Morgan Lewis

COMPLYING WITH NEWLY FINALIZED CCPA REGULATIONS

September 8, 2020

Presenters

W. Reece Hirsch

Andrew J. Gray IV

Morgan Lewis

Agenda

- Latest changes in the final CCPA regulations
- AB 1281 extending employment and B2B exemptions
- Proposition 24 (California Privacy Rights and Enforcement Act of 2020)
- Compliance and implementation hypotheticals and best practices
- Prospects for CCPA enforcement and litigation
- Implementing a CCPA compliance program during the pandemic

The Latest Developments: Final Regs, AB 1281, Prop 24

Morgan Lewis

The CCPA Is Final, And Enforcement Will Follow

- The CCPA regulations are now final, marking the beginning of a new era of US privacy regulation
  - California Attorney General can now enforce both the CCPA statute and regulations
- Despite petitioning from the business and technology communities, AG has given no indication that CCPA enforcement will be deferred during the COVID-19 pandemic
- CCPA builds upon other regulatory regimes such as GDPR, the FTC Act, and prior California privacy and security laws, but it presents its own unique compliance challenges

Businesses Subject to the CCPA

- A "business" subject to the CCPA must be a for-profit organization or legal entity that
  - Does business in California
  - Collects consumers' personal information, either directly or through a third party on its behalf
    - "Collects" is broadly defined to include "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means"
  - Either alone, or jointly with others, determines the purposes and means of processing of consumers' personal information
    - Resembles GDPR's "data controller" concept
- Business includes an entity that controls or is controlled by a business **if** it shares common branding with the business

Additional Criteria for Businesses

- A business must also satisfy one of three thresholds:
  (1) Annual gross revenues in excess of $25 million (does not appear to be limited to California revenues);
  (2) Annually buys, receives, sells or shares the personal information of 50,000 or more consumers, households, or devices, alone or in combination; **or**
  (3) Derives 50% or more of its annual revenue from selling consumers' personal information.
- Applies to brick-and-mortar businesses, not just the collection of personal information electronically or over the internet
- Does not apply to non-profits

CCPA Does Not Apply To …

- Medical information and entities subject to HIPAA or the California Confidentiality of Medical Information Act
- Personal information subject to the Gramm-Leach-Bliley (GLBA) or the California Financial Privacy Act
- Sale of personal information to or from a consumer reporting agency
- Personal information subject to the federal Driver's Privacy Protection Act
- Employment-related data
- B2B transaction data
- Vehicle information

CCPA Privacy Rights Overview

- Right to know specific pieces of personal information 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

How We Got Here: CCPA Regulations Timeline

- October 10, 2019: AG's office issues proposed CCPA regulations
  - Regs primarily address consumer privacy rights and do not address subsequent CCPA amendments, private right of action for security breaches, or enforcement
  - 45-day comment period ended on December 6, 2019
- February 7, 2020: AG's office issues first set of modifications to proposed CCPA regulations
- February 10, 2020: AG's office issued a slightly revised version of the modifications Proposed correct an omission in the February 7, 2020 version
  - Modifications address many topics, including definitions of "personal information" and "households," notices, affirmative authorization, responses to consumer requests, service providers, discriminatory practices, and privacy policies
  - 15-day comment period ended on February 25, 2020

CCPA Regulations Timeline (cont.)

- March 11, 2020: AG's office issues the second set of modifications to proposed regulations (amidst COVID-19)
  - Modifications primarily address definitions of "personal information" and "financial incentives," Do Not Sell button, privacy policy requirements, notice at collection requirements, service providers, and employment-related privacy notices
  - 45-day comment period ended on March 27, 2020
- March 30, 2020: Governor Gavin Newsom issues an Executive Order in response to COVID-19 providing the Office of Administrative Law (AOL), which normally has 30 working day review period, an additional 60 calendar days to review regulations

CCPA Regulations Timeline (cont.)

