shall take appropriate steps to address any breaches of those contractual commitments

Publicly Available PI Exception

CPRA broadens the exception for PI that is publicly available

PI made publicly available:

- By the consumer
- By widely available media
- By someone who received the PI from the consumer without a duty of confidentiality

VCDPA treats publicly available personal data similarly

CPRA Physical Item Exception

Upon request, no need to delete or refrain from selling PI contained in physical items (e.g., yearbooks), if:

- The consumer consented to the business's use, disclosure, or sale of their PI to produce the physical item
- The business incurred significant expense in reliance on the consumer's consent
- Honoring the request would not be commercially reasonable
- Business complies with the consumer's request as soon as it is commercially reasonable to do so

VCDPA Exceptions

VCDPA does not have specific exceptions for each provision

Instead, it has several generic exceptions at the end that apply to the whole Act

Several are like the CCPA's exceptions

- e.g., except as required by law

VCDPA Exceptions

Generic exceptions compensate for some of the exceptions that are absent from specific provisions

E.g., the VCDPA shall not restrict a controller's or processor's ability to:

- Provide a product or service specifically requested by a consumer; perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty; or take steps at the request of the consumer prior to entering into a contract
- Conduct internal research to develop, improve, or repair products, services, or technology
- Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller or that are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party

These can possibly be used as exceptions to consumer deletion requests and to the processor's duty to delete data at end of term

Additional Regulations Under CPRA

New California Privacy Protection Agency will promulgate regulations and enforce CCPA

Automated decisions and profiling

Audits by the California Privacy Protection Agency

Opt-Out Preference Signal

22 total itemized regulation powers, plus "additional regulations as necessary to further the purposes of this title"

Enforcement

CPRA		VCDPA
California Privacy Protection Agency (CPPA).	Enforcement Body	Virginia Attorney General.
30 days; applies only to violations stemming from data security incidents.	Cure Period	30 days.
Yes; expanded to include unauthorized access of email addresses and passwords or security questions.	Private Right of Action?	No.
Consumers: $100-$750 per consumer per incident or actual damages, whichever is greater, injunctive or declaratory relief, and other relief the court deems proper. **CPPA:** Fine of up to $2,500 per violation or $7,500 per intentional violation (or violations involving the PI of consumers known to be under 16).	Possible Damages	**AG:** Civil penalties of up to $7,500 per violation, injunctive relief, expenses, and attorney's fees.

To Do 2021

- ❑ Prepare to fold employee personal information and personal information of business representatives into your CCPA compliance program (CA), including how you will receive and honor their CPRA requests.
- ❑ Businesses need to have legacy agreements with service providers/processors (CA and VA) and other third parties (CA) amended by 1/1/23. To achieve this, businesses should start using the new addenda in agreements they enter into now.
- ❑ Prepare internal written guidelines on de-identification, aggregation, and pseudonymization to meet the criteria of CPRA and VCDPA.
- ❑ Prepare an internal written data retention policy with criteria for how long each category of personal information will be retained (CA).

To Do 2021

- ❑ If you are a service provider to businesses, determine what, if anything, you must change about the scope of your use of personal data that you process for your business customers.
- ❑ Determine whether you process sensitive personal information/data (as defined differently by CPRA and VCDPA) and, if so, plan to give consumers the required opt-out (CA) and opt-in (VA) rights.
- ❑ Determine whether you "sell" or "share" personal information, or use it for targeted advertising or automated decisions, and determine what opt-in and opt-out rights you will be required to give to consumers.
- ❑ Consider an internal process for sending deletion requests to all third parties to which you have disclosed personal information, not only your service providers (CA).

To Do 2022

- ❑ Update your Privacy Notices in accordance with CPRA and VCDPA.
- ❑ Update (or prepare) a Privacy Notice to employees in accordance with the CPRA.
- ❑ Update your internal procedure to process individual requests in accordance with the CPRA and VCDPA, and add an appeals process.
- ❑ Update your internal CCPA training materials to conform to the CPRA and VCDPA.
- ❑ Identify what your business does that requires a data protection assessment (VA) or a risk assessment (CA), prepare assessment templates, and conduct any required assessments.
- ❑ Review your financial incentive programs for compliance with CPRA and VCDPA.

Questions?

THANK YOU

Kristen J. Mathews
Partner, New York
Privacy + Data Security
kmathews@mofo.com
(212) 336-4038

Courtney Barton
VP & Senior Counsel
Marriott