PROGRAM MATERIALS
Program #30284
December 16, 2020

# Inside the Proposed "New York Privacy Act"



Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 310, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969


December 16, 2020
2:00 p.m. ET
Inside the Proposed "New York Privacy Act"
PRIVACY
LOGIN >
Presented by:
Viola Trebicka, Serafina Concannon, Sophia Qasir and Dylan Bonfigli
Quinn Emanuel Urquhart & Sullivan, LLP

# Agenda

- Existing privacy regulation in the United States and globally
- Existing privacy laws in New York
- A look at the proposed New York Privacy Act
- Comparison of NYPA with existing and proposed legislation elsewhere
- Potential impact of NYPA and how to prepare

# Existing Privacy Regulation

# U.S. Privacy and Data Security Landscape

- Each of the 50 U.S. states has its own laws that govern an individual's right to privacy and/or establish a company's obligations or liabilities in the event of a data breach.
  - Privacy protections – how personal information may be obtained from an individual (notices it must provide, etc.) and what can be done with the personal information lawfully obtained from an individual.
  - Data security protections – obligations to keep an individual's personal data secure, notifications in the case of a data breach, and rules concerning liability in the event of a data breach.
- Every state has breach notification laws, which focus more on data security protections.
- Laws that focus more on comprehensive privacy protections are just starting to emerge.

# Comprehensive Privacy Legislation in the United States and Globally

- General Data Protection Regulation (GDPR) (European Union) – took effect May 2018
- California Consumer Privacy Act (CCPA) – took effect January 2020
- California Privacy Rights Act – passed November 2020 (takes effect 2023)
- Illinois Biometric Information Privacy Act (BIPA) – took effect 2008
- Nevada, An Act Relating to Internet Privacy – took effect October 2019
- Maine, An Act to Protect the Privacy of Online Customer Information – took effect July 2020
- Comprehensive privacy laws are being considered in at least 17 other states
- Several federal privacy bills also under consideration

# General Data Protection Regulation (GDPR)

- Applies to residents and citizens of the European Union.
- Provides consumers with the right to access, correct, and delete personal data collected by a company that is a data controller or processor.
- Applies to personal data, which is any piece or information that relates to an identifiable person.
- Applies to all companies that collect data of EU residents and citizens, though the protections that must be implemented need to be appropriate to the size of the company and how it uses the personal data.
- Fines imposed for smaller offenses of up to 10 million Euros or 2% of a company's global annual revenue, whichever is greater, and fines imposed for large offenses of up to 20 million Euros or 4% of company's global annual revenue, whichever is greater.
- Provides for private right of action for material and non-material damage. How "non-material damage" is calculated is still unclear and has varied from country to country.

# California Privacy Legislation – CCPA

- The California Consumer Privacy Act (CCPA) was passed in 2018 via a ballot initiative and went into effect on January 1, 2020.

- The CCPA gives consumers more control over the information that businesses collect about them and grants consumers new privacy rights, including:

  - The right to know about the personal information that businesses collect and how that information is used and shared.

  - The right to opt out of the sale of personal information.

  - A private right of action for consumers whose nonencrypted and nonredacted "personal information" is subject to an unauthorized access and exfiltration, theft, or disclosure.

  - For purposes of the private right of action, "personal information" is defined as an individual's first name or first initial and the individual's last name in combination with certain data elements, such as a social security number or driver's license number, when those data elements are not encrypted or redacted.

- The California Attorney General began enforcing the CCPA as of July 1, 2020.

# California Privacy Legislation – CPRA

- On November 3, 2020, Californians passed Proposition 24, also known as the California Privacy Rights Act of 2020 (CPRA).
- The Proposition amends the CCPA by, among other things:
  - Changing existing consumer data privacy laws by, for example, changing which businesses are subject to the CCPA and requiring that businesses notify consumers of the amount of time that they will keep personal data.
  - Providing new consumer privacy rights, such as the right to limit sharing of personal data, correct personal data, and limit the use of "sensitive" personal information (a new subset of "personal information," which includes, for example, a consumer's precise geolocation).
  - Changing existing penalties by permitting enhanced penalties for violations of the privacy rights of minors.
  - Creating a new state agency (the California Privacy Protection Agency) to oversee and enforce consumer data privacy laws in conjunction with the California Department of Justice.
- Most of the changes will take effect on January 1, 2023, although some changes, such as the creation of the new state agency, will take effect when the election results are certified in December 2020.
- The creation of a state agency to enforce the CCPA will likely result in an uptick in enforcement actions, given that the California Department of Justice was previously responsible for enforcing the CCPA but was only able to handle a few cases per year.

