Morgan Lewis

THE CALIFORNIA CONSUMER PRIVACY ACT: PREPARING FOR 2020

August 1, 2018

Joseph Duffy
Reece Hirsch
Mark Krotoski

Overview

- Legislative History and Influencing Factors
- Businesses Subject to the CCPA
- Broad Definition of "Personal Information"
- New Statutory Rights
- Violations, Security Breaches, Enforcement and Private Rights of Action
- Amendments and Regulations
- Early Questions
- Preparing for 2020

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

LEGISLATIVE HISTORY AND INFLUENCING FACTORS

The California Consumer Privacy Act of 2018

- On June 28, 2018, California enacted the California Consumer Privacy Act (CCPA)
  - A unique and comprehensive consumer privacy law
  - Unlike any other US privacy law
  - "GDPR-like" consumer privacy rights
  - New private right of action for security breaches and potential statutory damages
- Organizations subject to the CCPA must comply by January 1, 2020
  - As we learned with GDPR compliance, a year and a half isn't that long when you're changing processes to comply with significant new privacy requirements
- IAPP estimates that the law will likely affect more than 500,000 US companies doing business in California
  - Including many small and midsized businesses

The CCPA's Fire Drill Enactment

- The CCPA was originally an initiative slated to appear on the November ballot
- Widely opposed by technology companies and other business interests
- A replacement CCPA bill (AB 375) was introduced within a week of its passage
- Governor Brown signed the CCPA into law hours before the deadline to withdraw the initiative
- The CCPA as enacted is a slightly "watered down" version of the initiative
- The fire-drill drafting process resulted in a law with numerous ambiguities and outright errors
  - Corrections will need to be made prior to Jan. 2020

California Consumer Privacy Act Clears Major Hurdle: Submits 629,000 Signatures Statewide

May 3, 2018

Sacramento, Calif. – Today, Californians for Consumer Privacy announced submission of 629,000 signatures statewide to qualify The California Consumer Privacy Act for the November ballot.

"Today is a major step forward in our campaign, and an affirmation that California voters care deeply about the fundamental privacy protections provided in the California Consumer Privacy Act," said **Alastair Mactaggart**. "This initiative will give consumers a real choice about whether they want their private information bought and sold by companies they've never heard of, will help shine a light onto the business of data brokerage, and will empower California consumers to protect their sensitive personal information."

California lawmakers agree to new consumer privacy rules that would avert showdown on the November ballot

LA Times | By JOHN MYERS and JAZMINE ULLOA JUN 21, 2018 | 8:40 PM | SACRAMENTO

Governor Brown Signs Legislation

Published: Jun 28, 2018

SACRAMENTO – Governor Edmund G. Brown Jr. today announced that he has signed the following bills:

- AB 375 by Assemblymember Ed Chau (D-Arcadia) – Privacy: personal information: businesses.

https://www.caprivacy.org/post/california-consumer-privacy-act-clears-major-hurdle-submits-625-000-signatures-statewide
http://www.latimes.com/politics/la-pol-ca-privacy-initiative-legislature-agreement-20180621-story.html
https://www.gov.ca.gov/2018/06/28/governor-brown-signs-legislation-9/

Factors Influencing the CCPA

- GDPR
  - CCPA is influenced by concepts such as GDPR's "right to be forgotten"
  - GDPR's heightened transparency requirements
  - Right of portability

- CCPA builds upon other unique California privacy laws
  - California Online Privacy Protection Act (CalOPPA)
  - The "Shine the Light" law
  - The "Reasonable security" law

- Reflects recent concerns expressed in congressional hearings and the press regarding collection and use of personal information by social media and other tech companies

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

BUSINESSES SUBJECT TO THE CCPA

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

Additional Criteria for Businesses

- A business must also satisfy one of three thresholds:
  1) The annual gross revenue in excess of $25 million
  2) Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices, alone or in combination
  3) Derives 50% or more of its annual revenue from selling consumers' personal information

