Before we begin: Morgan Lewis and Global Technology

Be sure to follow us at our website and on social media:

Web: **www.morganlewis.com/sectors/technology**

Twitter: **@MLGlobalTech**

LinkedIn Group: **ML Global Tech**

Check back to our Technology May-rathon page frequently for updates and events covering the following timely topics:

21st Century Workplace	**Diversity, Environment, Social Justice**	**Medtech, Digital Health and Science**
Artificial Intelligence and Automation	**Fintech**	**Mobile Tech**
Cybersecurity, Privacy and Big Data	**Global Commerce**	**Regulating Tech**

Morgan Lewis

TECHNOLOGY MAY-RATHON

New State Consumer Privacy Laws: Growing Complexity

May 19, 2021

Reece Hirsch, Greg Parks, Mark Krotoski,
Kristin Hadgis, and Taylor Day

Presenters

W. Reece Hirsch

Gregory T. Parks

Mark L. Krotoski

Kristin M. Hadgis

Taylor C. Day

Morgan Lewis

Agenda

- Latest changes in the final CCPA regulations
- The California Privacy Rights Act
- Virginia's Consumer Data Protection Act
- Comparison of privacy laws in California and Virginia
- 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 Cal. Civil Code 1798.81.5 (California's "reasonable security" law)
- California Privacy Rights Act adds additional privacy protections more closely aligned with GDPR
- Virginia Consumer Data Protection Act generally follows the GDPR-aligned standards of the CPRA
  - And, in at least one notable area (opt-in consent for use and disclosure of sensitive information), goes beyond the CPRA

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 (CPRA raises this to 100,000) 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 nonprofits

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

The Final CCPA Regulations (So Far)

- Additional regulations announced March 15, 2021 reflect minimal changes
- Bans so-called "dark patterns" that delay or obscure the process for opting out of the sale of personal information
- Businesses must name their notice of the right to opt out as "Do Not Sell My Personal Information"
- New regulations provide businesses with an optional opt-out "icon" (not "button") regarding the right to opt-out of sale of personal information


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
- Adds right to opt out of 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

Sensitive Personal Information

- CPRA defines "sensitive personal information" (SPI) to include account and login information; precise geolocation data; contents of mail, email, and text messages; genetic data; and certain sexual orientation, health, and biometric information
- A consumer has the right to direct a business that collects SPI to limit its use of the consumer's SPI to uses necessary to perform the services or provide the goods
  - As reasonably expected by an average consumer
- If a business uses or discloses SPI for other purposes, the consumer must be given right to opt out of those uses or disclosures of SPI
- However, if SPI is collected "without the purpose of inferring characteristics about a consumer" it can be treated as "personal information"
  - Businesses need to carefully consider whether SPI is being collected for consumer profiling purposes, or whether collection is incidental to services
  - Standard will be clarified through future regulations

Sensitive Personal Information Opt Out

- Business must provide a "Limit the Use of My Sensitive Personal Information" link on its homepage
- Consumer must be given the option to restrict uses and disclosures of SPI to what is reasonably necessary to provide goods and services
- Similar to GDPR concept
- Virginia Consumer Data Protection Act also includes similar provision regarding sensitive information
  - Significantly, requires opt-in, rather than opt-out
- If a national company adopts a more stringent opt-in approach to SPI, would that satisfy CPRA?
  - Unclear at this time, but appears that a bifurcated compliance approach for CA and VA would be needed

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

Online Advertising Pre-CPRA

- One of the most discussed aspects of the CCPA is its applicability to the online advertising industry
- Does sharing of personal information with a business that delivers online ads constitute a "sale" of PI?
  - First set of CCPA regulation modifications (February 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 Pre-CPRA (cont.)

