Morgan Lewis

UPDATE ON STATE PRIVACY LAWS & FEDERAL CYBER REPORTING REQUIREMENTS FOR ENERGY COMPANIES

December 7, 2022

Presenters

Kristin M. Hadgis

J. Daniel Skees

Catherine North Hounfodji

Arjun Prasad Ramadevanahalli

Terese M. Schireson

Morgan Lewis

Agenda

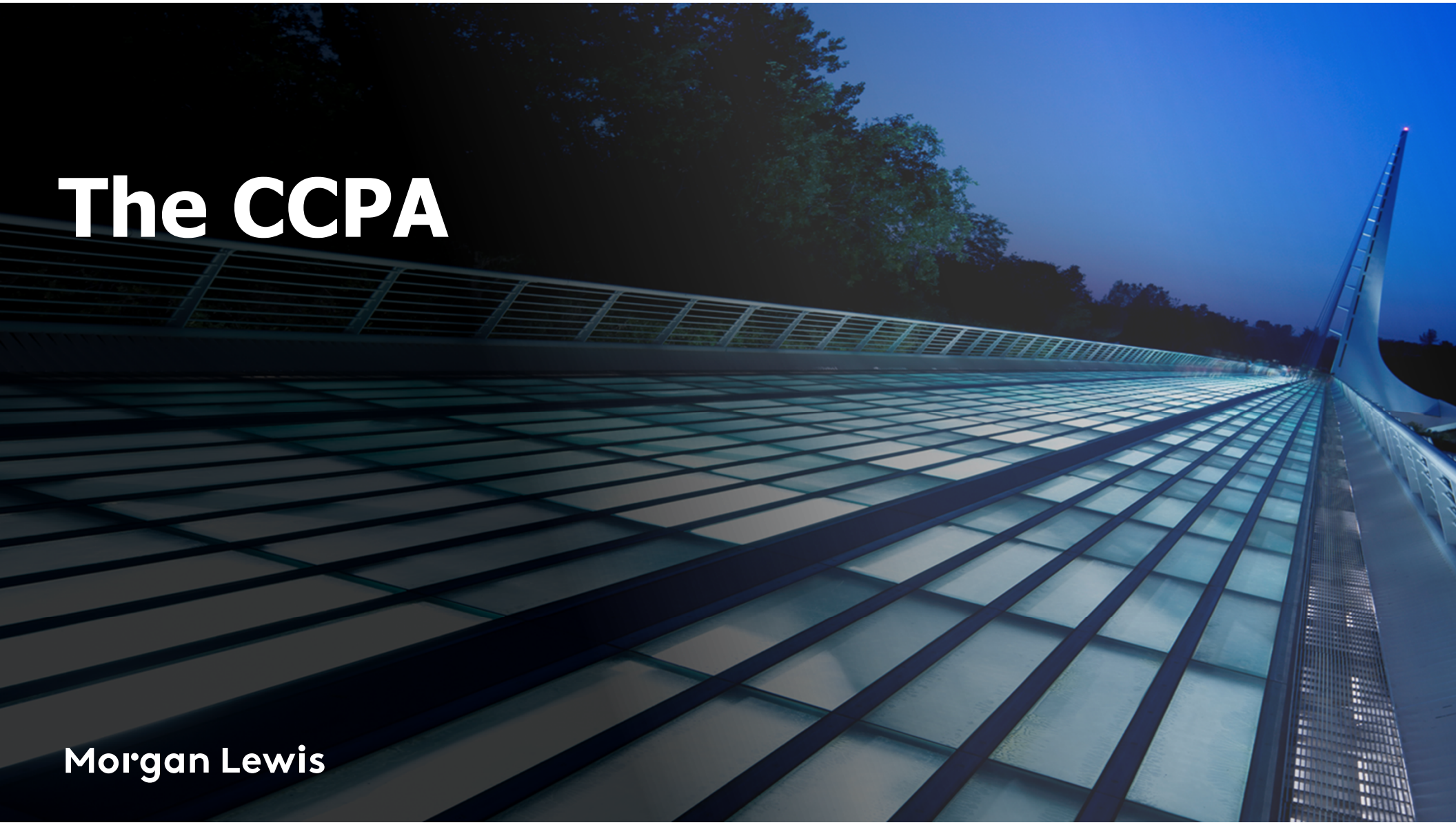
- New State Consumer Privacy Laws
  - California Consumer Privacy Act (CCPA)/California Privacy Rights Act (CPRA)
  - Virginia's Consumer Data Protection Act
  - Colorado's Privacy Act
  - Utah's Consumer Privacy Act
  - Connecticut's Data Privacy Act
- Comparison of data privacy laws in California, Virginia, Colorado, Utah, and Connecticut
- Consumer privacy compliance in the current environment
- The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

New State Consumer Privacy Laws

Morgan Lewis

New State Privacy Laws—Moving Closer to GDPR

- The CCPA incorporates elements from
  - GDPR
  - Existing California privacy laws like California Online Privacy Protection Act and California Civil Code 1798.81.5 (California's "reasonable security" law)
- California Privacy Rights Act (CPRA) adds additional privacy protections more closely aligned with GDPR
- Other new state-privacy laws generally follow the CCPA/CPRA template, with some variations
- The California Privacy Protection Agency has issued draft CPRA regulations that provide a glimpse into where privacy regulation is likely headed in California and, by extension, the United States