- Applies to brick-and-mortar businesses, not just collection of personal information electronically or over the internet
- Does not apply to nonprofits

CCPA Does Not Apply To …

- "Protected health information" (PHI) collected by covered entities governed by HIPAA or the California Confidentiality of Medical Information Act (CMIA)
  - Appears to apply to HIPAA business associates because PHI received by a BA could be said to be "collected by" a CE
- Personal information subject to the Gramm-Leach-Bliley Act (GLBA) "if the CCPA conflicts with that law"
  - Suggests that a financial institution must comply with both CCPA and GLBA, performing a preemption analysis
  - Difficult to imagine how CCPA and GLBA would be coherently reconciled
  - More likely that a blanket exception was intended, similar to HIPAA exception, but clarification is needed

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

BROAD DEFINITION OF "PERSONAL INFORMATION"

Very Broad Definition of "Personal Information"

- Personal information includes any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"
  - Much broader than the definition of personal information under CA's security breach notification law

- Extremely broad definition intended to include the sort of robust consumer profile and preference data collected by social media companies and online advertisers

Compare California Data Breach Notification Statute

"Personal Information" includes:

- (1) An individual's first name or first initial and last name in combination with:

  (A) Social Security number.

  (B) Driver's license number or California identification card number.

  (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

  (D) Medical information.

  (E) Health insurance information.

  (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

- (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

CCPA Definition of Personal Information

1) Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, or passport number
2) Categories of PI described in California's customer records destruction law
3) Characteristics of protected classifications under CA or federal law
4) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies
5) Biometric information
6) Geolocation data
7) Internet or other electronic network activity, such as browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
8) Audio, electronic, visual, thermal, olfactory, or similar information
9) Professional or employment-related information
10) Education information that is subject to the Family Educational Rights and Privacy Act
11) Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

Aggregate Consumer Information

- Excluding "Aggregate Consumer Information"
- Defined as:
  - Data that is "not linked or reasonably linkable to any consumer or household, including via a device"
  - Information that is publicly available from federal, state, or local government records
- Is an employer's data on employees "personal information"?
  - Probably not, but CCPA is ambiguous on that point

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

NEW STATUTORY RIGHTS

New Statutory Rights

- Right to know the categories of information
- Right of access and data portability
- Right to be forgotten
- Right to opt out of the sale of personal information to third parties
- Right to equal service and price

Right to Know the Categories of Information

- A business is required to disclose
  - At or before the point of collection
  - In its website privacy policy or otherwise
  - The categories of personal information to be collected about a consumer
    - Including the categories of the consumer's personal information that were actually collected during the last 12 months
    - PI sold or disclosed for business purposes in the last 12 months
  - The purposes for which the information will be used

Verifiable Consumer Requests

- In addition to website privacy policy, CCPA requires each business to respond to "verifiable consumer requests" with individualized disclosures about the business's collection, sale, or disclosure of PI belonging to the specific consumer making the request

- "Verifiable consumer request" is a request by "a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State"
  - Consumer can make two requests in a 12-month period

CCPA Definition of Personal Information

- Business must offer two or more methods for making the requests
  - At a minimum: a toll-free phone number and a website address

- Does your business have the ability to produce this sort of highly granular report for each consumer?

In response to a request, the business must disclose:

(1) The categories of personal information collected about the consumer

(2) The categories of sources from which personal information is collected

(3) The business or commercial purpose for collecting or selling the PI

(4) The categories of third parties with which the business shares PI

(5) The specific pieces of PI the business has collected about the consumer

(6) The categories of the consumer's PI that were sold or disclosed for business purposes in the 12 months preceding the request

Right of Access and Data Portability

- CCPA gives each consumer the right to access a copy of the "specific pieces of information that the business has collected about that consumer"
  - To be delivered free of charge
  - Within 45 days
  - By mail or electronically
- Does not apply to PI that is collected for "single, one-time transactions"
- Implies an obligation for businesses to preserve these consumer records
- Information produced must be portable, to the extent "technically feasible"
- In a readily usable format
- "Technical feasibility" standard appears to be drawn from Art. 20 of GDPR, which also creates a right of portability

