Morgan Lewis

TECHNOLOGY MAY-RATHON

California Consumer Privacy Act (CCPA) What Should I Do Now?

May 30, 2019

Gregory T. Parks
W. Reece Hirsch
Mark L. Krotoski
Kristin M. Hadgis

Agenda

- California Consumer Privacy Act (CCPA) – Background and Basics
- Status of Legislative Amendments
- What to DO:
  - Privacy policy
  - Consumer requests for information, deletion, or do not sell
  - Other steps
- Enforcement
- Other States

California Consumer Privacy Act (CCPA) -- Background

- Privacy advocates seeking ballot initiative
- Law passed under tight deadline to remove ballot initiative
- Original effective date 1.1.2020; Amendment effectively pushes to 7.1.2020
- Broad obligations to respond to "consumer requests" for information, to stop selling information, and to delete information

Broad Definition of Personal Information

- Identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.
- Examples:

• Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, and passport number

• Signature, physical characteristics or description, telephone number, insurance policy number, education, employment, employment history, or financial account information

• Characteristics of protected classifications under California or federal law (race, gender, national origin, etc.)

• Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies

• Biometric information

•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

• Geolocation data

• Audio, electronic, visual, thermal, olfactory, or similar information

• Professional or employment-related information

• Education information that is not publicly available

• Inferences drawn from any of the information listed above to create a profile about a consumer

Exclusion for "Aggregated Data"

- Excluded from this definition is "aggregate consumer information"
- Data that is "not linked or reasonably linkable to any consumer or household, including via a device," as well as information that is "publicly available from federal, state, or local government records"
- Gets back to question of anonymization

CCPA New Privacy Policy Requirements

- 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
- Must have a "do not sell my personal information" button on home page

CCPA Consumer Requests for Information

- Business must respond to requests for "specific pieces of personal information collected" and the sharing of that information
- Within 45 days – by mail or electronically
- Response must include portable data where reasonably possible
- Exception for one-time transactions

CCPA Consumer Requests for Deletion

- Must also delete information when consumer requests
- Exceptions – where necessary to keep to:
  - Complete a transaction
  - Compatible with the purposes for which it was originally gathered
  - Detect or respond to security incidents or illegal activity
  - Comply with a legal obligation

CCPA -- 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"

[§ 1798.150(a)(1)]

CCPA Amendments in the Pipeline

- Seven CCPA amendment bills are currently advancing through the California Legislature, most notably:
  - AB 25: Excludes a business's employees as "consumers," so long as the information processed is in the context of an employee relationship
  - AB 846: Makes clear that customer loyalty programs can be reconciled with CCPA requirements
  - AB 981: Would exempt insurance institutions, agents and support organizations subject to the Insurance Information and Privacy Protection Act (IIPPA)
  - AB 873: Clarifies the definitions of "personal information" and "de-identified" by removing the terms "household" and "capable of being associated with"
  - AB 1564: Instead of requiring a business to maintain two or more designated methods for consumers to submit CCPA requests, only a toll-free telephone number OR an email address would be sufficient

And One That's No Longer in the Pipeline

- SB 561
  - Introduced by Sen. Hannah-Beth Jackson and supported by CA AG Xavier Becerra and would have:
    - Eliminated the CCPA provision that gives companies 30 days to cure a violation of the law before a private action may be brought
    - Expanded the private right of action to apply to all violations of the CCPA, not just security breaches
- On May 16, the California Senate Appropriations Committee blocked the progress of SB 561

CCPA Checklist – 14 Steps

CHECKLIST

1. Determine whether the California Consumer Privacy Act (CCPA) applies to your business.

- **A business is only subject to the CCPA if it**
  - Is for profit
  - Does business in California
  - Collects consumers' personal information
  - Determines the purposes and means of processing consumers' personal information
- **In addition, the CCPA only applies to a business that**
  - Has annual gross revenue in excess of $25 million
  - Annually buys, receives for commercial purposes, sells, or shares for commercial purposes personal information of 50,000 or more consumers, households, or devices, or
  - Derives 50% or more of its annual revenue from selling consumers' personal information
- **Exceptions: The CCPA does not apply to**
  - Medical information collected by a covered entity governed by the Health Insurance Portability and Accountability Act (HIPAA) or California Confidentiality of Medical Information Act (CMIA); entities subject to HIPAA or CMIA; or information collected as part of a clinical trial
  - Personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act or California Financial Privacy Information Act
  - Information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994
  - The sale of personal information to or from a consumer reporting agency to be reported in or used to generate a consumer report
  - Efforts to comply with federal, state, or local law; a civil, criminal, or regulatory investigation; or a subpoena or summons
  - Cooperation with law enforcement agencies or exercising/defending legal claims