The CCPA
Morgan Lewis

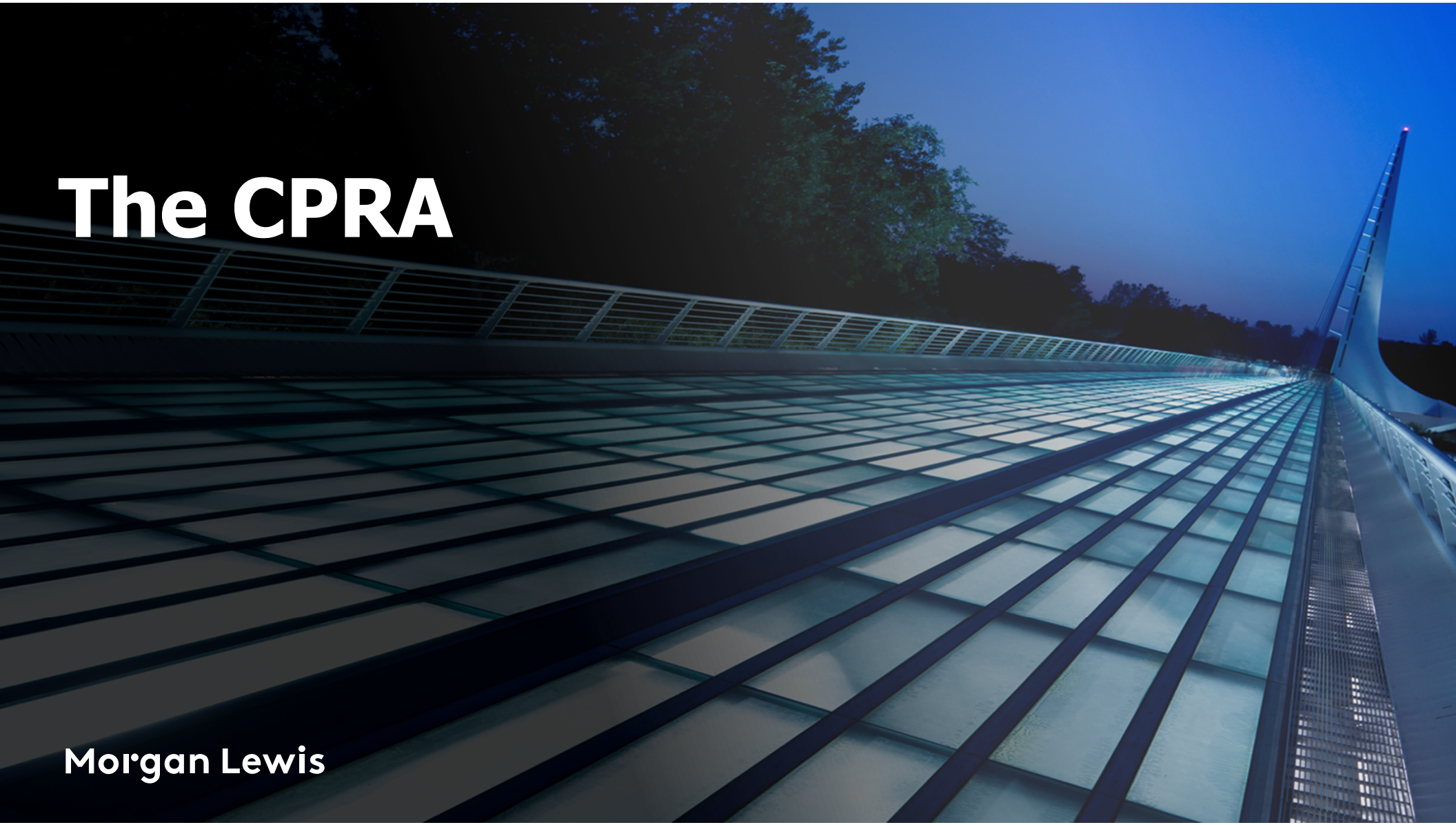
CCPA Privacy Rights Overview

Right to know specific pieces of personal information (PI) collected about the consumer in the preceding 12 months

Right to delete personal information

Right to opt out of sale of personal information

Right to a website privacy policy that describes how to exercise these privacy rights


The CPRA
Morgan Lewis

California Privacy Rights Act (CPRA)

CPRA "CCPA 2.0" ballot initiative passed on Nov. 3, 2020 (effective Jan. 2023, with enforcement commencing July 1, 2023)

- Adds protections for "sensitive personal information"
- Adds right to opt out of "sharing" of data, not just "selling" of data
  - "Sharing" includes cross-context behavioral advertising
- Adds the right to correct inaccurate PI
- CCPA's partial exceptions for employees, applicants, officers, directors, contractors, and business representatives extended, but will expire Jan. 1, 2023
- Extends lookback period for requests to know beyond 12 months

California Privacy Rights Act (CPRA) (cont.)

- Adds requirements for businesses to protect PI
  - Minimizing data collection
  - Limiting data retention
  - Protecting data security
  - Performing privacy risk assessments and cybersecurity audits
- Expands the private right of action to cover (1) nonredacted and nonencrypted information, ***and*** (2) email addresses with a password or security question and answer that would permit access to the account (*this second category is new*)
  - **NEW:** Security measures implemented after a breach do not constitute a cure of that breach
- Establishes California Privacy Protection Agency to enforce CCPA/CPRA

CPRA Privacy Rights Overview

Right to know categories and specific pieces of personal data collected about the consumer

Right to correct inaccuracies in personal data

Right to delete personal data

Right to opt out of the sale and sharing of personal data

Right to limit use of sensitive personal data

Behavioral Advertising Opt-Out

- CPRA expands consumer right to opt out to include "sharing" as well as "sale"
- New definition of "sharing" includes sharing, renting, transferring, or communicating PI to a third party for "cross-context behavioral advertising"
  - Whether or not for monetary or other valuable consideration
- "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded websites, applications, or other services
  - OTHER THAN the business, distinctly branded website, application, or service with which the consumer intentionally interacts
- CPRA regulations provide that an entity that contracts with a business to provide targeted ads cannot be a service provider, and that sharing is subject to the opt-out for sale of PI

Privacy Notice

CPRA regulations require that the CCPA privacy notice must list the names of ***all*** third parties that the business allows to collect PI from the consumer

Including the names of all third parties who set cookies on the business's website

CPRA regulations also require that the privacy notice specify the length of time that the business intends to retain ***each category of PI***

If that is not possible, the privacy notice must state the criteria used to determine the period for which it will be retained

CCPA/CPRA—Employment and B2B Exceptions

- The CPRA extends the CCPA's exceptions for employment and B2B data until January 1, 2023.
- Bills to extend the exceptions beyond January first failed to pass.
- Therefore, unlike the other state consumer privacy laws, starting January 1, consumer privacy rights under CCPA/CPRA will be available to all Californians, including employees, contractors, candidates, and B2B contacts.