Right to be Forgotten

- Under the CCPA, consumers have the right to request that a business delete any PI collected about the consumers
  - Extends to PI held by a third-party service provider
- Exceptions where PI is necessary to:
  (1) Complete a transaction, provide goods and services, or otherwise perform a contract with a consumer
  (2) Detect security incidents
  (3) Exercise free speech
  (4) Enable internal uses that are reasonably aligned with consumer expectations
  (5) Comply with a legal obligation
  (6) Otherwise use the consumer's PI in a lawful manner that is compatible with the context in which the PI was provided

Right to be Forgotten Versus Preservation of Evidence

- The right to be forgotten may not be consistent with a company's need to preserve evidence for litigation

- CCPA will entail a review of a company's document retention policy
  - Policy will need to be revised to reconcile:
    - Need to preserve evidence for litigation
    - Honor CCPA's right to be forgotten
    - Avoid sanctions for spoliation of evidence

Right to Opt Out of Sale of Personal Information

- The CCPA provides consumers with the right to opt out of the sale of their personal information to third parties
  - Businesses that sell personal information to third parties must provide notice to consumers that
    - Their personal information may be sold
    - They have the right to opt out of the sale

- A business must post a "clear and conspicuous link" on its website's home page titled "Do Not Sell My Personal Information"
  - The page must also be linked in the business's privacy policy

Minors' Opt-in Right

- CCPA provides minors with a "right to opt in"
  - Businesses are prohibited from selling PI of consumers between the ages of 13 and 16 without first obtaining affirmative opt-in consent
    - From the consumers or
    - From the parent or guardian where a consumer is under the age of 13
  - CCPA age requirements are stricter than the federal Children's Online Privacy Protection Act (COPPA)
  - CCPA also differs from the Privacy Rights for California Minors in the Digital World law, which permits persons under age 18 to remove certain posted online content

What is a Sale?

- A "sale" is defined as
  - "selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating
  - orally, in writing, or by electronic or other means,
  - a consumer's personal information
  - by the business to another business or a third party
  - for monetary or other valuable consideration"

- Limited exceptions, including "intentional interaction" directed by a consumer and disclosure to a service provider
- Definition is extremely broad and needs to be clarified

Is Affiliate Sharing a Sale?

- When a business shares PI with an affiliate, would that constitute a sale requiring opt-in consent?
  - Arguably a "transfer" of PI to another business or third party
  - However, the definition of "business" includes another entity under the business's control that operates under the same brand
  - Under current definitions, the answer will depend on the facts and circumstances
    - Is the affiliate using the same brand?
    - Is monetary or "other valuable consideration" changing hands?
      - This is probably not a high bar under California contract law authorities

Right to Equal Service and Price

- CCPA grants consumers a "right to equal service and price"
  - Prohibits businesses from discriminating against consumers who exercise their rights under the CCPA
- A business is specifically prohibited from
  (1) Denying goods or services to a consumer
  (2) Charging a consumer a different price or rate for goods or services, including through the use of discounts or other benefits
  (3) Imposing penalties
  (4) Providing a consumer with a different level of quality or service
  (5) Suggesting a consumer will receive a different price or rate or different level of quality of goods or services

Right to Equal Service and Price (cont.)