2. Determine what data elements are collected from California consumers and for what purposes they are used.

- The scope of "personal information" under the CCPA is broad and includes any information that "identifies, relates to, describes, references, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including the following 11 enumerated categories of consumer information:
  1. Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, and passport number
  2. Personal information under California's records destruction law (Cal. Civ. Code § 1798.80(e)), which additionally includes signature, physical characteristics or description, telephone number, insurance policy number, education, employment, employment history, or financial account information
  3. Characteristics of protected classifications under California 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. 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
  7. Geolocation data
  8. Audio, electronic, visual, thermal, olfactory, or similar information
  9. Professional or employment-related information
  10. Education information that is not publicly available personally identifiable information, as defined in the Family Educational Rights and Privacy Act (20 USC § 1232(g), 34 CFR Part 99)
  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, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
- Excluded from this definition is "aggregate consumer information," which is defined as data that is "not linked or reasonably linkable to any consumer or household, including via a device," as well as information that is publicly available from federal, state, or local government records.

3. Consider how consumers' personal information should be organized.

- Provide required CCPA notices and opt-out and opt-in rights (see steps 4, 5, 10)
- Delete data to comply with the CCPA's right to be forgotten (see steps 4, 5, 8, 9)
- Provide consumer data upon request in a "readily useable format" (see step 6)
- Ensure that agreements with service providers are CCPA compliant (see step 12)
- Train personnel to properly process new requests to exercise privacy rights (see step 11)

4. Revise your website's home page.

- **Right to opt out of sale of personal information to third parties**. Businesses must provide notice to consumers that their personal information may be sold and inform consumers that they have the right to opt out of such sale. In order to comply with this right to opt out, a business must post a "clear and conspicuous link" on its website's home page titled "Do Not Sell My Personal Information," and describe the right and include a link to the "Do Not Sell My Personal Information" page in its privacy policy (see step 5).
- **Right to be forgotten**. Businesses must also inform consumers of their right to be forgotten. The CCPA does not state how consumers should be informed of this right. Paths to compliance could include adding instructions in the privacy policy or having a link on the home page

5. Revise your privacy policy.

- **Right to know**. Businesses covered by the CCPA must disclose, at or before the point of collection, in their website privacy policy or otherwise, the following:
  - The categories of personal information to be collected about the consumer and the purposes for which the information will be used
  - The categories of consumers' personal information that were actually collected in the preceding 12 months and sold or disclosed for business purposes in the preceding 12 months
- **Right to be forgotten**. Businesses must also inform consumers of their right to be forgotten. The CCPA does not state how consumers should be informed of this right, but one of the best paths to compliance would be to add such a provision to the privacy policy.
- **Right to opt out of sale of personal information to third parties**. As mentioned in step 4, in order to comply with the right to opt out, a business must describe the right and include a link to the "Do Not Sell My Personal Information" page in its privacy policy.

6. Create a process and identify individuals responsible for preserving copies of "specific pieces of personal information that the business has collected about [each] consumer" and promptly responding to consumers' requests to access same.

- Such information must be delivered free of charge to a consumer within 45 days, by mail or electronically.
- Information provided pursuant to a request must be portable, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity "without hindrance."
- There is an exception for personal information that is collected for "single, one-time transactions."

7. Create a documented process (including, but not limited to, a toll-free number and website address) and identify individuals responsible for responding to "verifiable consumer requests" with individualized disclosures about the business's collection, sale, or disclosure of the personal information belonging to the specific consumer making the request.

- Businesses must make available two or more designated methods for the consumer to request this information, including, at a minimum, a toll-free telephone number and website address (if the business maintains a website).
- Consumers have the right to make such requests twice in any 12-month period.
- In response to such requests, the CCPA requires businesses to disclose
  - The categories of personal information the business collected about the consumer
  - The categories of sources from which personal information is collected
  - The business or commercial purpose for collecting or selling personal information
  - The categories of third parties with whom the business shares personal information
  - The specific pieces of personal information the business has collected about the consumer
  - The categories of the consumer's personal information that were sold or disclosed for business purposes in the 12 months preceding the consumer's verifiable request

8. Create policies that reconcile the CCPA's requirement to delete data upon request with the need to preserve evidence in litigation and avoid sanctions for spoliation of evidence.