Virginia's Consumer Data Protection Act

Morgan Lewis

Virginia's Consumer Data Protection Act (CDPA)

- Virginia's privacy law will go into effect on January 1, 2023
- The CDPA will apply to businesses that:
  - Operate in Virginia or produce products or services that are targeted to Virginia residents and that either:
    - Control or process the personal data of at least 100,000 Virginia residents during a calendar year, or
    - Control or process the personal data of at least 25,000 Virginia residents and derive at least 50% of their gross revenue from the sale of personal data
- Applies to brick-and-mortar businesses, not just the collection of personal data electronically or over the internet
- Does not apply to employment-related data or B2B transaction data

Virginia Privacy Rights Overview

- Right to access personal data
- Right to correct inaccuracies in personal data
- Right to delete personal data
- Right to data portability
- Right to opt out of targeted advertising and sale of personal data
- Consumer right to appeal a controller's response to a consumer request

Enforcement of Virginia's Privacy Law

- **There is no private right of action under the CDPA (even for data breaches)**
- **The VA Attorney General will have exclusive authority to enforce the CDPA, subject to a 30-day cure period**
- **Violators are subject to civil penalties of up to $7,500 for each violation**

Colorado's Privacy Act

Morgan Lewis

The Colorado Privacy Act (CPA)

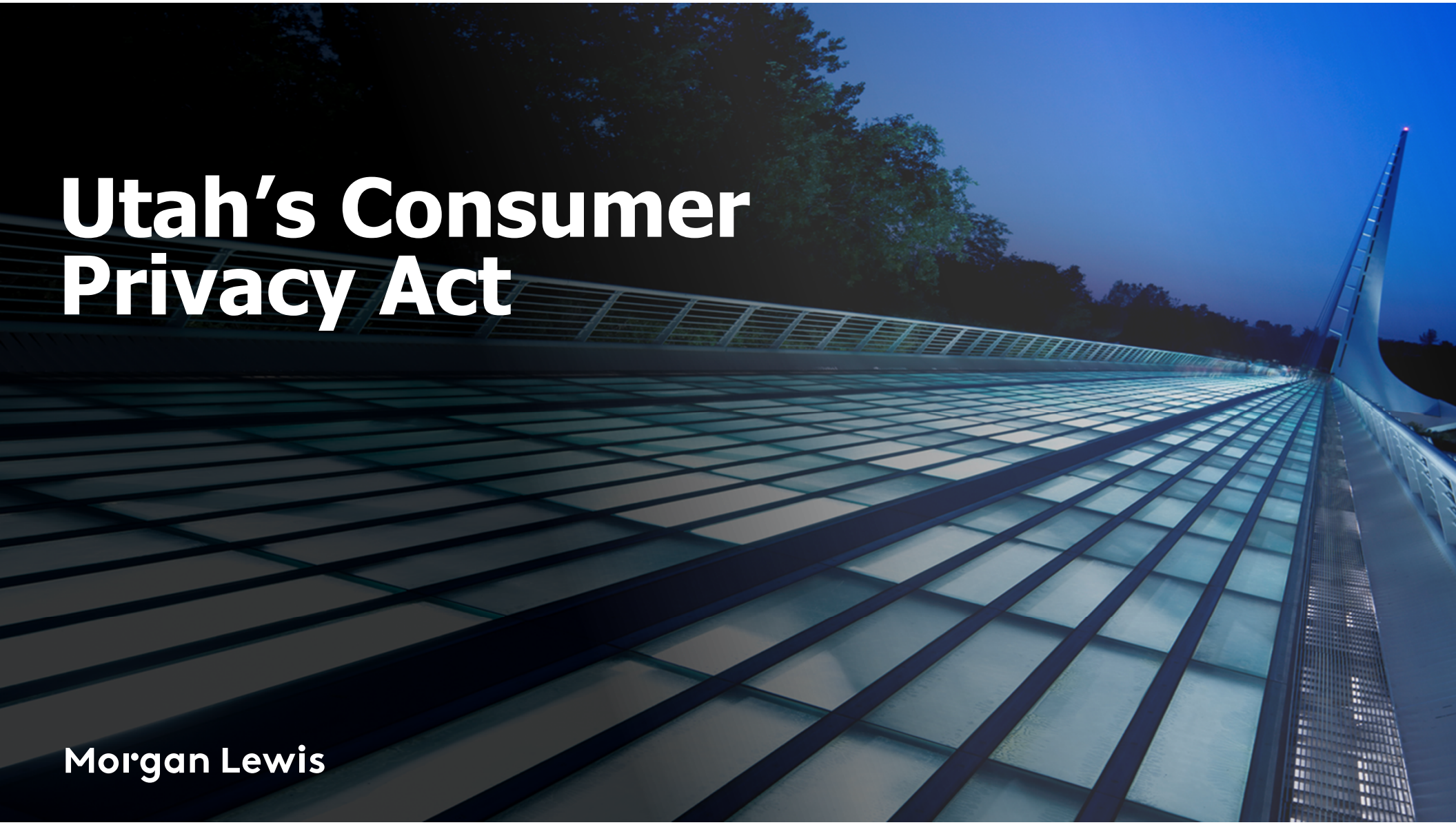
- Colorado's privacy law will go into effect on July 1, 2023
- The CPA will apply to businesses that:
  - Conduct business in Colorado or produce or deliver commercial products or services that are intentionally targeted to residents of Colorado and:
    - Control or process the personal data of at least 100,000 Colorado residents during a calendar year, or
    - Derive revenue or receive a discount on the price of goods or services from the sale of personal data and process or control the personal data of 25,000 consumers or more.
- Grants attorney general rulemaking powers
- Does not apply to employment-related data or B2B transaction data
- Exempts customer data maintained by a public utility if the data are not collected, maintained, disclosed, sold, communicated, or used, except as authorized by state and federal law