# Illinois Biometric Information Privacy Act (BIPA)

- Legislative intent is to protect the public by regulating the growing collection, use, handling, storage, retention, and destruction of biometric identifiers and biometric information.

- Prohibits private entities (e.g., corporations) from:

  - Collecting, capturing, purchasing, receiving, or otherwise obtaining a person's "biometric identifier" and/or "biometric information" without that person's informed written.

  - Selling, leasing, trading, or otherwise profiting from a person's "biometric identifier" and/or "biometric information"

  - Disclosing a person's "biometric identifier" and/or "biometric information" without that person's consent.

- Private entities must exercise reasonable care in storing, transmitting, and protecting from disclosure a "biometric identifier" and/or "biometric information," and such information must be stored in a manner that "is the same as or more protective" than the manner in which the entity stores other "confidential and sensitive information."

- Provides a private right of action for persons "aggrieved by a violation of the Act," and allows for actual damages or statutory damages of $1,000 if the violation was negligent or $5,000 if the violations was willful.

# Other State Privacy Laws

- Nevada, An Act Relating to Internet Privacy – took effect October 2019
  - Applies to owners or operators of internet websites or online services for commercial purposes who collect and maintain covered information from consumers who reside in Nevada and visit the website or online service and who engage in activity that constitutes a sufficient legal nexus with Nevada under the Constitution.
  - Allows consumers to opt-out of sale of covered information.
  - Covered information includes first and last name, address, email address, telephone number, social security number, identifiers allowing a person to be contacted physically or online, or other information concerning a person that, together with an identifier, makes information personally identifiable.
- Maine, An Act to Protect the Privacy of Online Customer Information – took effect July 1, 2020
  - Applies to fixed and mobile broadband internet access service (BIAS) providers
  - Requires BIAS to:
    - Provide customers with notice
    - Implement reasonable data security measures
    - Obtain opt-in consent before using, disclosing, selling, or permitting access to customer personal information

# Proposed Privacy Legislation in Other States - Washington Privacy Act (PSSB 6281)

- Did not pass in 2019; scheduled to be discussed again during 2021 legislative session.
- Would apply to entities that control or process personal data of 100,000 or more consumers, or that derive over 25% (Senate version) or over 50% (House version) of their gross revenue from the sale or personal data and process or control personal data of 25,000 or more consumers.
- Includes requirement to independently test facial recognition services for processors that provide them.
- Senate version does not contain private right of action; House version does contain private right of action to seek injunction, actual damages, treble damages, and attorneys' fees and costs.

# Proposed Federal Privacy Legislation

- Online Privacy Act of 2019 (H.R. 4978) – introduced Nov. 5, 2019
- Consumer Online Privacy Rights Act (S. 2968) – introduced Dec. 3, 2019
- Data Protection Act of 2020 (S. 3300) – introduced Feb. 13, 2020
- Consumer Data Privacy and Security Act of 2020 (S. 3456) – introduced Mar. 12, 2020
- In addition, two discussion drafts circulated in 2019:
  - United States Consumer Data Privacy Act – discussion draft circulated Nov. 27, 2019
  - Draft by House Energy and Commerce Committee circulated Dec. 18, 2019

# Proposed Federal Privacy Legislation – Comparison of Proposals

- H.R. 4978, S. 2968, and S. 3456 (as well as the two discussion drafts) generally similar:
  - Provide individuals with rights to access, delete, correct, and obtain data
  - Require notice and consent to use personal information
  - Require entities to limit how they collect and use data
  - Require entities to take steps to protect personal data by implementing physical security and cybersecurity policies
- S. 3300 differs in its approach altogether:
  - Would not impose any new privacy obligations
  - Would create new agency—Data Protection Agency—vested with power to enforce existing federal privacy laws, for e.g.:
    - Gramm-Leach Bliley Act
    - Children's Online Privacy Protection Act of 1998
    - Health Insurance Portability and Accountability Act
  - Agency would also have power to issue privacy regulations to prevent "unfair or deceptive" acts or practices in connection with the "collection, disclosure, processing, and misuse of personal data."