- AG's office made no further changes and submitted the regs to California's Office of Administrative Law (OAL) on June 1, 2020
  - OAL had an extended 60-day period per the March 30 Executive Order to review and confirm that administrative requirements were followed
- July 1, 2020: Enforcement date for CCPA statute (even though regulations have not yet been finalized by OAL)
- August 14, 2020: AG announces that final CCPA regulations have been approved by OAL and go into effect immediately
- As of August 14, businesses subject to the CCPA must now comply with both the statute and regulations

The Final CCPA Regulations

- Final regulations are similar to the proposed regulations submitted on June 1
  - But AG made several changes characterized as "non-substantive changes for accuracy, consistency, and clarity"
  - Several were substantive although likely not controversial
  - AG also withdrew certain provisions for "additional consideration"

- Four provisions were deleted that were included in the prior proposed regulations

Withdrawn: Express Consent to Materially Different Purpose

- Withdrawn Section 999.305(a)(5):
  - "A business shall not use a consumer's personal information for a purpose materially different than those disclosed in the notice at collection. If the business seeks to use a consumer's previously collected personal information for a purpose materially different than what was previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose."
  - Obtaining such an express notice to a materially different use of information remains consistent with FTC privacy standards

Withdrawn: Requiring Opt-out Notices Through an Offline Method

- Withdrawn Section 999.306(b)(2):
  - "A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include, but are not limited to, printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice, and posting signage directing consumers to where the notice can be found online."
- Provides some added flexibility for retailers and offline businesses
- But remember that a business that doesn't operate a website must still provide another method of informing consumers of the opt-out right

Withdrawn: Simple Methods and Minimal Steps for Consumers to Submit Opt-out Requests

- Withdrawn Section 999.315(c):
  - "A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not utilize a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's decision to opt-out."

Withdrawn: Denial of Requests from Agents

- Withdrawn Section 999.326(c):
  - "A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on their behalf."
  - Similar language also deleted from Section 999.315(g)
  - However, new language in Section 999.315(g) states that requests may be denied if the agent cannot provide the business with the consumer's signed permission

Withdrawn: Severability

- Section 999.341 was deleted in its entirety
- Provided that if any provision of the CCPA regulations was found to be unconstitutional, in excess of AG's authority, etc., the determination would not affect the validity of the remaining regulations

- AG did not explain whey these provisions were withdrawn
- Reserves the right to submit these withdrawn provisions "after further review and possible revision"
- The withdrawn provisions do not drastically alter a business's compliance obligations

Additional Revisions

- Under proposed final regulations, businesses could name their notice of the right to opt out either:
  - "Do Not Sell My Personal Information" or
  - "Do Not Sell My Info"

- Now businesses can only use "Do Not Sell My Personal Information"
  - Consistent with CCPA statute

AB 1281 Passed by CA Legislature

- On August 30, the California Legislature passed AB 1281, which would extend the CCPA's limited exemptions for employment-related and B2B data
  - Not yet signed by Governor Newsom
- Welcome development for the many businesses and employers that rely on these two exemptions

- Exemptions provide that the "request" provisions of the CCPA that allow for requests to know, to delete or requests to opt out of sale do not extend to employees, contractors, job applicants, or business to business contacts

Effect of AB 1281

- CCPA statute currently provides that employment and B2B exemptions will sunset on January 1, 2021

- If California voters pass Proposition 24, the Consumer Personal Information Law and Agency Initiative, which will be on November 3, 2020 ballot
  - Employment and B2B exemptions will be extended until January 1, 2023

- But what if Prop 24 is voted down?
  - AB 1281 addresses this problem
  - If Prop 24 is not approved, then the one-year extension of the employment and B2B exemptions provided in AB 1281 will take effect
  - Ensures that, at a minimum, the exemptions will be available until January 1, 2022

CCPA 2.0: The California Privacy Rights and Enforcement Act of 2020

- It is important to keep up with the California Privacy Rights and Enforcement Act of 2020 ballot initiative ("CPREA" or "CCPA 2.0"), also known as Proposition 24
- Sponsored by Californians for Consumer Privacy
- Obtained signatures sufficient to appear on the November 3 ballot
- In order to become law, the initiative must be approved by a simple majority of votes cast for or against the measure
- If passed CPREA becomes effective January 1, 2023, and enforced July 1, 2023

What's New In The CPRA?

- **Sensitive personal information**: Consumers could opt-out of a business's use and disclosure of sensitive personal information
  - Includes account and login information, precise geolocation data, contents of mail, email and text messages, genetic data, and certain sexual orientation, health and biometric information
- **Expanded breach liability**: In addition to the private right of action for breaches of nonencrypted, nonredacted PI under the CCPA, there would be a private right of action for unauthorized access or disclosure of an email address in combination with a password or security question that would permit access to an account if the business failed to maintain reasonable security
- **Right of correction:** Consumer would have right to have inaccurate PI corrected
- **Extending employee and B2B exceptions:** CCPA's partial exceptions for employees, applicants, officers, directors, contractors and business representatives would be extended through January 1, 2023

What's New In The CPRA? (cont.)