9. Create a process and identify individuals responsible for deleting consumer data in response to such a request.

- Exceptions to such requests include where retention of the consumer's personal information is necessary to
  - Complete a transaction for which the personal information was collected, provide goods and services to the consumer, or otherwise perform a contract with the consumer
  - Detect security incidents, fraud, or illegal activity
  - Exercise free speech, or ensure the right of another consumer to exercise his or her right of free speech
  - Enable internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business
  - Comply with a legal obligation
  - Otherwise use the consumer's personal information internally and in a lawful manner that is compatible with the context in which the consumer provided the information

10. Provide minors with a "right to opt in."

- Businesses are prohibited from selling personal information of consumers between the ages of 13 and 16 without first obtaining affirmative opt-in consent (1) from the consumer or (2) from a parent or guardian where the consumer is under the age of 13.

11. Provide training for employees on the CCPA's prescribed consumer rights.

- Businesses must ensure that personnel responsible for handling consumer inquiries regarding these new privacy rights are informed of the applicable requirements and know how to direct consumers to exercise those rights.

12. Review existing agreements with third parties or service providers to ensure that contracts limit the service provider's use of personal information as strictly as the CCPA prescribes, and revise as needed.

- The CCPA allows businesses to share personal information with third parties or service providers for business purposes, so long as there is a written contract prohibiting the third party or service provider from selling the personal information or "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."
- The CCPA defines "business purpose" as "the use of personal information for the business's or service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which it was collected." The CCPA enumerates 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, and providing analytic services; and undertaking internal research for technological development and demonstration.
- 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.

13. Provide consumers the 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
  - Denying goods or services to a consumer
  - Charging a consumer a different price or rate for goods or services including through the use of discounts or other benefits
  - Imposing penalties on a consumer
  - Providing a consumer with a different level of quality or service
  - Suggesting a consumer will receive a different price or rate or different level of quality of goods or services

14. Create and maintain a robust incident response plan.

- While implementing a robust incident response plan has been a best practice for some time, the CCPA's new statutory damages and civil penalties further underscore the need for a thoughtful and comprehensive approach to breach response because the act will almost certainly lead to a spike in data breach-related litigation in California.

Morgan Lewis

Determine Whether the California Consumer Privacy Act (CCPA) Applies to Your Business

- **Thresholds** – for profit, collects information, "determines the purposes and means of processing"
- **Big business –** revenue > $25 million, personal information of 50k, or 50% of revenue from selling personal information
- **Exceptions (double-edged sword):**
  - Financial information subject to GLBA
  - Medical information subject to HIPAA
  - Driver information subject to DPPA
  - Consumer Report subject to FCRA and CCRA
  - Law enforcement information or co-operation

Determine What Data Elements are Collected from California Consumers and for What Purposes They are Used

- Collection:
  - Online
  - In person
  - Through paper
- Use:
  - Marketing
  - Employment
  - Selling

Consider How Consumers' Personal Information Should be Organized

- Provide required CCPA notices and opt-out and opt-in rights (see steps 4, 5, 10)
- Delete data to comply with the CCPA's right to be forgotten (see steps 4, 5, 8, 9)
- Provide consumer data upon request in a "readily useable format" (see step 6)
- Ensure that agreements with service providers are CCPA compliant (see step 12)
- Train personnel to properly process new requests to exercise privacy rights (see step 11)

Revise Your Website's Home Page

- **Right to opt out of sale of personal information to third parties**. Must post a "clear and conspicuous link" on its website's home page titled "Do Not Sell My Personal Information," and describe the right and include a link to the "Do Not Sell My Personal Information" page in its privacy policy (see step 5).
- **Right to be forgotten**. Businesses must also inform consumers of their right to be forgotten. The CCPA does not state how consumers should be informed of this right. Paths to compliance could include adding instructions in the privacy policy or having a link on the home page.

Revise Your Privacy Policy

- **Right to know**. Businesses covered by the CCPA must disclose, at or before the point of collection, in their website privacy policy or otherwise, the following:
  - The categories of personal information to be collected about the consumer and the purposes for which the information will be used
  - The categories of consumers' personal information that were actually collected in the preceding 12 months and sold or disclosed for business purposes in the preceding 12 months
- **Right to be forgotten**. Businesses must also inform consumers of their right to be forgotten. The CCPA does not state how consumers should be informed of this right, but one of the best paths to compliance would be to add such a provision to the privacy policy.
- **Right to opt out of sale of personal information to third parties**. As mentioned in step 4, in order to comply with the right to opt out, a business must describe the right and include a link to the "Do Not Sell My Personal Information" page in its privacy policy.

Specific Pieces of Personal Information That the Business has Collected about [each] Consumer

- Such information must be delivered free of charge to a consumer within 45 days, by mail or electronically.
- Information provided pursuant to a request must be portable, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity "without hindrance."
- There is an exception for personal information that is collected for "single, one-time transactions."

Create a Documented Process (Including, but not Limited to, a Toll-Free Number and Website Address)

- Businesses must make available two or more designated methods for the consumer to request this information, including, at a minimum, a toll-free telephone number and website address (if the business maintains a website).
- Consumers have the right to make such requests twice in any 12-month period.
- In response to such requests, the CCPA requires businesses to disclose
  - The categories of personal information the business collected about the consumer
  - The categories of sources from which personal information is collected
  - The business or commercial purpose for collecting or selling personal information
  - The specific pieces of personal information the business has collected about the consumer
  - The categories of the consumer's personal information that were sold or disclosed for business purposes in the 12 months preceding the consumer's verifiable request

Create a Process and Identify Individuals Responsible for Deleting Consumer Data in Response to Such a Request

- Exceptions to such requests include where retention of the consumer's personal information is necessary to
  - Complete a transaction for which the personal information was collected, provide goods and services to the consumer, or otherwise perform a contract with the consumer
  - Detect security incidents, fraud, or illegal activity
  - Exercise free speech, or ensure the right of another consumer to exercise his or her right to free speech
  - Enable internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business
  - Comply with a legal obligation
  - Otherwise use the consumer's personal information internally and in a lawful manner that is compatible with the context in which the consumer provided the information

Provide Minors With a "Right to Opt in"

- Businesses are prohibited from selling personal information of consumers between the ages of 13 and 16 without first obtaining affirmative opt-in consent (1) from the consumer or (2) from a parent or guardian where the consumer is under the age of 13

Provide Training for Employees on the CCPA's Prescribed Consumer Rights

- Businesses must ensure that personnel responsible for handling consumer inquiries regarding these new privacy rights are informed of the applicable requirements and know how to direct consumers to exercise those rights.

Review Existing Agreements with Third Parties or Service Providers to Ensure that Contracts Limit the Service Provider's use of Personal Information as Strictly as the CCPA Prescribes, and Revise as Needed

- The CCPA allows businesses to share personal information with third parties or service providers for business purposes, so long as there is a written contract prohibiting the third party or service provider from selling the personal information or "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."
- The CCPA defines "business purpose" as "the use of personal information for the business's or service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which it was collected." The CCPA enumerates 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, and providing analytic services; and undertaking internal research or technological development and demonstration.
- 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

Provide Consumers the 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
  - Denying goods or services to a customer
  - Charging a consumer a different price or rate for goods or services including through the use of discounts or other benefits
  - Imposing penalties on a consumer
  - Providing a consumer with a different level of quality or service
  - Suggesting a consumer will receive a different price or rate or different level of quality of goods or services

Create and Maintain a Robust Incident Response Plan

- While implementing a robust incident response plan has been a best practice for some time, the CCPA's new statutory damages and civil penalties further underscore the need for a thoughtful and comprehensive approach to breach response because the act will almost certainly lead to a spike in data breach-related litigation in California.

CCPA - Attorney General Enforcement

- **Attorney General Rule Making**

- Concluded preliminary public forums on March 5, 2019:
  - San Francisco (Jan. 8, 2019)
  - San Diego (Jan. 14, 2019)
  - Inland Empire/Riverside (Jan. 24, 2019)
  - Los Angeles (Jan. 25, 2019)
  - Sacramento (February 5, 2019)
  - Fresno (February 13, 2019)
  - Stanford (March 5, 2019)

- Concluded comment period on rule making on March 8, 2019.

CCPA - Attorney General Enforcement

Attorney General Rule Making

- Establishing rules and procedures:
  - Submission of a request by a **consumer to opt-out** of the sale of personal information.
  - Business **compliance with a consumer's opt-out request**.
  - Development and use of "a **recognizable and uniform opt-out logo or button** by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information."
  - business **notices and information** "in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer" (including for financial incentive offerings).
  - Consumer's **ability to obtain information upon request**, "with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business" and pertaining to a business' determination that a request for information received by a consumer is a verifiable consumer request.

CCPA - Attorney General Enforcement

Attorney General Rule Making

- Updating categories of personal information
- Updating definition of unique identifiers
- Establishing CCPA exceptions for businesses to comply with state or federal law (including trade secrets and intellectual property rights)
- Adjusting the CCPA monetary thresholds for businesses
- AG "may adopt **additional regulations as necessary** to further the purposes of" the CCPA

CCPA - 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 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"

[§ § 1798.155, 1798.150]

More States Are Following Suit

- Not surprisingly, other states are introducing "CCPA-like" legislation:
  - Hawaii
  - Maryland
  - Massachusetts
  - New Jersey
  - New Mexico
  - New York
  - North Dakota
  - Rhode Island
  - Washington

Hawaii (SB 418)

- Introduced 1.18.19.
- Identifying information: "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"; does not include publicly available information.
- "Business" not defined; appears to apply to all companies doing business in Hawaii.
- Would require businesses to:
  - Disclose a consumer's identifying information upon request;
  - Identify third parties to whom the business has sold or transferred identifying information about a consumer upon request;
  - Publicly disclose, at or before the time of collection, the categories of identifying information collected from consumers and the purposes for collection;
  - Delete identifying information collected from a consumer upon request and allow consumers to opt out of the sale of their identifying information; and
  - Require opt-in consent from all consumers under 16.
- No private cause of action.
- Attorney general enforcement not specified.

Maryland (SB0613)

- Introduced 2.4.19.
- Personal information: "information relating to an identified or identifiable consumer and information that identifies, relates to, describes, as capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device"; does not include publicly available information.
- Applies to: for-profit entities that:
  - Have $25M+ in revenue;
  - Collect personal information from more than 100,000 consumers; or
  - Derive more than half of revenue from third-party disclosure of personal information.
- Would require businesses to:
  - Establish a means for consumers to submit requests for information; and
  - Provide notice, at or before collection, regarding what personal information will be collected and why.
- Includes a broader right to deletion of data than the CCPA, allowing consumers to demand deletion of any of their personal information a business maintains, regardless of the source of the data.
- No private cause of action.
- Attorney general enforcement: $2,500 per violation ($7,500 if intentional).

Massachusetts (S. 120)

- Introduced 1.11.19.
- Personal information: "any information relating to an identified or identifiable consumer"; "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device"; does not include publicly available information.
- Applies to: for-profit entities that collect personal information from Massachusetts residents and:
  - Have $10M+ in revenue; or
  - Derive more than half of revenue from third-party disclosure of personal information.
- Would require businesses to:
  - Provide notice, at or before collection, regarding what personal information will be collected and why; and
  - Allow consumers to request a copy of collected personal information, request deletion of collected personal information, and opt out of any transfers of their personal information to other businesses.
- Would create a private cause of action for consumers who allege that their personal information or biometric data was improperly collected or distributed, and would not require proof of actual damages.
- Attorney general enforcement: $2,500 per violation ($7,500 if intentional).

New Jersey (S2834)

- Introduced 7.23.18.
- Personally identifiable information: "any information that personally identifies, describes, or is able to be associated with a customer of a commercial Internet website or online service."
- Applies to: operators of Internet websites or online services that collect and maintain personally identifiable information from a customer and that are operated for commercial purposes.
- Would require businesses to:
  - Provide notice in privacy policy that includes, at a minimum, a complete description of the PII collected, third parties to which it may disclose such PII, and an email address or toll-free telephone number that the customer may use for specific privacy inquiries;
  - Clearly and conspicuously post on website or online service homepage a link titled "Do Not Sell My Personal Information," enabling the customer to opt out of the disclosure of the customer's PII; and
  - Within 30 days of a request from a customer, provide the following information at no cost: (1) the customer's PII that it disclosed in the past 12 months and (2) the names and contact information for the third parties that received the customer's PII.
- Attorney general enforcement and private cause of action not specified.