Colorado Privacy Rights Overview

- Right to access personal data
- Right to correct inaccuracies in personal data
- Right to delete personal data
- Right to data portability
- Right to opt out of targeted advertising and sale of personal data
- Consumer right to appeal a controller's response to a consumer request

Enforcement of Colorado's Privacy Law

- There is no private right of action under the CPA
- Provides for broad enforcement authority to the CO Attorney General and district attorneys, subject to a 60-day cure period
- Violators are subject to civil penalties of up to $20,000 for each violation



Utah's Consumer Privacy Act

Morgan Lewis

The Utah Consumer Privacy Act (UCPA)

- Utah's privacy law will go into effect on December 31, 2023
- The UCPA will apply to businesses that:
  - Conduct business in Utah or produce a product or service targeted to Utah residents;
  - Have annual revenue of $25 million or more; ***and either:***
    - Control or process the personal data of at least 100,000 Utah residents during a calendar year, or
    - Derive more than 50% of gross revenue from the sale of personal data and control or process personal data of 25,000 consumers or more.
- Does not apply to employment-related data or B2B transaction data
- No requirement that businesses conduct data-protection assessments

Utah Privacy Rights Overview

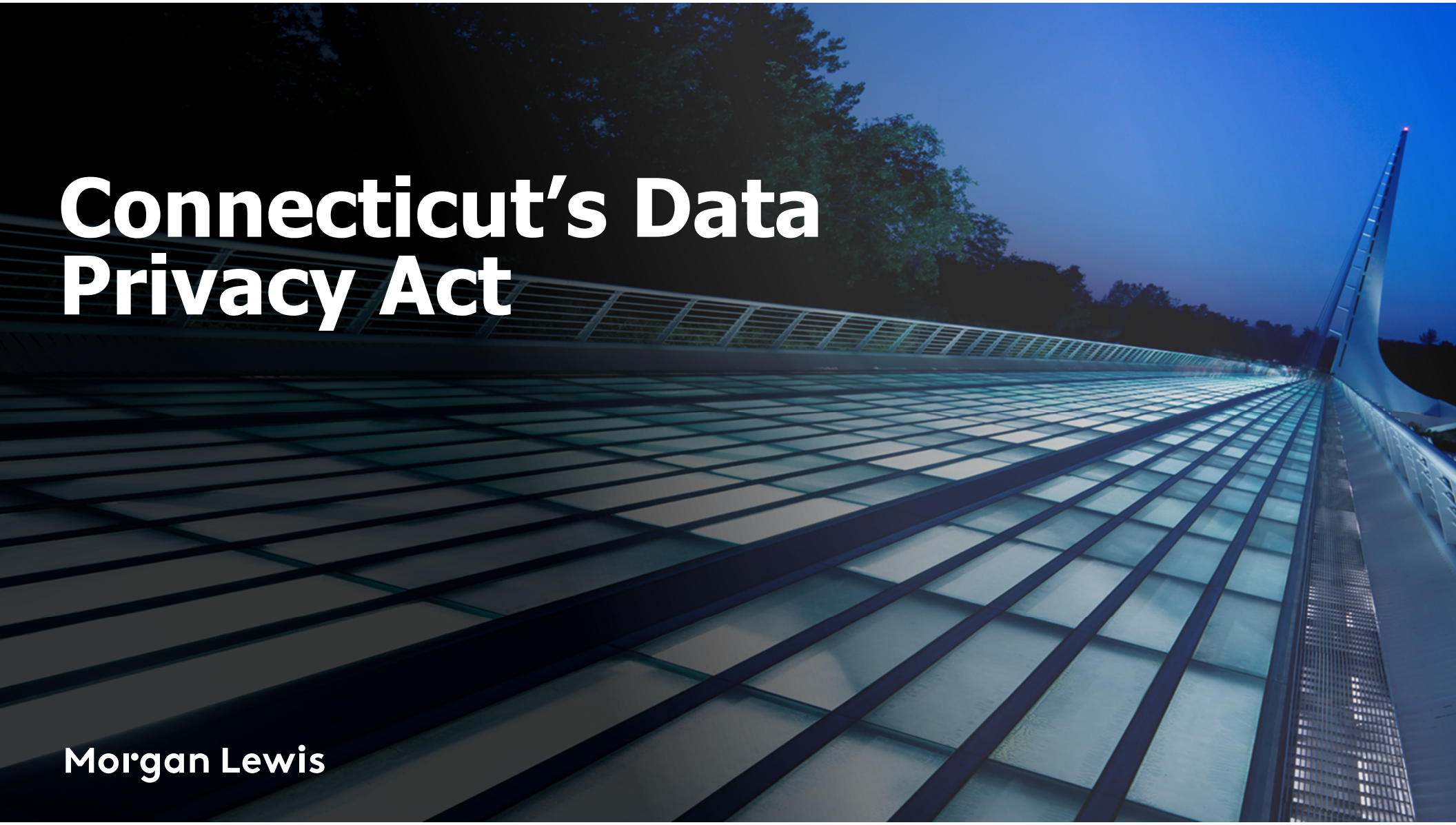
- Right to access personal data
- Right to delete personal data that the consumer provided to the controller
- Right to data portability that the consumer provided to the controller
- Right to opt out of targeted advertising and sale of personal data
- No right to correct inaccuracies in personal data
- No requirement that controllers provide appeals process