- **Advertising opt-out:** Consumer could opt out of a business's sharing of PI for cross-site behavioral advertising purposes

- **Extending requests to know:** Consumer would have the right to make a request to know that extends earlier than 12 months preceding the request
  - Business must comply unless doing so "proves impossible or would involve a disproportionate effort"

- **Proportionality:** Collection, use, retention and sharing of PI by businesses must be proportional to the purpose

The California Privacy Protection Agency

- **The CPRA creates a new enforcement agency: California Privacy Protection Agency**
  - The Agency would assume the California AG's responsibility for interpreting and enforcing CCPA/CPRA
  - The Agency would consist of a 5-member board
    - The Governor would appoint the Chair and 1 member
    - The Attorney General, Senate Rules Committee, and Speaker of the Assembly would each appoint 1 member
  - The appointments shall be made from among Californians with expertise in the areas of privacy, technology, and consumer rights.
- The functions of the Agency would include:
  - Implementation and enforcement of the CPREA
  - Rule making authority
  - Providing guidance to businesses and consumers regarding the CPREA
  - Issuing orders that require violators to pay administrative fines of up to $2,500 per violation of the Act or up to $7,500 per intentional violation

Compliance Hypotheticals and Best Practices

Morgan Lewis

Online Advertising

- One of the most discussed aspects of the CCPA is its applicability to the online advertising industry
- Does sharing personal information with a business that delivers online ads constitute a "sale" of PI?
  - First set of CCPA regulation modifications (Feb. 2020) included "guidance" interpreting definition of "personal information"
    - "If a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household then the IP address would not be 'personal information.'"

Online Advertising (cont.)

- In March 2020 modifications to CCPA regulations, this guidance was deleted
- Nevertheless, the principle stated in the guidance remains supported by the definition of "personal information," which applies to information
  - "that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"
  - If an IP address collected to deliver online ads is not linked, or reasonably linkable, by the business to a consumer's identity, then it is arguably not personal information subject to the CCPA

Online Advertising (cont.)

- Sharing PI with an online ad service is not a sale if the service enters into a service provider agreement with the business
- Google offers a Restricted Data Processing (RDP) option that imposes service provider restrictions for online ads and other services using California PI
- Facebook offers a Limited Data Use (LDU) option that applies service provider restrictions
- It's important to remember that:
  - The RDP and LDU options do not apply to all products and services
  - The business must affirmatively elect the RDP/LDU terms

Applicability to Parent Companies and Affiliates

- The definition of "business" includes any entity that controls or is controlled by a business that meets the general definition and that shares common branding with the business
  - "Control" includes ownership or voting power over 50% of shares
  - "Common branding" means a shared name, service mark or trademark

- Example:
  - BigBrand California is the California subsidiary of BigBrand Parent
  - BigBrand Parent also controls subsidiaries in 49 other states

Applicability to Parent Companies and Affiliates (cont.)

- BigBrand Parent would be a business subject to the CCPA because it
  - Owns more than 50% of the shares of BigBrand California
  - Shares use of the BigBrand name/trademark
- From a practical perspective, BigBrand California would be responsible for implementing CCPA compliance because it maintains the California PI
- However, because BigBrand is also a business, the California AG could bring an enforcement action against both parent and subsidiary
  - Parent may provide a deeper pocket for a settlement

Applicability to Parent Companies and Affiliates (cont.)

- But what about the other 49 subsidiaries that BigBrand Parent controls?
  - Technically, they are all entities "controlled" by a business (Big Brand Parent)
  - So all 49 subsidiaries might be considered businesses subject to a CCPA enforcement action stemming from the conduct of BigBrand California
  - Seems like an unintended overreach by the California Legislature and the California AG

- Businesses should carefully consider the scope of CCPA's applicability to their family of companies
  - Particularly if California PI is shared with those companies

Service Provider Agreements

- When a business shares PI with a third party for a business purpose pursuant to a written contract, that disclosure will constitute a sale unless:
  - The business has satisfied the CCPA's opt-out requirements (which may include simply stating in the privacy policy that the business does not sell personal information); and
  - ***The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose***
  - See CCPA's definition of "sale" in Cal. Civ. Code § 1798.140(t)(2)(C)

- While a CCPA-specific service provider agreement is desirable, consider whether an existing agreement already contains provisions that restrict the service provider's uses of PI in accordance with the highlighted provision

Service Provider Agreements (cont.)