New Mexico (SB 176)

- Introduced 1.2.19.
- Personal information: "information, other than publicly available information, from federal, state or local government records that identifies, describes or could reasonably be linked with a particular consumer or household."
- Applies to: corporations, partnerships, LPs, LLCs, joint ventures, real estate investment trusts, and sole proprietors.
- Would require businesses to:
  - Allow consumers to access, request deletion of, and opt out of the sale of their personal data;
  - Provide notice, at or before collection, regarding what personal information will be collected and why; and
  - Disclose in online privacy policy the categories of information collected, sold to third parties, and disclosed for business purposes.
- Creates a private cause of action.
- Attorney general enforcement: $10,000 per violation.

New York (S00224)

- Introduced 1.9.19.
- Personal information: "any information that identifies or references a particular individual or electronic device, including, but not limited to, a real name, alias, postal address, telephone number, electronic mail address, Internet protocol address, account name, social security number, driver's license number, passport number, or any other identifier intended or able to be uniquely associated with a particular individual or device."
- Applies to: all businesses doing business in NY.
- Would require businesses to:
  - Identify third parties with whom information is shared, as well as the categories of information that were shared;
  - "make available to the customer free of charge access to, or copies of, all of the customer's personal information retained by the business"; and
  - Disclose rights of customers in online privacy notices.
- Creates a private cause of action.
- Attorney general enforcement not specified.

North Dakota (HB 1485)

- Introduced 1.14.19.
- Personal information: "information that identifies, describes, or could reasonably be linked with a particular individual"; does not include publicly available information.
- Applies to entities that:
  - Have $25M+ in revenue;
  - Collect personal information from 50,000+ consumers, households, or devices; or
  - Derive more than half of revenue from selling personal information.
- Would require businesses to:
  - Allow consumers to request that businesses delete and refrain from collecting their data;
  - Refrain from disclosing an individual's personal information to anyone other than the individual without the "express written consent"; and
  - Send a brief summary of its privacy practices to the individual by "mail or electronic mail" and receive an affirmative response to obtain consent;
- Creates a private cause of action.
- Attorney general enforcement: cease-and-desist order; violation of cease-and-desist order carries $100,000-$250,000 penalty.

Rhode Island (S0234)

- Introduced 1.31.19.
- Personal information: "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household"; does not include publicly available information.
- Applies to entities that:
  - Have $5M+ in revenue;
  - Collect personal information from 50,000+ consumers; or
  - Derive more than half of revenue from third-party disclosure of personal information.
- Would require businesses to:
  - Allow consumers to access personal information, request deletion of personal information, and request information about third parties to whom their information is sold;
  - Provide notice prior to or immediately after disclosure of personal information to a third party; and
  - Maintain privacy policies explaining consumers' rights.
- Creates a private cause of action.
- Attorney general enforcement not specified.

Washington (SB 5376)

- Introduced 1.18.19.
- Personal data: "any information relating to an identified or identifiable natural person."
- Applies to:
  - Businesses that control or process data of 100,000+ Washington residents;
  - Data brokers that have data of 25,000+ Washington residents.
- Would require businesses to:
  - Allow consumers to access, update, and correct their personal data; receive their data in a portable format; and object to their data being processed for direct marketing.
  - Give notice of deployment of facial recognition technology and have humans review the results of facial recognition programs before making a decision that will have legal effects.
- No private cause of action.
- Attorney general enforcement: $2,500 per violation ($7,500 if intentional).

Morgan Lewis Technology May-rathon 2019

A full listing and of our tech May-rathon programs can be found at

https://www.morganlewis.com/topics/technology-may-rathon

Please be sure to tweet **#TechMayRathon**

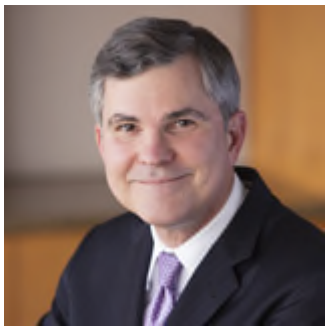
Thank you.

Gregory T. Parks

Greg 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 500 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.

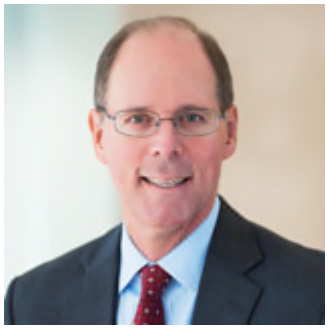
W. Reece Hirsch



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

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
+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.
- 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.

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).

THANK YOU