- A business may charge a consumer who exercises rights a different rate or provide a different level of service so long as the difference is directly related to "value provided to the consumer by the customer's data"
  - How would that difference in value be quantified and supported?
- Businesses may offer financial incentives, including payments to consumers as compensation, for the collection, sale, or deletion of personal information
- Businesses must ensure that personnel responsible for handling consumer inquiries under the CCPA are informed of the requirements and how to direct consumers regarding granting those rights

Limitations on Disclosures to Third Parties and Service Providers

- CCPA allows businesses to share PI with third parties or service providers for business purposes
  - So long as there is a written contract prohibiting a service provider from
    - selling the PI or
    - "retaining, using, or disclosing the PI for any purpose other than for the specific purpose of performing the services specified in the contract"
- "Business purpose" is defined as "the use of PI for the business's or service provider's operational purposes, or other notified purposes, provided that the use of PI shall be reasonably necessary and proportionate to achieve the operational purpose for which it was collected"

Categories of "Business Purposes"

- CCPA lists categories of activities that constitute "business purposes," including:
  - Auditing
  - Detecting security incidents
  - Performing services, such as
    - Maintaining or servicing accounts
    - Providing customer service
    - Processing payments
    - Fulfilling orders and transactions
    - Providing analytic services
    - Undertaking internal research for technological development and demonstration

CCPA-Compliant Service Provider Agreements

- A business that satisfies CCPA's contracting requirements will not be liable for the service provider's or third party's violation of the CCPA
  - Provided that the business did not have actual knowledge or reason to believe at the time that the PI was disclosed that the recipient intended to violate the CCPA
- A CCPA-compliant service provider agreement will not constitute a sale of PI triggering the CCPA's opt-out right
- CCPA contracting requirements are generally consistent with good privacy practices, but they create a new filter that must be applied to agreements
  - Does the agreement limit use of PI to the specific purpose of performing the specified services?
  - Is the use of PI reasonably necessary and proportionate to the operational purpose?
  - Is the purpose of the agreement a "business purpose"?

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

VIOLATIONS, SECURITY BREACHES, ENFORCEMENT AND PRIVATE RIGHTS OF ACTION

Violations, Security Breaches, Enforcement and Private Rights of Action

- Attorney General Civil Enforcement

- Limited Consumer Private Right of Action

Attorney General Enforcement

- **Attorney General Civil Enforcement Action**
  - $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 under the CA Unfair Competition Law (UCL) (Cal. Bus. & Prof. Code § 17206)

  - 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"

Civil Penalties

- **Limited Consumer Private Right of Action**
  - Individual consumer or classwide basis

(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"

Civil Penalties

- **Limited Consumer Private Right of Action**

- Statutory or actual damages (greater of)
- Injunctive or declaratory relief
- Any other relief the court deems proper

Civil Penalties

Statutory or Actual Damages

- **Greater of**:
  - Not less than $100 and not greater than $750 per consumer per incident
  - Or actual damages

Civil Penalties

Statutory or Actual Damages

- **Greater of**:
  - Not less than $100 and not greater than $750 per consumer per incident
  - Or actual damages

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"

Prior Business Written Notice Requirement

- Before filing a civil action for **statutory damages**:
  - Consumer must provide 30 days' written notice "identifying the specific provisions of this title the consumer alleges have been or are being violated."
    - If actually cured within 30 days and business provides "an express written statement that the violations have been cured and that no further violations shall occur," no statutory damages action may be initiated.
    - A civil action may be filed "to enforce the written statement" for statutory damages "for each breach of the express written statement" and "any other violation of the title that postdates the written statement."

- For **actual pecuniary damages**, no written notice required

Attorney General Notification

- Within 30 days of filing a consumer civil action for statutory damages, consumer notifies Attorney General

- Attorney General within 30 days:

  (1) Notifies consumer of the AG's **intent to prosecute** an action against the violation.

  - If no prosecution within six months, consumer may proceed with the action.

  (2) If **AG refrains** from acting within 30 days, consumer may proceed with the action.

  (3) Notifies the consumer that the civil action **may not proceed**.