- What if the vendor is using the PI for its own purposes (such as improving its products or services) in addition to the business's business purpose?
  - Unclear whether those uses of PI would trigger a "sale"

- What if the business has already negotiated a GDPR data processing addendum with the vendor?
  - The addendum may cause the vendor to qualify as a CCPA service provider based parallels between GDPR and CCPA requirements
  - But is the scope of the GDPR DPA broad enough to encompass California operations and PI?

ENFORCEMENT AND LITIGATION

Morgan Lewis

Background – Attorney General Enforcement

- **Attorney General Civil Enforcement Action**
  - Not more than $7,500 for each intentional violation of the CCPA
  - $2,500 for unintentional violations that the company fails to cure within 30 days of notice
  - Injunctive relief

  - New Consumer Privacy Fund
    - 20 percent of the collected UCL penalties allocated to a new fund to "fully offset any costs incurred by the state courts and the Attorney General"
    - 80 percent of the penalties allocated "to the jurisdiction on whose behalf the action leading to the civil penalty was brought"

CCPA Enforcement – Attorney General's Opinion

- Despite the industry efforts to postpone the July 1 enforcement deadline, the Attorney General's office kept the enforcement deadline as is.
- An advisor to the Attorney General reportedly stated that the Attorney General's office is "committed to enforcing the law upon finalizing the rules or July 1, whichever comes first …"
- Also, on April 10, 2020, AG Becerra issued an alert reminding consumers of their data privacy rights during the COVID-19 public health emergency, without referencing any delays of the July 1 enforcement deadline.

Limited Private Right of Action

- **Limited Consumer Private Right of Action**
  - Individual consumer or classwide basis
  - Only to data breaches, but proposed legislation looks to expand the private right of action to violations of the privacy requirements.

(1) Nonencrypted or nonredacted **personal information***

(2) "subject to an unauthorized access and exfiltration, theft, or disclosure

(3) as a result of the business's violation of the duty to implement and maintain **reasonable security** procedures and practices appropriate to the nature of the information to protect the personal information"

Limited Private Right of Action (cont.)

- A consumer seeking statutory damages must first provide the intended defendant with 30 days' advance written notice of the alleged violations of the CCPA
- If the business cures the alleged violation and provides an express written statement to that effect, the prospective plaintiff may not initiate an action for statutory damages
- But if a security breach was truly caused by a lack of reasonable security, it may be difficult to establish cure after the fact

CCPA's Private Right of Action and Reasonable Security

- The success of CCPA security breach cases is likely to turn on the meaning of "reasonable security"
- CCPA references California Civil Code Section 1798.81.5, California's often-ignored "reasonable security" law
  - Obligates a company that processes personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information it processes
- February 2016: California Dept. of Justice, in its California Data Breach Report, identified the 20 data security controls published by the Center for Internet Security (CIS Controls) as a standard for reasonable security

CCPA's Private Right of Action and Reasonable Security

- DOJ: "The failure to implement all the controls that apply to an organization's environment constitutes a lack of reasonable security"

- Businesses subject to the CCPA would be well served to document
  - compliance with the CIS Controls or similar industry standards
  - a determination that the business's security measures satisfy the CCPA's "reasonable security" standard

- Businesses should formally document their security policies and procedures in a written information security program (WISP) that is reviewed regularly

Statutory Damages Range

- Court imposes the **greater** of **statutory or actual damages**

- **Statutory Damage Range**
  - Statutory damages are "not less than" $100 and "not greater than" $750 "per consumer per incident"
- **Statutory Damages Factors**
  - Nature and seriousness of the misconduct
  - Number of violations
  - Persistence of the misconduct
  - Length of time over which the misconduct occurred
  - Willfulness of the defendant's misconduct
  - Defendant's assets, liabilities, and net worth
  - Other "relevant circumstances presented by any of the parties"

[Cal. Civil Code § 1798.150(a)(2)]

CCPA New Era in Data Breach Litigation

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

CCPA Litigation So Far

- The CCPA statute took effect on January 1, 2020
- Since then, approximately 50 private lawsuits have been filed citing the CCPA in some respect as a basis for the action
- The CCPA expressly provides that a private right of action is only available for certain data breach incidents "and shall not be based on violations of other sections of the CCPA"
  - CCPA also states, "nothing in this title shall be interpreted to serve as a basis for a private right of action under any other law"
- Plaintiffs' ability to litigate alleged CCPA violations apart from security breaches will face strong opposition, but that issue will be contested in the courts in the coming year

CCPA Litigation So Far (cont.)

