

Morgan Lewis

TECHNOLOGY MARATHON

New State Consumer Privacy Laws

Greg Parks, Reece Hirsch, Mark Krotoski, Kristin Hadgis,
Terese Schireson, and William P. Childress, III

Wednesday, June 8, 2022

Presenters



W. Reece Hirsch



Gregory T. Parks



Mark L. Krotoski



Kristin M. Hadgis



Terese M. Schireson



William P. Childress, III

Morgan Lewis

Agenda

- Latest draft CCPA/CPRA regulations
- The California Privacy Rights Act
- Virginia's Consumer Data Protection Act
- Colorado's Privacy Act
- Utah's Consumer Privacy Act
- Connecticut's Data Privacy Act
- Comparison of privacy laws in California, Virginia, Colorado, Utah and Connecticut
- Compliance best practices in an evolving privacy landscape
- What is next in privacy legislation

The CCPA



Morgan Lewis

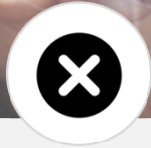
Moving Closer to GDPR

- 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
- On May 27, the California Privacy Protection Agency issued draft CPRA regulations that provide a glimpse into where privacy regulation is likely headed in California and, by extension, the United States

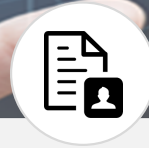
CCPA Privacy Rights Overview



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 Consumer 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 through January 1, 2023
- Extends lookback period for requests to know beyond 12 months

California Consumer Privacy Rights Act (CPRA) (cont.)

- Adds requirements for businesses to protect PI
 - Minimizing data collection
 - Limiting data retention
 - Protecting data security
 - 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 CPRA

Draft CPRA Regulations

On May 27, California Privacy Protection Agency released a preliminary draft of proposed CPRA regulations

At least a 45-day period for public comment

Agency is required to finalize CPRA Regulations by July 1, 2022

The Draft Regulations provide extensive guidance and make clear that the CPRA intends to build upon its already-stringent requirements

- Creating the most comprehensive, consumer-oriented privacy law in the United States

Given the many new concepts reflected in the Draft Regulations, there are likely to be modifications

Many CPRA topics are not addressed: employment and B2B data exceptions, cybersecurity audits, retention, and privacy risk assessments

Focus on Consumer-Friendly Privacy Options

- **Draft Regulations emphasize that methods for submitting CCPA requests and obtaining consumer consent must:**

- Be easy to understand
- Provide “symmetry in choice”

- **What is symmetry in choice?**

- Example: A choice to opt-in to the sale of personal information that provides the choices “Yes” and “Ask Me Later” is not equal or symmetrical because there’s no option to opt-out
- A symmetrical choice would be “Yes” or “No”

Avoid Dark Patterns

Draft Regulations require that privacy choices be “easy to execute,” not adding unnecessary burden or friction to a CCPA request process

- **Example:** When clicking a “Do Not Sell My Personal Information” link, the consumer should not be required to search or scroll through the entire privacy policy to locate the opt-out request mechanism
- Link should go directly to the opt-out provisions

Use of “dark patterns” will not constitute consumer consent

- A user interface is a dark pattern if it has the effect of substantially subverting or impairing user autonomy, decision making, or choice, regardless of the business’s intent
- **Example:** If a business offers choices in the order of “Yes” then “No”, it may be a dark pattern if the order is switched to “No” then “Yes” when asking the consumer to make a choice that would benefit the business

The Average Consumer's Expectations

- Draft Regulations provide that a business's collection, use, retention and/or sharing of a consumer's personal information must be reasonably necessary and proportionate to achieve the purposes for which the PI was collected or processed
 - Must be consistent with ***what the average consumer would expect*** when the PI was collected
- This standard becomes critical because the Draft Regulations require the consumer's explicit, opt-in consent before collecting, using, retaining, and/or sharing the PI for unrelated or incompatible purposes

Is the CPRA Moving From Opt-Out to Opt-In?