- In March 2020 modifications to the 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 adds 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 Pre-CPRA (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 is 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
  - When the CPRA becomes effective in 2023, new behavioral advertising opt-out rules will apply
- Perhaps in anticipation of CPRA, some major tech companies are beginning to require opt-in for behavioral ad tracking through apps

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"
  - "Impossible" is a very high standard
  - What amount of cost/effort is "disproportionate"? Would that mean assembling data that is in the business's possession but not currently associated with the consumer?
- Businesses will need to consider what sort of lookback period is feasible and should document that determination
- Hopefully, CPRA regulations will provide guidance

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

The California Privacy Protection Agency

- **The CPRA creates a new enforcement agency: California Privacy Protection Agency**
  - The Agency will assume the California AG's responsibility for interpreting and enforcing CCPA/CPRA
  - The Agency will consist of a 5-member board.
    - Members may not serve longer than 8 consecutive years
- The functions of the agency will include:
  - Implementation and enforcement of the CPRA
  - Adopting CPRA regulations by July 1, 2022
  - Providing guidance to businesses and consumers regarding the CPRA
  - 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
- AG will retain authority to go to court to enforce the CPRA

Agency Board Appointments

- California Privacy Protection Agency board members were announced March 17, 2021
  - Jennifer M. Urban, Chair, Law Professor, U.C. Berkeley
  - John Christopher Thompson, Senior VP, Government Affairs, LA 2028
  - Angela Sierra, Chief Assistant AG, Public Rights Division
  - Lydia de la Torre, Law Professor, Santa Clara University
  - Vihncent Le, Technology Equity Attorney, Greenlining Institute

- What does this indicate about agency enforcement priorities and approach?
  - Broad range of backgrounds, perspectives
  - Possible focus on algorithmic bias


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 act 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 its gross revenue from the sale of personal data
- Applies to brick-and-mortar businesses, not just the collection of personal data electronically or over the internet
- Does not apply to employment-related data or B2B transaction data

Virginia Privacy Rights Overview

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

Enforcement of Virginia's Privacy Law

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


Comparison of Data Privacy Laws in California and Virginia
Morgan Lewis

Data Subject Rights

DATA SUBJECT RIGHTS	VA CDPA	CA CCPA	CA CPRA
Access	Yes	Yes	Yes
Correct	Yes	No	Yes
Delete	Yes (data provided by or obtained about consumer)	Yes (data collected from consumer)	Yes (data collected from consumer)
Portability	Yes	Yes	Yes
Opt-Out of Sale	Yes	Yes	Yes
Opt-Out of Sharing	No	No	Yes
Non-Discrimination	Yes	Yes	Yes
Appeals Process	Yes	No	No

Controller Obligations

Controller Obligations	VA CDPA	CA CCPA	CA CPRA
Data Minimization	Yes	No	Yes
Purpose Limitation	Yes	Yes	Yes
Security Requirements	Yes	No	Yes
Special Requirements for Children's Data	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
Data Protection Assessment	Yes	No	Yes – submitted to the CA Privacy Protection Agency

Sensitive Data

- Virginia's privacy law prohibits controllers from processing 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 contains 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

Advertising

- The Virginia CDPA grants consumers the right to opt out of, and requires 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

- Virginia's CDPA requires 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 CDPA additionally obligates controllers to establish a process for consumers to appeal the refusal to take action on a request
  - Controllers must respond within 60 days of a receipt of a consumer appeal
  - If the appeal is denied, the controller must inform the consumer how they can submit a complaint to the VA Attorney General

Responding to Consumers Requests to Know, cont.

- Like Virginia's privacy law, both the CCPA and CPRA require a business to respond within 45 days of a verifiable request, with one 45-day extension if certain requirements are met
- There is no comparable mandatory appeal process in either the CCPA or the CPRA
- Instead, the CCPA and CPRA require businesses who 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
- 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, but so was January 1, 2020 and May 25, 2018.
- Use the runway available – but not just to wait. Try things out.
- Recognize 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, job satisfaction.


Looking Ahead
Morgan Lewis

What's Next in Privacy Legislation?

- Federal action?
  - In March 2021, the Information Transparency and Personal Data Control Act was introduced in the 117th US Congress by Rep. Suzan DelBene (D-WA)
  - The first, but certainly not the last, comprehensive federal privacy bill of 2021

- Nearly a dozen states are actively debating a comprehensive privacy law
  - Debate, however, does not guarantee that a law will pass
  - The Washington Privacy Act bill failed for the third straight year

Coronavirus COVID-19 Resources

We have formed a multidisciplinary **Coronavirus/COVID-19 Task Force** to help guide clients through the broad scope of legal issues brought on by this public health challenge.