Enforcement of Utah's Privacy Law

There is no private right of action under the UCPA

Provides for broad enforcement authority to the UT Attorney General, subject to a 30-day cure period

Violators are subject to civil penalties of up to $7,500 for each violation



Connecticut's Data Privacy Act

Morgan Lewis

The Connecticut Data Privacy Act (CTDPA)

- Connecticut's privacy law will go into effect on July 1, 2023
- The CTDPA will apply to businesses that:
  - Conduct business in Connecticut or produce or deliver commercial products or services that are intentionally targeted to residents of Connecticut and:
    - Control or process the personal data of at least 100,000 Connecticut residents during a calendar year, *excluding residents whose personal data is controlled or processed solely for the purpose of completing a payment transaction*; or
    - Control or process the personal data of 25,000 or more Connecticut residents, or where the business derives more than 25% of their gross revenue from the sale of personal data.
- Does not apply to employment-related data or B2B transaction data
- Does not apply to nonprofits

Connecticut Privacy Rights Overview

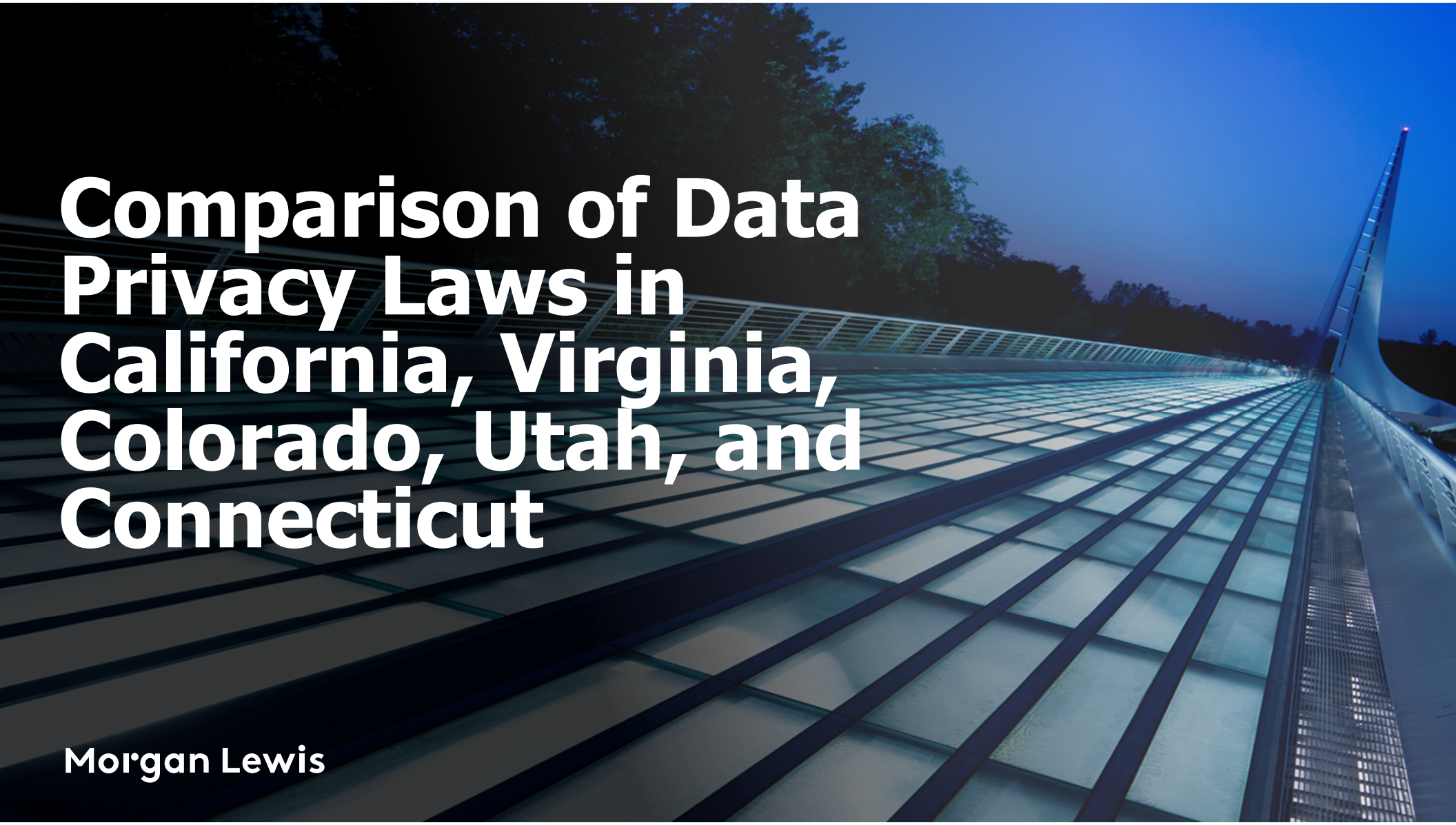
- Right to access personal data
- Right to correct inaccuracies in personal data
- Right to delete personal data
- Right to data portability
- Right to opt out of targeted advertising and sale of personal data
- Right to appeal a controller's response to a consumer request

Enforcement of Connecticut's Privacy Law

There is no private right of action under the CTDPA

Provides for broad enforcement authority to the CT Attorney General, subject to a 60-day cure period (cure period sunsets December 31, 2024)

Violators are subject to civil penalties of up to $5,000 for each willful violation



Comparison of Data Privacy Laws in California, Virginia, Colorado, Utah, and Connecticut