- Example: An online retailer collects PI from consumers who buy its products.
 - Retailer provides a consumer's name, address and phone number to a delivery company
 - Consistent with reasonable consumer expectations because it's necessary for shipping the product to the consumer
 - Retailer uses consumer's PI to market other business's products
 - This use of PI would not be necessary and proportionate, or compatible with the consumer's expectations
 - Retailer would have to obtain the consumer's **explicit consent** before engaging in this marketing activity
 - This is a significant departure from FTC privacy principles, which would generally permit a business to provide a privacy policy that informs the consumer of these sorts of marketing activities, without obtaining opt-in consent

Downstream Obligations

Draft Regulations expand the required terms for agreements between a business and service providers, contractors, and third parties

- **Example:** Businesses are strongly incentivized to conduct due diligence of service providers and contractors
- A business that never enforces the terms of the contract or exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intended to use PI in violation of the CCPA

Contracts with service providers and contractors must specify the business purpose for which PI is being disclosed

- A description "in generic terms" is not sufficient
- Could require amendment of certain downstream agreements

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
- Draft 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



Draft 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



Draft 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 it will be retained

Request-to-Know Lookback Period

- Consumer will have the right to make a request to know that extends earlier than 12 months preceding the request
 - Potentially extends lookback period to the start of the relationship with the consumer
 - Business must comply unless doing so “proves impossible or would involve a disproportionate effort”
- Draft Regulations provide that if a business determines that looking back beyond 12 months is impossible or involves disproportionate effort, such business:
 - Must provide the consumer with a “detailed explanation” that includes enough facts to give the consumer a meaningful understanding of the business’s decision
 - Cannot simply state that it is impossible or requires disproportionate effort

Status of Employment and B2B Exceptions

- The CPRA extends the CCPA's exceptions for employment and B2B data until January 1, 2023
- What happens after January 1?
- Two California bills would extend the exceptions
 - AB 2891: extension until January 1, 2026
 - AB 2871: would permanently codify exceptions
- Extension of the exceptions would be consistent with other new state consumer-privacy laws
- CPRA provides that any legislative amendment "must be consistent with and further the purpose and intent of the CPRA," which raises the possibility of a court challenge
- Hopefully, picture will become clearer by the end of the 2022 California legislative session on August 31

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




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
- Applies to non-profit entities

Colorado Privacy Rights Overview



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



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




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 | No | No | No | No | 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 |

Sensitive Data

- The laws in Virginia, Colorado, and Connecticut prohibit 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

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 a 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 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 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



Compliance in the Current Environment

Morgan Lewis

Practical Compliance

- January 1, 2023, is a long time away, but so were January 1, 2020 and May 25, 2018.
- Use the runway available, but not just to wait. Try things out.
- Recognize that the landscape is going to change, so do not finalize until next year.
- 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.

Looking Ahead



Morgan Lewis

What's Next in Privacy Legislation?

◆ WSJ NEWS EXCLUSIVE **TECH**

Congress to Take Another Swing at Privacy Legislation **March 25, 2022**

House and Senate aides expected to meet in another bid to forge a bill to put restrictions on data gathering

TECH

Online Privacy Protections Gain Traction With Lawmakers, Tech Industry **April 26, 2022**

Disclosures of social-media harms to young people put pressure on Congress, tech companies to safeguard personal information

What's Next in Privacy Legislation?

TECHNOLOGY

Bipartisan draft bill breaks stalemate on federal data privacy negotiations

Leaders of key House and Senate committees have compromised in a draft bill released today.



What's Next in Privacy Legislation?



Federal action?

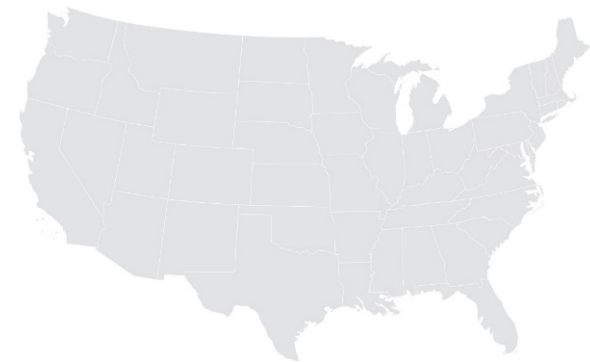
- The United States still does not have an all-encompassing federal data privacy law
- Several federal bills have been proposed over the years, but none have been successful
- **American Data Privacy Protection Act** introduced in May 2022 has bipartisan support
 - Limited private right of action and limited pre-emption
 - Chances for passage are unclear as it appears to lack key support

What's Next in Privacy Legislation?