Morgan Lewis

To help keep you on top of developments as they unfold, we also have launched a resource page on our website at **www.morganlewis.com/topics/coronavirus-covid-19**

If you would like to receive a daily digest of all new updates to the page, please visit the resource page to **subscribe** using the purple "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.

TAYLOR C. DAY

Taylor C. Day
Los Angeles
+1.213.612.7367
taylor.day@morganlewis.com

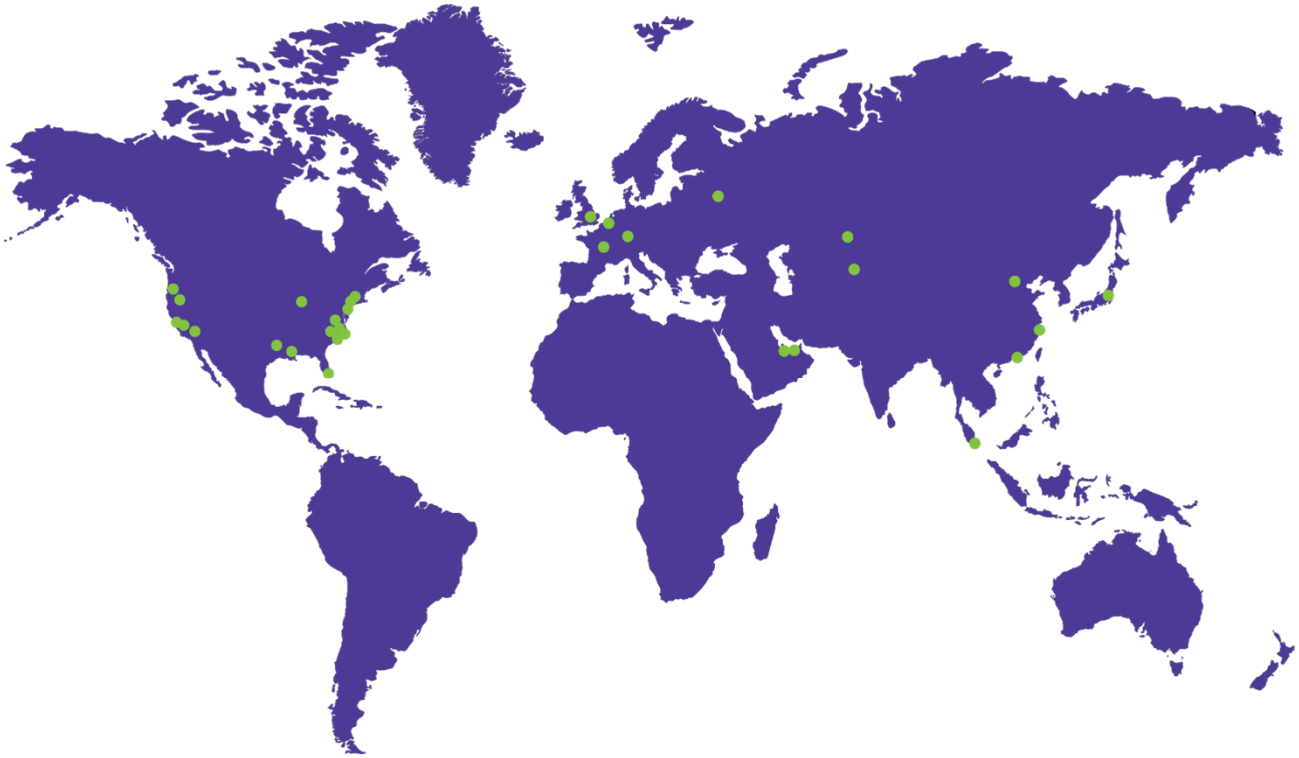
Taylor C. Day advises clients in complex commercial and consumer class action litigation across a variety of sectors, with an emphasis on the healthcare, financial services, and energy industries. He counsels clients in commercial disputes involving privacy, consumer protection, unfair competition, breach of contract, product liability, and tort law. Taylor also has experience advising clients with internal investigations. The International Association of Privacy Professionals has designated him a Certified Information Privacy Professional (CIPP).

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

THANK YOU