Morgan Lewis

Data Subject Rights

DATA SUBJECT RIGHTS	CT DPA	UT UCPA	CO CPA	VA CDPA	CA CCPA	CA CPRA
Access	Yes	Yes	Yes	Yes	Yes	Yes
Correct	Yes	No	Yes	Yes	No	Yes
Delete	Yes (data provided by or obtained about consumer)	Yes (data collected from consumer)	Yes (data concerning consumer)	Yes (data provided by or obtained about consumer)	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes	Yes	Yes	Yes
Opt-Out of Sale	Yes	Yes	Yes	Yes	Yes	Yes
Opt-Out of Sharing/Targeted Advertising	Yes	Yes	Yes	Yes	No	Yes
Non-Discrimination	Yes	Yes	Yes	Yes	Yes	Yes
Appeals Process	Yes	No	Yes	Yes	No	No

Controller Obligations

Controller Obligations	CT DPA	UT UCPA	CO CPA	VA CDPA	CA CCPA	CA CPRA
Data Minimization	Yes	Yes	Yes	Yes	No	Yes
Purpose Limitation	Yes	Yes	Yes	Yes	Yes	Yes
Security Requirements	Yes	Yes	Yes	Yes	No	Yes
Special Requirements for Children's Data	Yes (sensitive data of children under 13 years of age)	Yes (sensitive data of children under 13 years of age)	Yes (sensitive data of children under 13 years of age)	Yes (sensitive data of children under 13 years of age)	Yes (sale of PI of children under 16 and 13 years of age)	Yes (sale of PI of children under 16 and 13 years of age)
Privacy Notice	Yes	Yes	Yes	Yes	Yes	Yes
Data Protection Assessment	Yes	No	Yes	Yes	No	Yes – submitted to the CA Privacy Protection Agency

Responding to Consumers' Requests to Know

- All of the state consumer-privacy laws require controllers to respond within 45 days of receipt of an authenticated consumer request, which may be extended for an additional 45 days if reasonably necessary
- The Virginia, Colorado, and Connecticut laws also obligate controllers to establish a process for consumers to appeal the refusal to take action on a request
  - Controllers must respond within 45 days (CO) or 60 days (VA, CT) of the receipt of a consumer appeal
  - Under the Virginia and Connecticut laws, if the appeal is denied, the controller must inform the consumer how they can submit a complaint to the state attorney general

Responding to Consumers' Requests to Know, cont.

- There is no comparable mandatory appeal process in the CCPA, the CPRA, or the UCPA
  - Instead, the CCPA and CPRA require businesses that don't take action on a consumer request to inform the consumer of the reasons for not taking action and of any rights the consumer *may* have to appeal the decision
  - The UCPA requires businesses that don't take action on a consumer request to inform the consumer of the reasons for not taking action, but it does not require businesses to inform consumers of appeal rights
- While the CPRA does not come into effect until Jan. 1, 2023, consumer requests to access data can "look back" at data collected by a business on or after Jan. 1, 2022

Sensitive Data

- The laws in Virginia, Colorado, and Connecticut prohibit the processing of sensitive data without first obtaining the consumer's consent
  - "Sensitive data" includes (1) personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (2) processing of genetic or biometric data for the purpose of uniquely identifying a person; (3) personal data collected from a known child; and (4) precise geolocation data
  - "Consent" means a "clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement" to process personal data
- The CPRA and UCPA contain no comparable opt-in requirement
- Consumers have the right to limit the use of their sensitive personal information by submitting a request to a business under the CPRA and UCPA

Advertising

- The Virginia, Colorado, Utah, and Connecticut laws grant consumers the right to opt out of, and require controllers to disclose, the processing of personal data for purposes of targeted advertising
  - "Targeted advertising" means "displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from a consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests"
- There is no comparable requirement in the CCPA
- The CPRA addresses "cross-context behavioral advertising," which means the "targeting of advertising to a consumer based on the consumer's personal information 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"
- The CPRA treats the sharing of personal information for the purpose of cross-context behavioral advertising in the same way as a "sale" of personal information under the CCPA

Consumer Privacy Compliance in the Current Environment

Morgan Lewis

Practical Compliance

- Educate leadership about how this will evolve.
- Invest in teams and technology to be able to scale up on requests.
- Think about impact of employee rights in other contexts: litigation, labor disputes, and job satisfaction.
- Businesses that have been building compliance programs for CCPA will have a strong foundation for compliance with other state laws, but compliance programs will require updating.

The Cyber Incident Reporting for Critical Infrastructure Act of 2022

Morgan Lewis

New Law for Cyber Incident Reporting

- In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), Public Law 117–103, Div. Y
  - Establishes long awaited federal framework for incident reporting
  - To be codified at 6 U.S.C. §§ 681-681g
- Requires owners and operators of critical infrastructure to report cyber incidents and ransom payments to CISA
  - CISA is tasked with developing regulations to fill in the gaps
- Reporting is mandatory and subject to enforcement
  - 72-hour deadline for covered cyber incidents; 24-hour deadline for ransom payment
  - CIRCIA gives CISA subpoena power and other enforcement tools

Applicability

- CISA must complete rulemaking activities to define scope of requirements
- "Covered entity"
  - An entity in one of the 16 critical infrastructure sectors defined in PPD-21
- "Covered cyber incident"
  - Statute includes threshold criteria (e.g., loss of availability of information system or network, impact on the safety and resiliency of operational systems and processes)

Reporting Timelines

Covered cyber incident

- "A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity ***reasonably believes*** that the covered cyber incident has occurred."