Nearly a dozen states are actively debating a comprehensive privacy law



- Debate, however, does not guarantee that a law will pass
- In 2021, the **Washington Privacy Act** bill failed for the third straight year



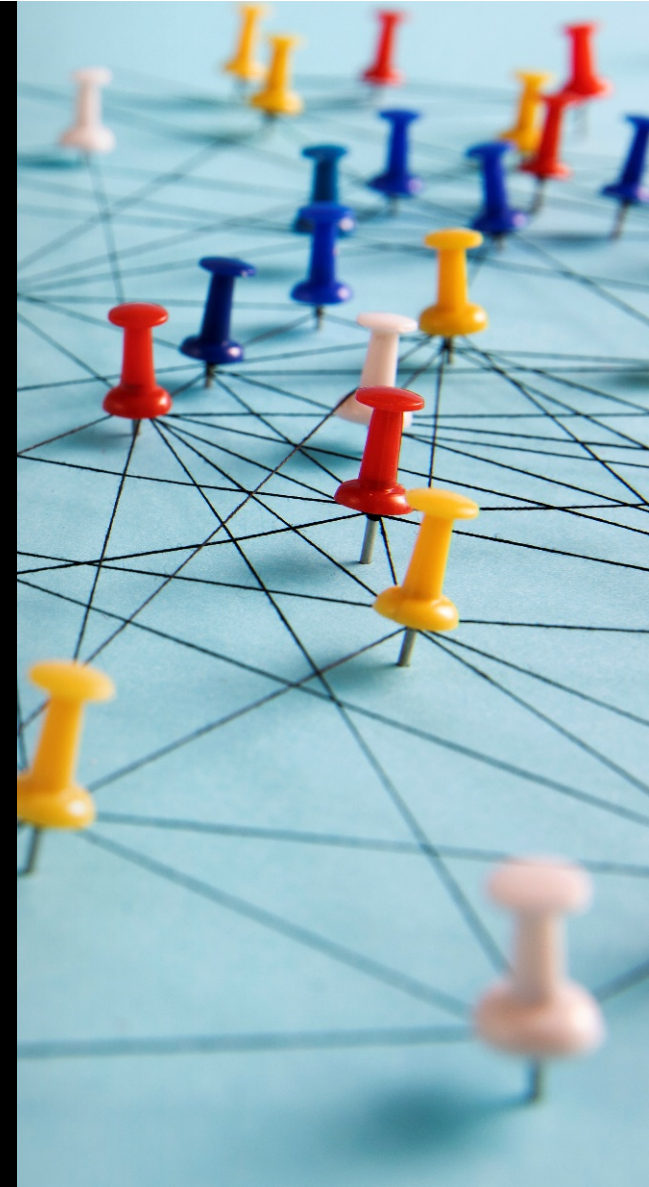
Ukraine Conflict Resources

Our lawyers have long been trusted advisers to clients navigating the complex and quickly changing global framework of international sanctions. Because companies must closely monitor evolving government guidance to understand what changes need to be made to their global operations to maintain business continuity, we offer a centralized portal to share our insights and analyses.

Morgan Lewis

To help keep you on top of developments as they unfold, visit the website at www.morganlewis.com/topics/ukraine-conflict

To receive a daily digest of all updates, please visit the resource page to **subscribe** using the "Stay Up to Date" button.