- Approximately half of the CCPA lawsuits relate to security breaches

- Plaintiffs in other cases have brought claims on alleged violations of consumer privacy rights, often asserting that noncompliance with the CCPA, by extension, constitutes a violation of California's Unfair Competition Law, Consumer Legal Remedies Act, or other causes of action

  – These suits are generally brought as class actions

CCPA Breach Litigation

- In CCPA breach cases, plaintiffs have generally sought statutory damages
  - But also restitution and an injunction against defendants' continued alleged improper handling of personal information
  - *Jose Lopez v. Tandem Diabetes Care, Inc.*, No. 3:20-cv-00723-LAB-LL, at 25 (S.D. Cal April 16, 2020)

- Fewer cases allege actual damages as a result of the security incident
  - Fuentes v. Sunshine Behavioral Health, No. 8:20-cv-00487, at 20-21 (C.D. Cal. March 10, 2020)
    - Alleged data breach caused actual harm because plaintiffs must now "freeze" credit cards, contact financial and health institutions, and monitor credit reports

COMPLIANCE IN THE CURRENT ENVIRONMENT

Morgan Lewis

Practical CCPA Compliance: Website Privacy Policy

- Amend your website privacy policy to address CCPA requirements
- AG may look at company websites to gauge compliance with CCPA
  - Companies that lack a compliant privacy policy may receive increased scrutiny
- More granular CCPA privacy policies may also provide a target for the FTC under its authority under Section 5 of the FTC Act to regulate "unfair or deceptive acts or practices"

Practical CCPA Compliance: Website Home Page

- Businesses that sell personal information must provide a "Do Not Sell My Personal Information" link on their websites

- If privacy policy indicates that personal information is sold, but "Do Not Sell" link is not provided, then CCPA violation is apparent

- Businesses that do not sell personal information should clearly indicate that in their privacy policies

Practical CCPA Compliance – Data Mapping

- Increase your data mapping efforts and form a compliance team to resolve practical CCPA compliance issues, such as:
  - Are you engaged in "sales," as broadly defined, triggering the opt-out right?
  - Are you providing "financial incentives" to consumers in exchange for the provision of personal information that would trigger a notice of financial incentives?
  - What methods should you make available for receiving consumer requests?
    - Two or more designated methods for submitting requests to delete and requests to know, which may include email, mail, form submitted in person and toll-free number
      - For requests to know, must include a toll-free telephone number
    - Is another method needed to "reflect the manner in which the business primarily interacts with the consumer"?

Practical CCPA Compliance – Amend Service Provider Agreements

- Businesses must ensure that their existing agreements with third-party vendors or service providers limit the service provider's use of personal information as prescribed in the CCPA

- Without a CCPA-compliant service provider agreement, the disclosure of personal information to a vendor may constitute a sale of personal information that triggers the consumer's opt-out right

Practical CCPA Compliance -- Training

- CCPA requires training of individuals responsible for handling consumer inquiries, ensuring that they understand how to respond to consumer rights requests

- During COVID-19 pandemic, CCPA training may need to be provided remotely

Practical CCPA Compliance – Document Retention

- Businesses must update their document retention policies to ensure that all records of consumer requests and the business's response are maintained for at least 24 months

- Companies maintain these records in accordance with reasonable security measures in order to reduce potential liability from security breaches

Practical CCPA Compliance – Employment-Related Notices

- Businesses must provide privacy notices describing personal information collected and how it is used to:
  - Employees
  - Job applicants
  - Contractors
  - Officers
  - Directors
- Do your notices describe any new types of personal information (such as COVID-19 test results) that are collected due to the pandemic and in compliance with CDC and other guidances?

The Challenge of CCPA Compliance

- Perfect CCPA compliance is challenging especially, at a time when
  - businesses are dealing with operational disruptions due to COVID-19
  - regulations have only just been finalized, after many businesses have already set their annual compliance budgets

- Reasonable, ongoing efforts to achieve CCPA compliance is an attainable objective

- Please see the Morgan Lewis CCPA Resource Page for our Practical Privacy series of articles on CCPA compliance

Biography

Andrew J. Gray IV
Silicon Valley
+1.650.843.7575
andrew.gray@morganlewis.com

Serving as the leader of Morgan Lewis's semiconductor practice and as a member of the firm's fintech and technology practices, Andrew J. Gray IV concentrates his practice on intellectual property (IP) litigation and prosecution and on strategic IP counseling. Andrew advises both established companies and startups on Blockchain, cryptocurrency, computer, and Internet law issues, financing and transactional matters that involve technology firms, and the sale and licensing of technology. He represents clients in patent, trademark, copyright, and trade secret cases before state and federal trial and appellate courts throughout the United States, before the US Patent and Trademark Office's Patent Trial and Appeal Board, and before the US International Trade Commission.