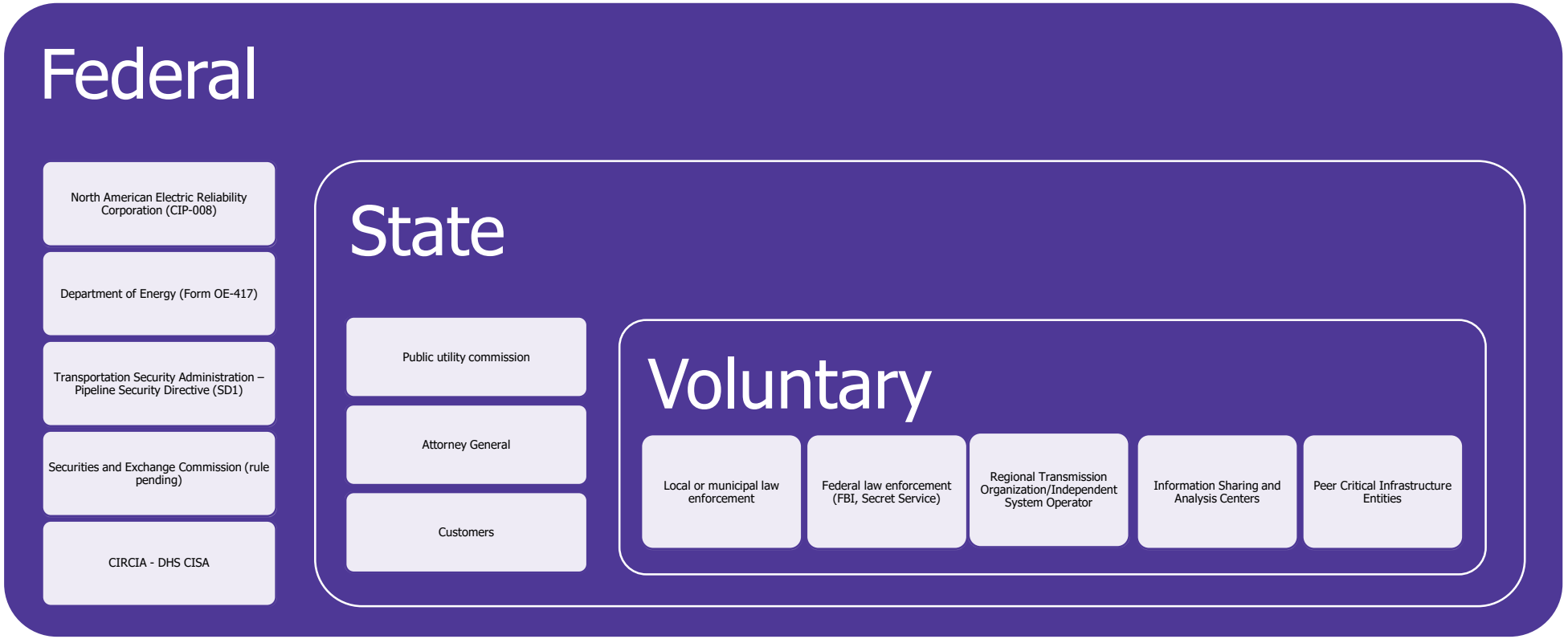
Ransomware payment

- "A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours ***after the ransom payment has been made***."

CISA Implementation

- Regulations are under development
- Key open issues
  - Gating definitions ("covered entity", "covered cyber incident", "reasonable belief")
  - Determining "when the clock starts"
  - Harmonization with other regulatory requirements
  - Supply-chain compromise/third-party suppliers
  - Use of information by federal entities
  - Data protections

Stacking Incident Reporting Requirements



Protections for Covered Entities

- Liability protections
  - "No cause of action shall lie or be maintained in any court . . . for the submission of a report . . . that is submitted *in conformance with this subtitle*"
- Confidentiality of submitted information
  - FOIA-exempt
  - Considered commercial, financial, and proprietary information of covered entity when so designated
  - No waiver of any privilege or legal protection
  - Not subject to any *ex parte* rule of any federal agency or judicial doctrine

Implications for Third-Party Providers

- Reportable incidents must include unauthorized access or operational disruption due to loss of service from:
  - Cloud service provider;
  - Managed service provider;
  - Other third-party data hosting provider; or
  - Supply-chain compromise.
- Third-party submitter
  - CIRCIA allows a covered entity to use a third party, such as an incident-response company, insurance provider, service provider, or law firm, to submit required reports.

Enforcement

- CIRCIA grants CISA broad enforcement authority
- Subpoena power
  - If unable to obtain information directly from covered entity within 72 hours, director may issue a subpoena to "gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred"
- Civil action
  - Director can refer to Attorney General to bring civil action in US District Court
- Referral for regulatory enforcement
  - CISA can refer to other federal regulators if it determines that information gained in response to subpoena "may constitute grounds for a regulatory enforcement action or criminal prosecution"

Next Steps

- CISA formalizing rulemaking
  - Formal request for information (RFI) concluded on November 14, 2022
- CISA is continuing "listening sessions" to solicit feedback from public and stakeholders
- Implementation
  - CISA to publish Notice of Proposed Rulemaking (NPRM) by March 2024
  - Final rule must be issued within 18 months after publication of NPRM

Biography

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

Kristin M. Hadgis counsels and defends retail and other consumer-facing companies in matters relating to privacy and cybersecurity, class actions, Attorney General investigations and enforcement actions, the California Consumer Privacy Act, consumer protection laws, retail operations, loyalty and gift card programs, and commercial disputes. Kristin also handles data security incident response crisis management, including any resulting litigation or government investigations.

Biography

J. Daniel Skees
Washington, D.C.
+1.202.739.5834
daniel.skees@morganlewis.com

J. Daniel Skees represents electric utilities before the Federal Energy Regulatory Commission (FERC) and other agencies on rate, regulatory, and transaction matters. He handles rate and tariff proceedings, electric utility and holding company transactions, utility financing, electric markets and trading issues, reliability standards development and compliance, including cybersecurity requirements, administrative litigation, and transmission development. In handling appeals of FERC decisions, Dan has successfully represented clients before both the US Court of Appeals for the District of Columbia Circuit and the US Court of Appeals for the Fifth Circuit. He currently serves as a deputy practice group leader for the firm's energy and project development practice.