W. REECE HIRSCH



W. Reece Hirsch

San Francisco

+1.415.442.1422

reece.hirsch@morganlewis.com

W. Reece Hirsch co-heads the firm's privacy and cybersecurity practice and counsels clients on a wide range of US privacy issues, specializing in healthcare privacy and digital health. Reece counsels clients on development of privacy policies, procedures and compliance programs, security incident planning and response, and online, mobile app, and Internet of Things privacy. Reece counsels clients in healthcare privacy and security matters, such as compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, state medical privacy laws, and Federal Trade Commission standards applicable to digital health companies. He has represented clients from all sectors of the healthcare industry on privacy and security compliance, including health plans, insurers, hospitals, physician organizations, and healthcare information technology, digital health, pharmaceutical, and biotech companies. Reece also advises clients on privacy issues raised by the coronavirus (COVID-19) pandemic, including those relating to workplace testing, HIPAA waivers and enforcement discretion, contact tracing, telehealth, and work-from-home and return-to-work policies.

GREGORY T. PARKS



Gregory T. Parks

Philadelphia

+1.215.963.5170

gregory.parks@morganlewis.com

Co-leader of the firm's privacy and cybersecurity practice and retail & ecommerce sector, Gregory T. Parks counsels and defends consumer-facing clients in matters related to privacy and cybersecurity, class actions, Attorney General investigations and enforcement actions, the California Consumer Privacy Act, consumer protection laws, loyalty and gift card programs, retail operations, payment mechanisms, product liability, retail waste, shoplifting prevention, compliance, antitrust, commercial disputes, and a wide variety of other matters for retail, ecommerce, and other consumer-facing companies. Greg also handles data security incident response crisis management and any resulting litigation, and manages all phases of litigation, trial, and appeal work arising from these and other areas.

MARK L. KROTOSKI



Mark L. Krotoski

Silicon Valley

Washington DC

+1.650.843.7212

+1.202.739.5024

mark.krotoski@morganlewis.com

Mark L. Krotoski is a litigation partner in Morgan Lewis's privacy and cybersecurity and antitrust practices, bringing substantial and government leadership experience on these issues. Mark served as the National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the US Department of Justice (DOJ) in Washington, DC, and as a CHIP prosecutor in Silicon Valley, among other DOJ leadership positions. Mark successfully led investigations and prosecutions of nearly every type of computer intrusion, cybercrime, and criminal intellectual property violation for all types of major and small companies. He was an instructor on economic espionage and trade secret cases, cybersecurity, using electronic evidence in investigations and at trial, and other law enforcement issues at the DOJ National Advocacy Center.

KRISTIN M. HADGIS



Kristin M. Hadgis

Philadelphia

+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. Kristin has advised on more than 250 data breaches in her career, counseling clients on how best to give notice to affected individuals or government and consumer reporting entities, following proper compliance protocol. Kristin also represents these companies on any class action and other litigation stemming from the incidents, and instructs them on implementing policies and procedures to prevent and mitigate future breaches.

TERESE M. SCHIRESON



Terese M. Schireson

Philadelphia

+1.215.963.4830

terese.schireson@morganlewis.com

Terese M. Schireson represents clients in diverse areas, including complex commercial disputes, class action lawsuits, and white collar litigation, in state and federal courts throughout the United States. Terese also counsels consumer-facing clients on issues such as retail operations and compliance, marketing and advertising, and privacy and cybersecurity. Terese primarily assists clients in business litigation matters involving breach of contract, unfair competition, fraud, and consumer protection claims. She also has experience in qui tam actions brought under the False Claims Act. Terese serves clients across diverse industries, including the retail, energy, technology, and healthcare sectors.