Biography

W. Reece Hirsch
San Francisco
+1.415.422.1422
reece.hirsch@morganlewis.com

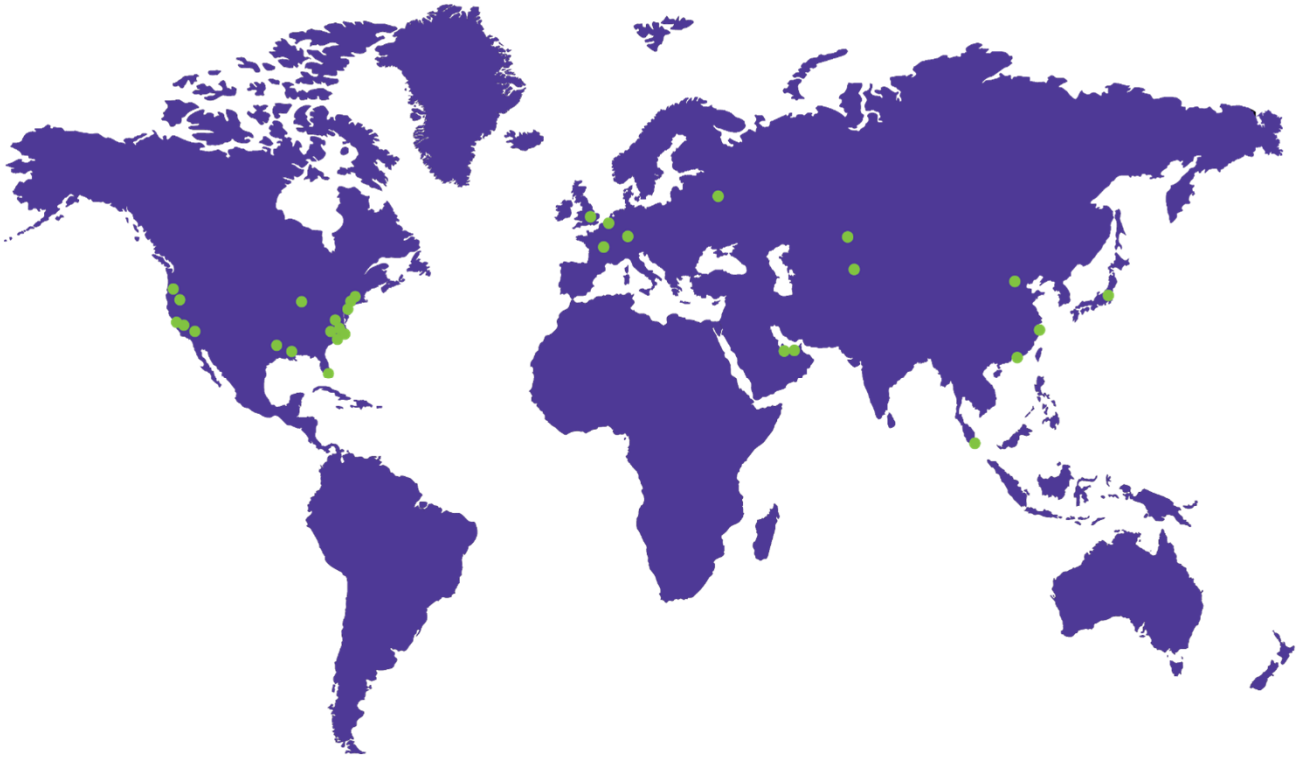
W. Reece Hirsch co-heads the firm's privacy and cybersecurity practice and counsels clients on a wide range of US privacy issues, specializing in healthcare privacy and digital health. Reece counsels clients on development of privacy policies, procedures and compliance programs, security incident planning and response, and online, mobile app, and Internet of Things privacy. In a Chambers USA ranking, Reece was recognized by his peers as "a consummate expert in privacy matters."

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. Morgan Lewis Stamford LLC is a Singapore law corporation affiliated with Morgan, Lewis & Bockius LLP.

THANK YOU