# Proposed Federal Privacy Legislation – Key "Sticking Points"

| Provision | H.R. 4978 | S. 2968 | S. 3456 | S. 3300 |
|---|---|---|---|---|
| Private right of action | Yes | Yes | No | No |
| Damages | "payment of damages or other monetary relief" | Civil penalty or actual damages, whichever greater | Civil penalty | "payment of damages or other monetary relief" |
| Preemption of state laws | Does not address | Only if conflict | Yes | Only if conflict |

# Existing Privacy and Cybersecurity Laws in New York

# Information Security Breach and Notification Act

- Took effect December 7, 2005
- Requires notification of data breaches that compromise personal information
- Applies to companies conducting business in New York
- Breach defined as unauthorized acquisition of computerized data
- “Personal information,” defined as information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such person

# Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)

- Expanded on prior data breach notification law (NY GBS § 899-AA) (took effect October 23, 2019)
- More businesses must comply. Applies to any entity or individual that owns or licenses private information of New York residents.
- Definition of data breach broader. Breach defined as unauthorized acquisition of computerized data *or* unauthorized access to computerized data.
- Scope of private information covered by law broader. Applies to "private information," which means either (1) personal information in combination with a social security number, identification card number, account number, credit card number, or debit card number where it can be used to access a financial account without a password or security code, or biometric information, or (2) user name or email address in combination with password or security question and answer that would permit access to account
- Notification must be made "in the most expedient time possible and without unreasonable delay."
- Notification not required if exposure of private information was inadvertent and by someone with authority to access the data, and business reasonably believes that the exposure will not likely result in misuse of the information or harm.

# NY SHIELD Act (continued)

- Enacted “reasonable security requirement” for businesses (NY GBS § 899-BB) (took effect March 23, 2020)
- Any person or business that owns or licenses computerized data that includes private information of a New York resident must develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information, including the disposal of data.
- Statute provides examples of reasonable administrative, technical, and physical safeguards, including:
  - Designating employee(s) to coordinate security program
  - Identifying reasonably foreseeable internal and external risks
  - Selecting service providers capable of maintaining appropriate safeguards and requiring them to do so
  - Detecting, preventing, and responding to attacks or system failures
  - Regularly testing and monitoring effectiveness of key controls, systems, and procedures
  - Detecting, preventing, and responding to intrusions
- Small businesses, defined as having fewer than 50 employees, less than $3 million in gross annual revenue, or less than $5 million in year-end total assets, must maintain security program but it can be shaped based on the size and complexity of the business, nature and scope of its activities, and sensitivity of the personal information that it collects from or about its consumers.
- NY attorney general may bring lawsuits on behalf of persons harmed for actual damages resulting from failure to notify.

# The Proposed New York Privacy Act

# Proposed New York Privacy Act

- Currently under consideration in the New York state legislature (S. 5642/A. 8526)
- Was expected to be voted on in 2020, but set aside due to shift in priorities.
- Key features:
  - No minimum thresholds
  - Broad definition of personal data
  - Fiduciary obligation
  - Opt-in requirement
  - Private right of action and proof of actual damages

# Proposed New York Privacy Act – No Minimum Threshold

- The proposed Act applies to any entities that conduct business in New York or produce products or services targeted to New York residents.
  - *Section 1101. Jurisdictional scope. 1. This article applies to legal entities that conduct business in New York state or produce products or services that are intentionally targeted to residents of New York state.*
- As such, the Act does not provide any limitations as to the types of businesses to which it will apply.
  - For example, there is no minimum revenue that businesses must have, or no minimum number of consumers whose personal data they use, in order for them to have to comply with the statute.
- The Act also is not limited to entities located in New York, but applies to any entity that intentionally targets New York residents.

# Proposed New York Privacy Act – Broad Definition of Personal Data

- In the definitions section (§ 1100(10)), "personal data" is defined to include:
  - *… "real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, … [IP] address, email address, account name, mother's maiden name, social security number, driver's license number, passport number, and other similar identifier"*
  - *… "employment history, bank account number, credit… [and] debit card number, insurance policy number, or any other financial information, medical information, mental health information, or health insurance information""*
  - *"commercial information" and "biometric information"*
  - *"internet or other electronic network activity information"*
  - *"historical or real-time geolocation data"*
  - *"education records," "political information," "characteristics of protected classes"*
  - *"inference drawn from any of the information described in this paragraph to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, … predispositions, behavior, attitudes, intelligence, abilities, or aptitudes"*
- Exempts "de-identified data," which is data that cannot be linked to the individual.
- Also does not include publicly available information, defined as *"information that is lawfully made available from… government records," and which does not include "biometric information collected by a covered entity about an individual without the individual's knowledge, or information used for a purpose that is not compatible with the purpose for which the information is maintained and made available in government records."*