WILLIAM CHILDRESS



William Childress

Philadelphia

+1.215.963.4999

william.childress@morganlewis.com

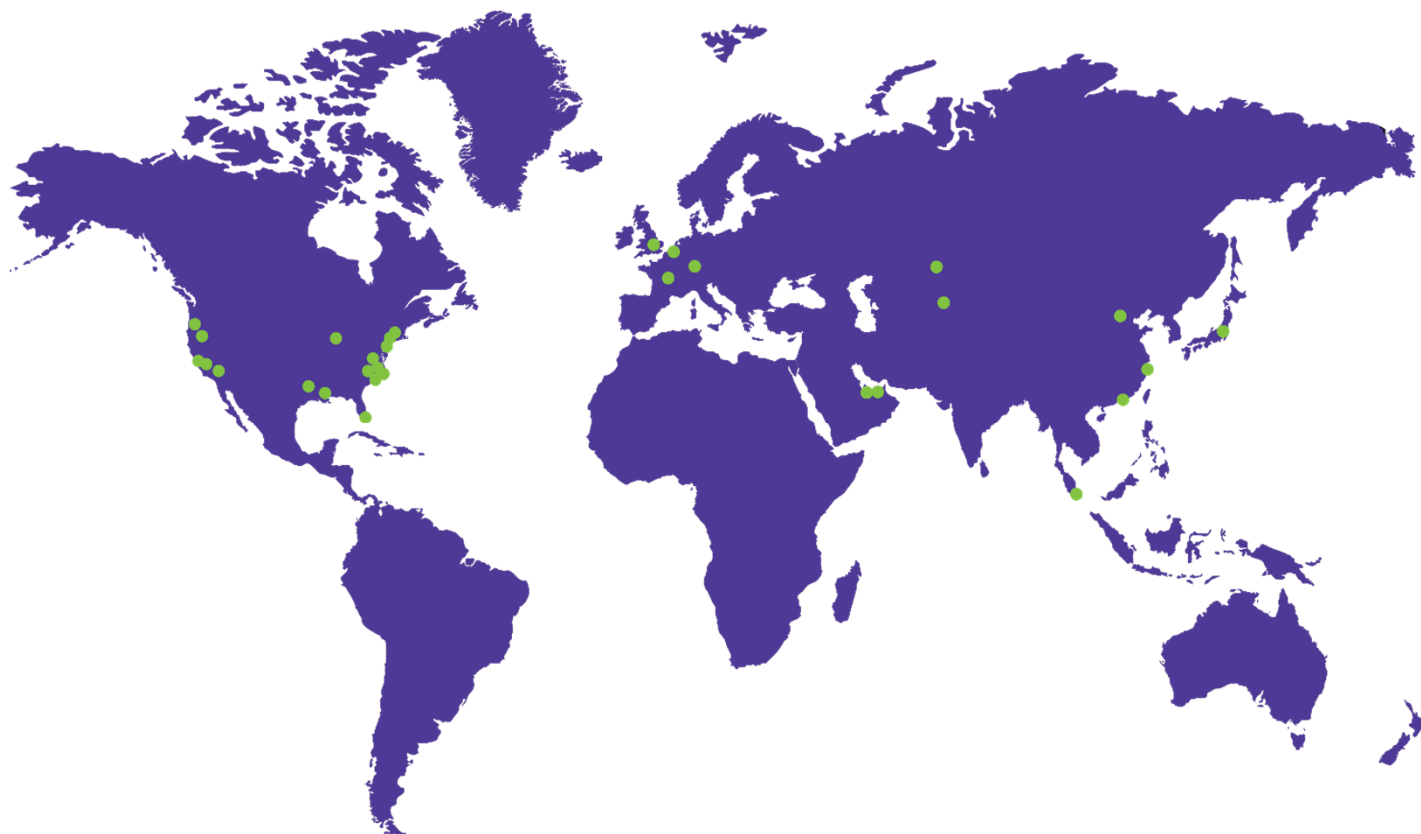
William Childress counsels clients on electronic discovery. William's practice focuses on negotiations with opposing counsel, motion practice related to discovery, and litigating discovery disputes. He has handled all phases of litigation. Prior to joining the firm, William clerked for Judge P. James Jones in the US District Court for the Western District of Virginia, worked as an associate in the litigation practice of an international law firm, and as a staff attorney for the Supreme Court of Virginia.

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
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 & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU

© 2022 Morgan, Lewis & Bockius LLP
© 2022 Morgan Lewis Stamford LLC
© 2022 Morgan, Lewis & Bockius UK LLP

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

Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan, Lewis & Bockius is a separate Hong Kong general partnership registered with The Law Society of Hong Kong. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.