Biography

Catherine North Hounfodji
Houston, TX
+1.713.890.5120
catherine.hounfodji@morganlewis.com

Catherine North Hounfodji regularly counsels clients on retail, ecommerce, logistics, and privacy matters, as well as compliance related to COVID-19 restrictions. In addition to her counseling practice, Catherine has more than 10 years of experience litigating commercial disputes and defending against wage and hour, healthcare, and tort claims.

Biography

Arjun Prasad Ramadevanahalli
Washington, D.C.
+1.202.739.5913
arjun.ramadevanahalli@morganlewis.com

Arjun Prasad Ramadevanahalli represents electric power, natural gas, and oil industry participants in regulatory and transactional matters. He assists clients on issues regarding wholesale markets, utility transactions, rate matters, and enforcement proceedings before the Federal Energy Regulatory Commission (FERC), and on cybersecurity matters in the energy industry. Arjun regularly advises utilities and other industry participants on North American Electric Reliability Corporation (NERC) reliability standards enforcement and compliance matters, including cybersecurity compliance and controls under the Critical Infrastructure Protection (CIP) suite of standards. Arjun counsels pipeline owners and operators on cybersecurity compliance before the Transportation Security Administration (TSA).

Biography

Terese M. Schireson
Philadelphia, PA
+1.215.963.4830
terese.schireson@morganlewis.com

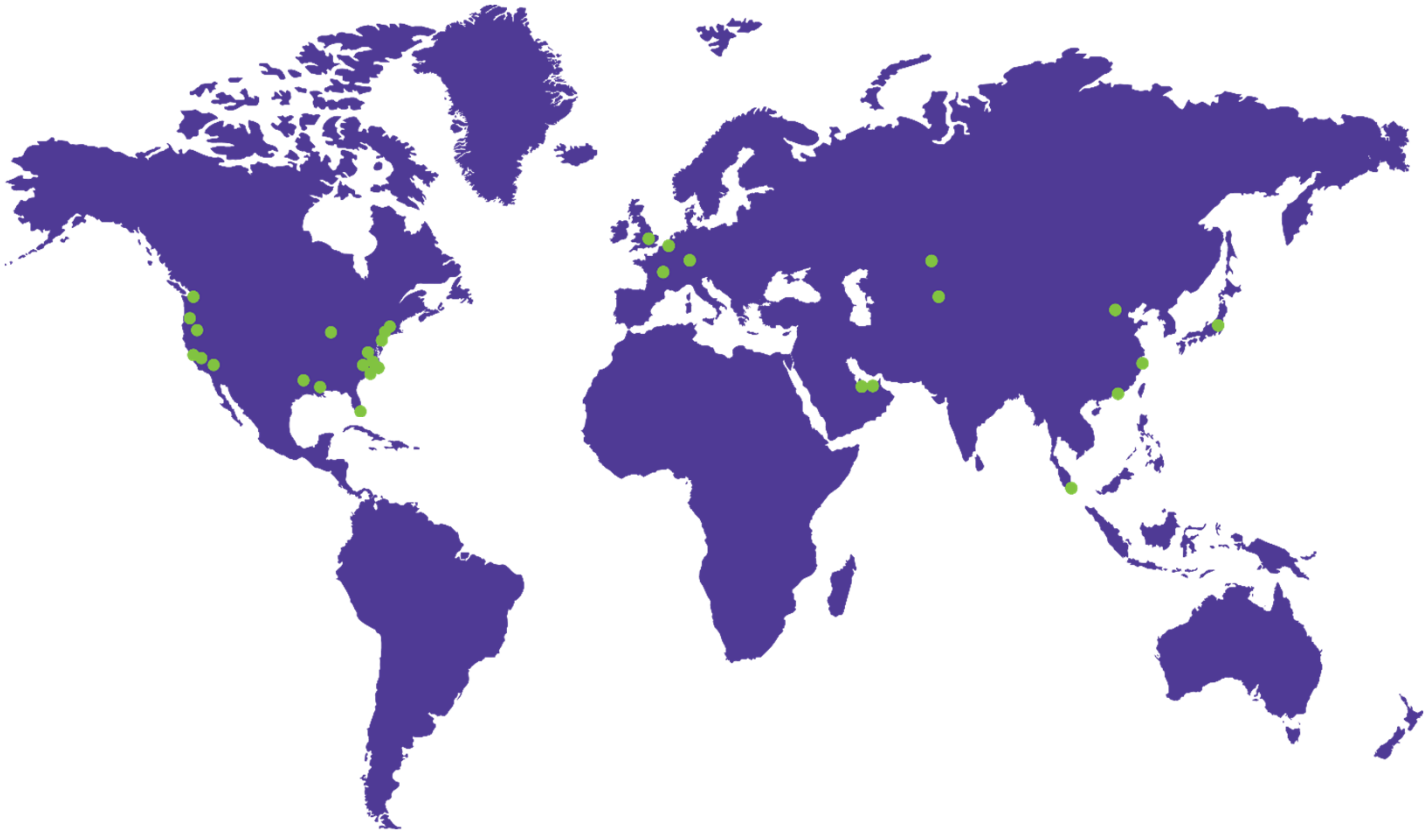
Terese M. Schireson represents clients in diverse areas, including privacy and cybersecurity, class action litigation, and complex commercial disputes, in state and federal courts across the country. She primarily counsels and defends clients in matters relating to compliance with new consumer privacy laws, data security incident response, and any related litigation or government investigations.

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
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU