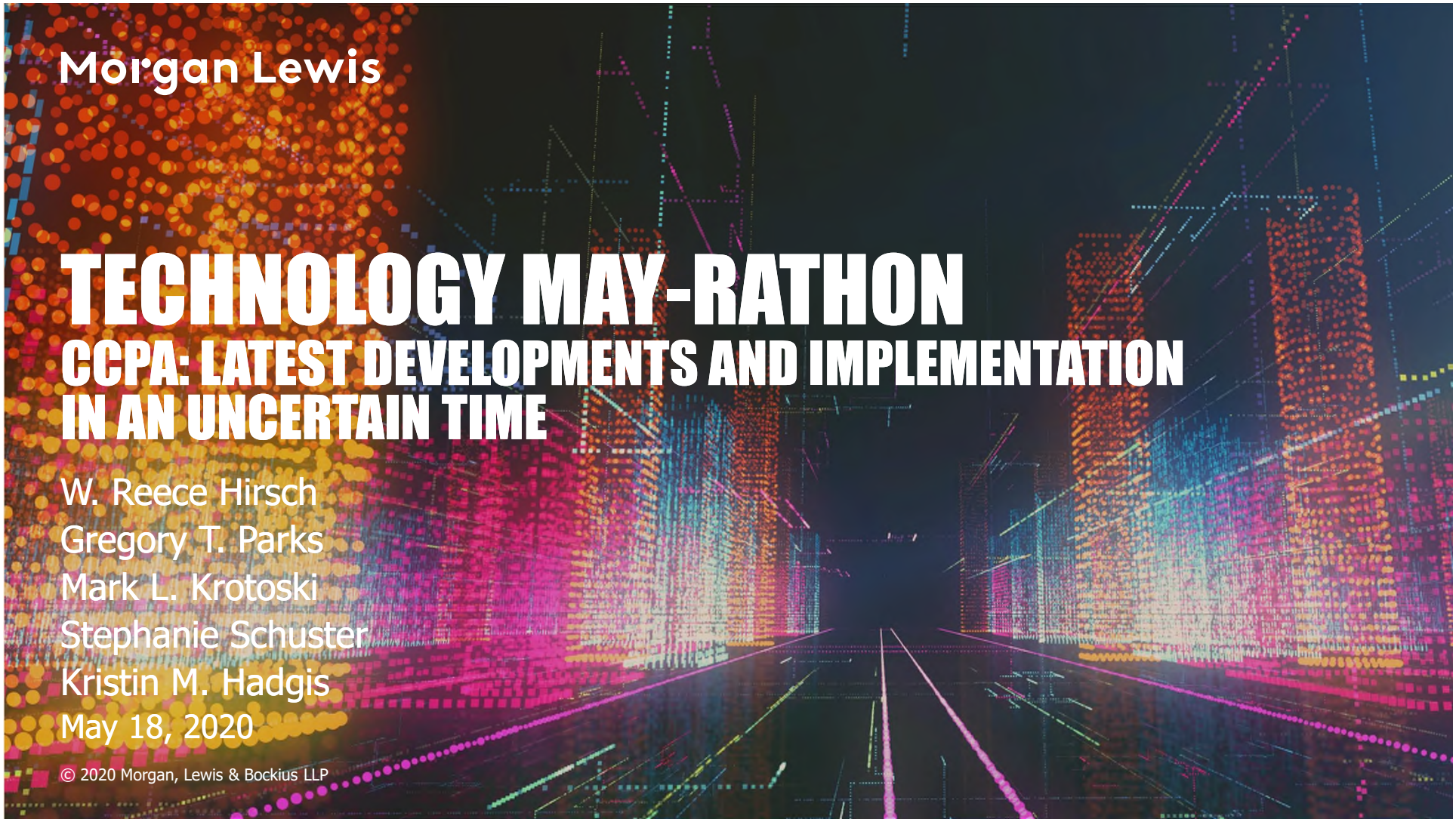

Morgan Lewis
TECHNOLOGY MAY-RATHON
CCPA: LATEST DEVELOPMENTS AND IMPLEMENTATION IN AN UNCERTAIN TIME
W. Reece Hirsch
Gregory T. Parks
Mark L. Krotoski
Stephanie Schuster
Kristin M. Hadgis
May 18, 2020
© 2020 Morgan, Lewis & Bockius LLP

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	**Cybersecurity, Privacy and Big Data**	**Medtech, Digital Health and Science**
Artificial Intelligence and Automation	**Fintech**	**Mobile Tech**
COVID-19	**Global Commerce**	**Regulating Tech**

Agenda

- Introduction
  - COVID-19 implications, latest modifications to regulations, and enforcement deadline
- COVID-19 implications:
  - Increased online activity, operational disruptions, collections of physiological data, July 1 enforcement deadline
- Pending ballot initiative (California Privacy Rights Act of 2020)
- Latest modifications to regulations
  - First set of modifications – released on February 7 and 10, 2020
  - Second set of modifications – released on March 11, 2020
- July 1 enforcement and industry efforts to postpone the enforcement
- Compliance in the current environment

SECTION 01

INTRODUCTION: COVID-19 IMPLICATIONS

Addressing COVID-19 Implications on CCPA: Takeaways

1. Increased online activities such as remote working, e-commerce, and online learning lead to increased collection and monitoring of personal information

2. Operational disruptions that affect businesses' compliance efforts (e.g. lack of on-site staff)

3. Increased screening and collection of physiological data (e.g. body temperatures) and personal movement tracking at work

4. Approaching July 1 CCPA enforcement deadline

COVID-19 Implications on Privacy: What Lies Ahead

- On April 30, 2020, four Senators announced that they intend to introduce federal privacy legislation called "COVID-19 Consumer Data Protection Act" to regulate the collection and use of personal information in connection with the Coronavirus pandemic.
- Under the Act, covered information would include "precise geolocation data, proximity data, and personal health information."
- The Act would primarily rely on the notice and consent requirements to protect information, making it unlawful for a covered entity to "collect, process, or transfer the covered data of an individual" without prior notice and express consent unless necessary to comply with a legal obligation.
- The requirements would apply to processing covered data to track the spread, signs, or symptoms of COVID-19 as well as other COVID-19-related requirements imposed by governments,

Morgan Lewis 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.

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.

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

What Lies Ahead

- If AG's office makes non-substantial changes, there will be no further notice and comment period
  - Regs will be submitted to California's Office of Administrative Law (OAL)
  - OAL will have an extended 60-day period per the March 30 Executive Order to review and confirm that administrative requirements have been followed
  - It is likely that the regulations will follow this path
- If AG's office makes substantial proposed changes, AG must repeat the full 45-day notice and comment process, which is less likely.
- Enforcement starts as of July 1, 2020 unless postponed

Preparing for July 1

- The current enforcement of the California Consumer Privacy Act is July 1, 2020
  - 43 days away, but there is still much uncertainty
  - Regulations are net yet final
  - Businesses need time to interpret and implement the yet-to-be finalized regulations
  - The Attorney General's office indicated no postponement of July 1 enforcement deadline

- This presentation will focus on some practical steps that you can take now to position your organization for July 1, 2020 enforcement.

CCPA 2.0: The California Privacy Rights Act of 2020

- In addition to the approaching CCPA enforcement deadline, it is important to keep up with the California Privacy Rights Act of 2020 ballot initiative ("CPRA" or "CCPA 2.0")
- On May 4, 2020, Californians for Consumer Privacy announced that it is submitting over 900,000 signatures to qualify the CPRA for the November 3 election
  - Needs 623,212 verified signatures
- In order to become law, the initiative must
  - Pass the signature verification process
  - Then will appear on ballot unless withdrawn by proponents prior to June 25
    - Legislative compromise is less likely this time because proponents have stated CCPA was "weakened" by legislative amendments
  - Be approved by a simple majority of votes cast for or against the measure
- If passed CPRA 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 CPRA
  - Rule making authority
  - 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

SECTION 02

MODIFICATIONS TO THE CCPA DRAFT REGULATIONS

First Set of Modifications to CCPA Regulations (February 7 and 10, 2020)

- In this Section, we will only discuss the modifications introduced in the first set that remain applicable after the release of the second set of modifications. If any modification that was initially introduced in the first set was later further revised in the second set, we will cover it when we discuss the second set or explicitly note the further changes.
- Key modifications that are still applicable, include:
  - Definition of "Household"
  - Notice of collection requirements
  - Mobile application and employment notices
  - Affirmative authorization
  - Consumer requests
  - Fee for verification requests
  - Authorized agents
  - Discriminatory practices
  - Annual disclosures
  - Consumers with disabilities

First Set of Modifications – Definitions

- **Definition of "Household" –** The definition is revised to mean a person or group of people who
  - reside at the same address,
  - share a common device or the same service provided by a business, and
  - are identified by the business as sharing the same group account or unique identifier.
- To respond to a household rights request, where a consumer has a password-protected account, the business may process requests to know and delete relating to household information through the business's existing business practices.

First Set of Modifications – Notice at Collection

- Under the initial proposed regulations, businesses are not allowed to use personal information for "any purpose other than disclosed in the notice at collection."
- The modifications revise the notice at collection requirements that the business does not need to notify and obtain consent from the consumer as long as the purposes for use of personal information are not "materially different" from those disclosed in the notice at collection.

First Set of Modifications – Mobile Applications

- **Mobile Application Notices** – The modifications add new language to address mobile applications. When a business collects personal information through a mobile application, it may provide a link to the notice and opt-out requirements on the mobile application's download page and within the application, such as through the application's settings menu.
- **Unexpected Collection on Mobile Device –** When a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, the business must provide a "just-in-time" notice containing a summary of the categories of personal information being collected and a link to the full notice at collection. The modifications provide an example of a flashlight application that also collects geolocation information.
  - The practice of "just-in-time" privacy notices within an app has previously been endorsed by the Federal Trade Commission and the California Attorney General.

First Set of Modifications – Employment Notices

- The modifications clarify that a business collecting employment-related information is not required to include a "Do Not Sell My Personal Information" link in its employee and job applicant privacy notices at least until January 1, 2021, when the employment exceptions will no longer apply.

First Set of Modifications – Affirmative Authorization

- The modifications add that a business is required to obtain affirmative authorization from the consumer if the business is to sell the personal information it collected during the time the business did not have a notice of right to opt-out notice posted.

First Set of Modifications – Consumer Requests

- **Methods for Submitting Request to Know**
  - Online Businesses – A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information is only required to provide an email address for submitting requests to know.
  - Business Websites – The modifications delete the previous language suggesting that businesses that operate a website must provide an interactive web form for the submission of requests to know.

First Set of Modifications – Consumer Requests (cont.)

- **Time to Respond to Consumer Requests** – The modifications clarify the period for responding to a request to know or a request to delete in terms of business or calendar days.
  - Confirmation of receipt to know or delete – 10 *business* days
  - Responding to the request to know or delete – 45 *calendar* days (for a maximum total of 90 *calendar* days)
  - Responding to a request to opt out of sale –15 *business* days

First Set of Modifications – Consumer Requests (cont.)

- **Not Required to Search** – The modifications add language indicating that when a business responds to a request to know, the business is not required to search for personal information if the business
  - (a) does not maintain personal information in a searchable or reasonably accessible format,
  - (b) maintains the personal information only for legal or compliance purposes,
  - (c) does not sell the information or use it for a commercial purpose, and
  - (d) describes to the consumer the categories of records not searched because it satisfies the three conditions above.

First Set of Modifications – Verification Fees

- The First Set of Modifications adds that a business cannot require consumers to pay a fee for the verification of their requests to know or requests to delete.
  - For example, a business may not require a consumer to provide a notarized affidavit to verify the consumer's identity unless the business compensates the consumer for the cost of notarization.
- The Second Set of Modifications further add that this prohibition is applicable to the consumer's authorized agent.

First Set of Modifications – Authorized Agents

- The modifications expand the obligations of an authorized agent of a consumer in the following ways:
  - An authorized agent must implement and maintain reasonable security procedures and practices to protect the consumer's information.
  - An authorized agent must also not use a consumer's personal information (or any information collected from or about the consumer) for any purpose other than to fulfill the consumer's requests, for verification, or for fraud prevention.

First Set of Modifications – Discriminatory Practices

- The modifications provide that a business cannot offer a financial incentive if it is unable to calculate a good-faith estimate of the value of the consumer's data or cannot show that the financial incentive is reasonably related to the value of the consumer's data.
- The modifications add that it is not discriminatory for a business to deny a consumer's request to know, request to delete, or request to opt out for reasons permitted by the CCPA.

First Set of Modifications – Annual Disclosures

- The threshold for recordkeeping metrics and privacy notice disclosure requirements that previously applied to businesses with the personal information of 4 million consumers has been increased to businesses with the personal information of 10 million or more consumers.
- The Second Set of Modifications adds that the recordkeeping obligations are triggered when a business "knows" or "reasonably should know" that it has personal information of 10 million or more consumers.
- These businesses must disclose recordkeeping metrics by July 1 of every calendar year in their privacy notice.

First Set of Modifications – Consumers with Disabilities

- **Online notices**
  - Must be "reasonably accessible"
  - Benchmark: Web Content Accessibility Guidelines (WCAG) 2.1 Level AA
- **Offline notices**
  - Must provide information about "alternative formats" (*e.g.*, Braille)
- **Risks**
  - AG enforcement for violations
  - CCPA's private right of action doesn't extend to accessibility violations
  - **BUT** CCPA accessibility violations likely is a basis for a claim California's Disabled Persons Act and possibly California's Unruh Act.
  - Both statutes provide for statutory damages + exemplary damages + attorneys' fees + injunctive relief

Second Set of Modifications to CCPA Regulations (March 11, 2020)

- This set of modifications consists of mostly minor adjustments, introducing fewer significant new concepts than the previous iterations on October 11, 2019 and February 7 and 10, 2020.
- Key modifications address the following:
  - Definition of "Personal Information"
  - Definition of "Financial Incentives"
  - Do Not Sell button
  - Privacy policy requirements
  - Notice at collection
  - Service providers
  - Employment related privacy notices

Second Set of Modifications – Definitions

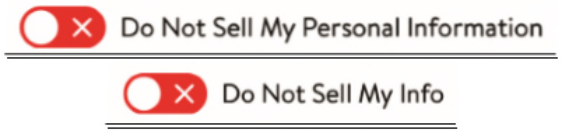
- **Definition of "Personal Information" –** The guidance in the First Set of Modifications includes an example providing that if a business collects the IP addresses of visitors to its website but does not link the addresses to any particular consumers or households, and could not reasonably link the addresses with a particular consumer or household, then the IP address would not be deemed personal information.
- The Second Set of Modifications eliminates this guidance.
- However, the CCPA statute's definition of personal information applies to information that "could be reasonably linked, directly or indirectly, with a particular consumer or household" and that definition, which is consistent with the deleted guidance, remains.

Second Set of Modifications – Definitions (cont.)

- **Definition of "Financial Incentive" –** The First Set of Modifications defines a financial incentive as *compensation for* the *disclosure, deletion, or sale* of personal information.
- The Second Set of Modifications broadens this definition to mean a program, benefit, or other offering, including payments to consumers *related to the collection, retention, or sale* of personal information. This revised definition's focus on payments "related to the collection" of personal information is likely to impact loyalty programs.

Second Set of Modifications – Do Not Sell Button

- The Second Set of Modifications eliminates the form opt-out button proposed in the First Set of Modifications seen below.



- Critics found the proposed button confusing and charged that the proposed button could be misconstrued as an actual, functioning toggle switch, rather than a logo.

Second Set of Modifications – Privacy Policy

- The First Set of Modifications deletes the requirement that a privacy policy specify the sources from which personal information is collected, as well as the business or commercial purpose for collecting personal information.
- The Second Set of Modifications *reinstates* the requirement to specify the sources of personal information that is collected. However, under this recent iteration, the sources do not have to be specified by category, which had been required under the original version of the CCPA regulations.

Second Set of Modifications – Notice at Collection

- The Second Set of Modifications adds "unique biometric data generated from measurements or technical analysis of human characteristics" to the list of sensitive data elements that a business's response to a request to know shall not include. Businesses must inform the consumer with sufficient particularity that it has collected the *type* of information.
  - For example, a business may state that it collects a fingerprint scan without disclosing the actual fingerprint scan data.
- The Second Set of Modifications also clarifies that a business that does not collect personal information directly from a consumer does not need to provide a notice at collection to the consumer if it does not sell the consumer's personal information.

Second Set of Modifications – Service Providers

- The Second Set of Modifications clarifies three aspects related to service providers as follows:
  - A service provider may collect personal information directly from a consumer, *or about a consumer*, and still qualify as a service provider under the CCPA.
  - A service provider may retain, use or disclose personal information to "*process or maintain personal information on behalf of the business that provided the personal information, or that directed the service provider to collect the personal information"* as long as it does so in compliance with the written contract for services required by the CCPA.
  - A service provider may internally use the personal information obtained in the course of providing services to build or improve the quality of its services but it cannot use it to provide services to another business.

Second Set of Modifications – Employment-Related Privacy Notices

- The Second Set of Modifications provides that the notice at collection of employment-related information is not required to provide a link to the business's privacy policy at least until January 1, 2021.

SECTION 03

APPROACHING JULY 1 ENFORCEMENT

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 is inclined to keep 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.

CCPA Enforcement – Industry Efforts to Delay Enforcement

- Businesses are taking actions to push the July 1 enforcement deadline to a later date in light of the COVID-19 crisis.
- March 17, 2020 Letter: A coalition of 35 companies, organizations, and trade associations, including the Association of National Advertisers (ANA), requested the July 1 enforcement deadline be postponed until January 2, 2021 in a letter addressed to the Attorney General. The letter states two reasons for the requested postponement:
  - the disruptions to businesses's CCPA compliance efforts (e.g. absence of an on-site staff to build and implement necessary systems for compliance)
  - the need for additional time to implement the yet-to-be-finalized CCPA regulations
- March 20, 2020 Letter: Another letter was sent to the Attorney General by a larger coalition of over 60 industry groups restating the same concerns.

Background – Civil Penalties

- **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"

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"

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?

SECTION 04

COMPLIANCE IN THE CURRENT ENVIRONMENT

Preparing for July 1 – Practical Steps

- Data mapping and forming 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 type of sensitive data (i.e. SSNs, ID numbers, fingerprint scan) are you collecting?
    - Regs require businesses to inform the consumer with "sufficient particularity" the type of sensitive personal information they collect
  - What methods should you make available for receiving consumer requests?
    - Are toll-free number and website form sufficient, or is another method needed to "reflect the manner in which the business primarily interacts with the consumer"?

Preparing for July 1 – Practical Steps (cont.)

- Amend website privacy policy
- Commence service provider agreement amendment/contracting process
  - Notifications versus written amendments
- For the right of access, create a "readily useable format" for the consumer
- Remote CCPA training for "individuals responsible for handling consumer inquiries"
  - Proposed regs say training should cover "all requirements" in the regs and how to direct consumers to exercise their CCPA rights
- Update document retention policies to ensure that all CCPA consumer request records are maintained for at least 24 months
  - Create "reasonable security procedures and practices" in maintaining these records.
- Update mobile applications to add notices and a link to privacy policy

Preparing for July 1 – Practical Steps (cont.)

- Perfect CCPA compliance on July 1 is impossible because the regulations are still a work in progress and they will likely be finalized right before the July 1 enforcement deadline not leaving sufficient time for businesses to make operational changes, especially at a time when businesses are dealing with operational disruptions due to COVID-19
  - 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

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. In a Chambers USA ranking, Reece was recognized by his peers as "a consummate expert in privacy matters."

Gregory T. Parks

Gregory T. Parks
Philadelphia
+1.215.963.5170
gregory.parks@morganlewis.com

Greg Parks is the co-leader of the firm's privacy and cybersecurity practice and retail & eCommerce industry sector. Greg counsels and defends retail companies and other consumer facing clients in matters related to privacy and cybersecurity, class actions and Attorney General actions, consumer protection laws, loyalty and gift card programs, retail operations, payment mechanisms, product liability, waste management, shoplifting prevention, compliance, antitrust, and commercial disputes. In the aftermath of data breaches—he's advised on more than 800 breaches in his career—Greg helps clients craft immediate responses. He counsels them on how best to give notice to affected individuals or government and consumer reporting entities, following proper compliance protocol. He also represents these companies on any data class action and other litigation stemming from the incidents, and instructs them on implementing policies and procedures to prevent and mitigate future breaches.

Mark L. Krotoski

Mark L. Krotoski
Silicon Valley
+1.650.843.7212
mark.krotoski@morganlewis.com

- Litigation Partner, Privacy and Cybersecurity and Antitrust practices with more than 20 years' experience handling cybersecurity cases and issues.
- Co-Head of Privacy and Cybersecurity practice
- 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.

Stephanie Schuster

Stephanie Schuster
Washington, DC
+1.202.373.6595
stephanie.schuster@morganlewis.com

Stephanie Schuster is an appellate litigator who helps clients navigate complex and cutting-edge issues from the earliest stages of litigation through appeal. Stephanie has delivered oral arguments in federal and state appellate courts and litigated more than 50 appeals in the areas of retail, technology, telecommunications, bankruptcy, tax, commercial, insurance, civil rights, arbitration, and constitutional law. Stephanie also litigates and counsels on issues involving the Americans with Disabilities Act (ADA) and new technologies, such as websites, mobile applications, and autonomous vehicle solutions.

Kristin M. Hadgis

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

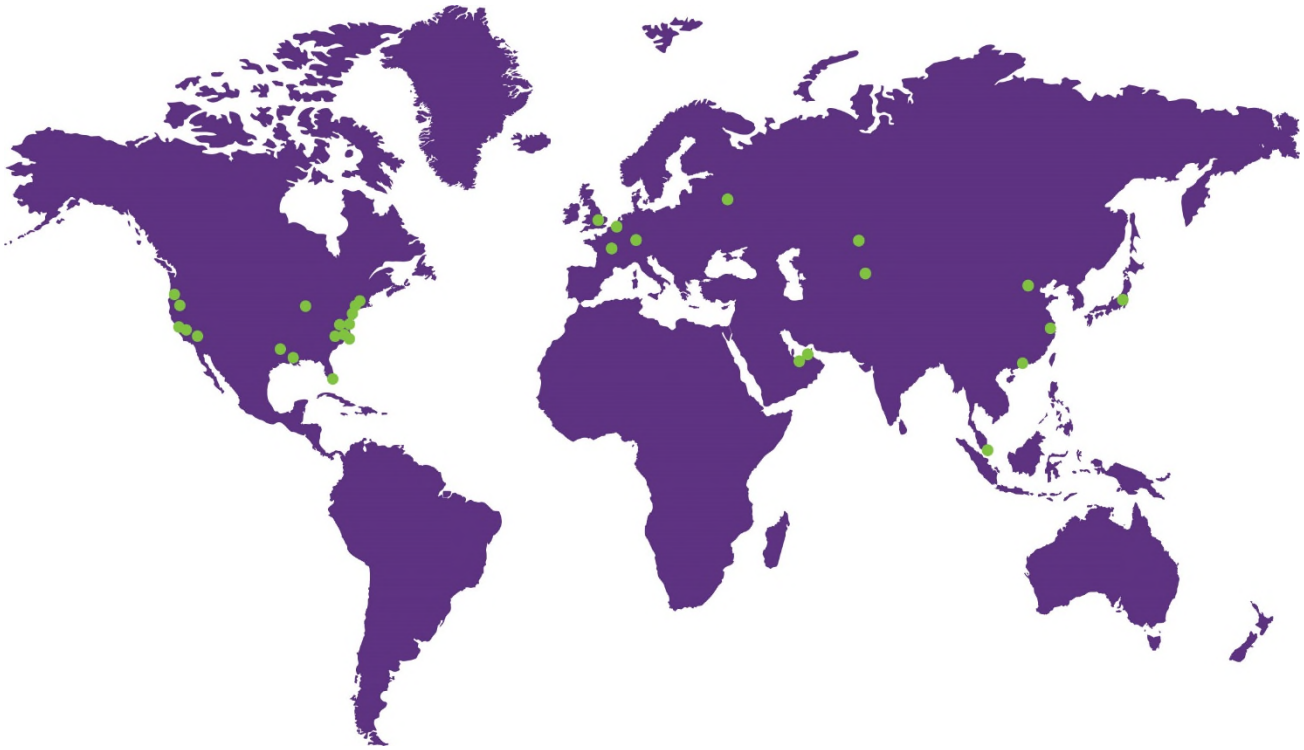
Kristin has represented companies faced with class actions and government investigations, and has advised hundreds of companies in connection with data breaches and privacy and cybersecurity compliance issues such as privacy policies, information security policies, incident response plans, and protocols for data collection, storage, and transfer. Her experience includes the General Data Protection Regulation (GDPR), state data security laws, the Fair Credit Reporting Act (FCRA), the Fair and Accurate Credit Transactions Act (FACTA), US federal and state CAN-SPAM laws, the Telephone Consumer Protection Act (TCPA), Federal Trade Commission (FTC) rules, the Securities and Exchange Commission privacy regulations (Reg. S-P), the Children's Online Privacy Protection Act (COPPA), and the Family Educational Rights and Privacy Act (FERPA).

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