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

CLASS ACTION LITIGATION AND THE CCPA

CCPA and Class Actions

- Impact of CCPA's statutory damages for security breach on class action litigation in California

- CCPA provides that any agreement or contract provision that seeks to waive or limit a consumer's rights under the CCPA
  - Including any "right to a remedy or means of enforcement," shall be deemed void and unenforceable
  - Could be interpreted to bar arbitration and class action waivers with respect to private actions under the CCPA

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

AMENDMENTS AND REGULATIONS

Amendments and Regulations

- The CCPA will be amended; the question is, how substantially?
- Will other state legislatures take the CCPA as a model?
  - Will CCPA catch on like CA's data breach notification law?
  - Or will it be a one-off experiment, like the Shine the Light law?
  - Either way, likely to be a de facto national standard

- On or before the 2020 compliance date, AG will seek public comment on regulations to implement the CCPA, including updates, as needed
  - Definition of "unique identifier" to address changes in technology

Regulations and Advisory Opinions

- One year after the CCPA's passage (June 28, 2019), AG must establish rules and procedures governing
  - Consumer's submission of an opt-out request
  - A business's processing of an opt-out request
  - Development of a uniform opt-out logo or button
  - Required notices to be provided by businesses

- A business or third party may also seek an advisory opinion from the AG for guidance on complying with the CCPA
  - Unclear when that process will be available

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

EARLY QUESTIONS ABOUT THE SCOPE AND APPLICATION OF THE CCPA

Early Questions

- Will Congress enact uniform data breach and privacy standards to reconcile the patchwork standards emerging in the states and other jurisdictions?

- Will other states adopt versions of the CCPA?

- Defining a host of new standards
  - Biometric information
  - Geolocation data
  - Internet or other electronic network activity
  - Inferences drawn to create a profile about a consumer

Early Questions

- Guidance on "reasonable security procedures and practices appropriate to the nature of the information"

- Reconciling standards with the California Data Breach Notification statute
  - Data breach vs. "unauthorized access and exfiltration, theft, or disclosure"
  - Encryption safe harbor

- Clarifying and removing ambiguity concerning scope of statutory exceptions
  - HIPAA
  - Gramm-Leach-Bliley Act (GLBA)

CALIFORNIA CONSUMER PRIVACY ACT OF 2018

PREPARING FOR 2020

Preparing for 2020

- While further details concerning the CCPA remain, the framework is in place
- Businesses can use the time now to begin thinking about how they would comply with the CCPA under the current framework
  - For the sweeping CCPA, a year and a half is not that long

- Companies that have recently prepared for GDPR compliance have seen the benefits of a head start
  - GDPR data-mapping and privacy assessment exercises will be useful
  - But CCPA is not simply CA's version of GDPR, and the requirements differ in many important respects

Initial CCPA Compliance Questions

- Does the CCPA apply to your business or do you fit into an exception?
- How many of the data elements included in CCPA's broad definition of personal information does your business collect?
  - Are additional data-tracking mechanisms needed?
- How would your business go about organizing consumer PI to
  - Provide required CCPA notices
    - Can build upon existing California privacy notices developed for CalOPPA and Shine the Light law
  - Provide opt-out and opt-in rights
  - Delete data to comply with the CCPA's right to be forgotten

Initial CCPA Compliance Questions (cont.)

- How would your business go about organizing consumer PI to
  - Provide consumer data upon request in a "readily useable format"
  - Ensure that agreements with service providers are CCPA-compliant
  - Train personnel to properly process new requests to exercise privacy rights

- This is also a good time to fine-tune your business's incident response plan to prepare for the likely boom in California security breach related litigation

W. Reece Hirsch

W. Reece Hirsh
San Francisco
reece.hirsch@morganlewis.com
+1.415.442.1422

Reece Hirsch is a partner in the San Francisco office of Morgan Lewis and co-head of the firm's Privacy and Cybersecurity practice. He advises clients on a wide range of privacy and cybersecurity matters, and has special expertise in California and healthcare privacy laws, including HIPAA. Reece edited and contributed to Bloomberg Law's California Privacy Law Profile. He has been listed in *Chambers USA: America's Best Lawyers for Business* since 2005, and has served on two advisory groups to the California Office of Privacy Protection and Department of Justice that developed recommended practices for security breach response and medical identity theft prevention. He is a Certified Information Privacy Professional, and is a member of the editorial advisory boards of *Bloomberg Health Law News, Healthcare Informatics,* and *Briefings on HIPAA.*

Mark L. Krotoski

Mark L. Krotoski
Silicon Valley | Washington, DC
mark.krotoski@morganlewis.com
+1.650.843.7212
+1.202.739.5024

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues
- Advises clients on mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, responding to regulatory investigations, and coordinating with law enforcement on cybercrime issues.
- Experience handling complex and novel cyber investigations and high-profile cases
  - At DOJ, prosecuted and investigated nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
  - Served as the National Coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, and as a cybercrime prosecutor in Silicon Valley, in addition to other DOJ leadership positions.

Joseph Duffy

Joseph Duffy
Los Angeles
joseph.duffy@morganlewis.com
+1.213.612.7378

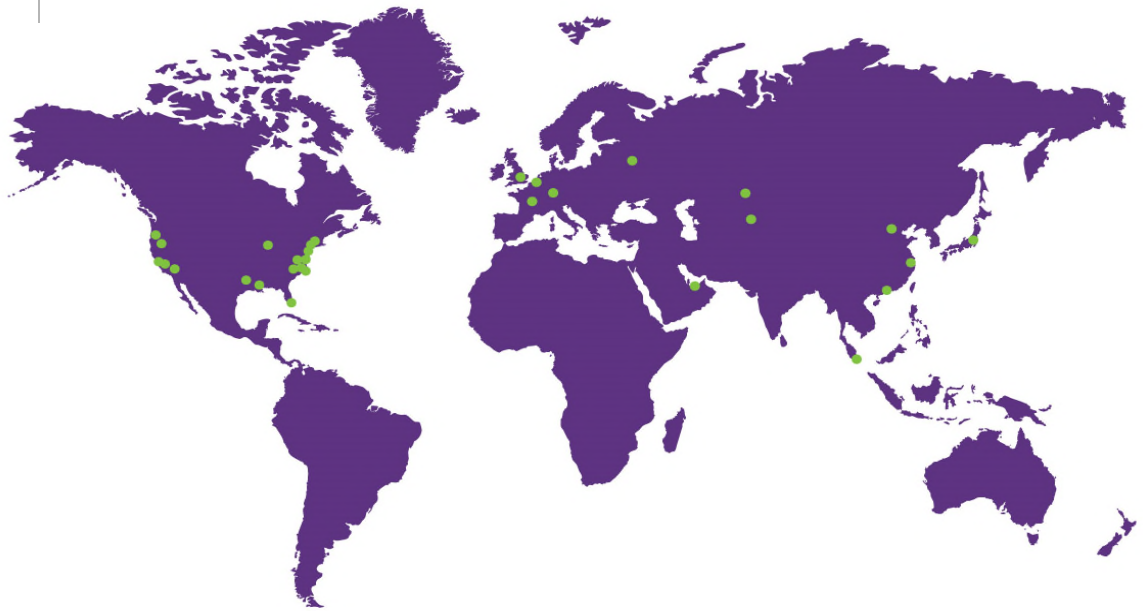
A nationally recognized litigator, Joseph Duffy defends class actions in US federal and state courts. As co-head of the litigation practice's Retail Industry Initiative, he focuses on the unique challenges facing retail companies, representing retailers in consumer class actions, contract disputes, and compliance and privacy matters. He also litigates class actions for financial services companies involving lending practices, foreclosure activity, and debt collection. Joseph earned recognition as a Class Actions and Mass Torts "Powerhouse" in BTI's Litigation Outlook 2014 Report. Joseph also defends a large number of national retailers facing class actions on behalf of consumers related to advertising, pricing, point of sale, privacy, and statutory claims. In addition, he serves as national coordinating and trial counsel in product liability and mass tort litigation, including having served as first- or second-chair trial counsel on more than a dozen cases.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
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.

THANK YOU