# Proposed New York Privacy Act – Fiduciary Obligation

- The proposed Act imposes a fiduciary obligation on all legal entities subject to the Act with respect to the handling of personal data
  - *Section 1102. Data fiduciary. 1…. Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to security the personal data of a consumer against a privacy risk, and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under he circumstances."*
- The obligation is imposed regardless of any consent provided by the consumer.
- The obligation applies to affiliates as well.
- The Act provides additional information on how to comply with the fiduciary obligation:
  - *Section 1102(a) Every legal entity, or affiliate of such entity, and every controller and data broker to which this article applies shall:*
    - *(i) reasonably secure personal data from unauthorized access; and*
    - *(ii) promptly inform a consumer of any breach of the duty…*
- The Act prohibits the use of personal data in a way that will:
  - *"benefit the online service provider to the detriment of an end user;"* and
  - *"will result in reasonably foreseeable and material physical or financial harm to a consumer or would be unexpected and highly offensive to a reasonable consumer"*
- Under the Act, the fiduciary obligation "*supersede[s] any duty owed to owners or shareholders of a legal entity or affiliate thereof, controller or data broker…"*
- The fiduciary obligation is a novel concept in privacy law, as it does not appear in any other current legislation.

# Proposed New York Privacy Act – Opt-In Requirement

- Companies will be required to provide notice to all consumers prior to using their personal data.

- NYPA requires that companies obtain affirmative consent from consumers before they are able to use their personal data:

  - *Section 1103. Consumer rights. Any entity subject to the provisions of this article shall provide notice to consumers of their rights under this article and shall provide consumers* ***the opportunity to opt in or opt out of processing their personal data in such a manner that the consumer must select and clearly indicate their consent or denial of consent****.*

  - *Section 1100. Definitions… 2. "Consent" means a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a* ***written statement or other clear affirmative action****.*

  - *Section 1100. Definitions… 17. "Opt-in" means* ***affirmative, express consent*** *of an individual for a covered entity to use, disclose, or permit access to the individual's personal data after the individual has received explicit notification of the request of the covered entity with respect to that data.*

- The proposed statute does not limit the opt-in requirement to any particular purposes. As such, companies would have to obtain affirmative consent prior to collecting, processing, sharing, or selling consumers' personal data.

# Proposed New York Privacy Act – Private Right of Action

- The Act provides enforcement by the attorney general as well as by individual consumers
  - *Section 1109. Enforcement. 2. The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this article.*
  - *3. In addition to any right of action granted to any governmental body pursuant to this section, any person who has been injured by reason of a violation of this article may bring an action in his or her own name to enjoin such unlawful act, or to recover his or her actual damages, or both such actions. The court may award reasonable attorney's fees to a prevailing plaintiff"*
- Anyone injured due to a violation of the Act may bring an action; the Act does not restrict on the type of violation for which an action can be brought. As such, an action can be brought for an entity's use or sale of personal data without an individual's consent, but an action can also be brought, for example, alleging a breach of fiduciary duty or an inadequate notice to a consumer
- However, although the actions are not limited, recovery can only be obtained for actual damages suffered as a result of a violation of the Act.
- The Act also provides for reasonable attorneys' fees to be collected.

# Comparison between Proposed New York Privacy Act and California Privacy Legislation

# Side-by-Side Comparison (NYPA and California Legislation)

| Provision | New York Privacy Act | California Consumer Protection Act | California Consumer Protection Act (as amended by the CPRA) |
|---|---|---|---|
| Entities Covered | All | $25 million minimum annual revenue; or<br>Receipt, sale, or sharing of personal information of 50,000 or more consumers, households, or devices; or<br>Receipt of 50% or more of annual revenues from selling personal information | $25 million minimum annual revenue; or<br>Receipt, sale, or sharing of personal information of **100,000 or more consumers or households**; or<br>Receipt of 50% or more of annual revenues from selling **or sharing** personal information |
| Fiduciary Obligation | Yes | No | No |
| Consent | Opt-in | Opt-out | Opt-out |
| Private Right of Action | Yes – no restrictions | Yes – subject to a 30-day cure period and only where personal information compromised in data breach | Extends right of action to cover data breaches of **email addresses** along with information that would permit access to the account; clarifies that implementing security procedures after a breach "does not constitute a cure with respect to that breach" |
| Damages | Actual damages required | Statutory (up to $750) or actual damages, whichever is greater | Statutory (up to $750) or actual damages, whichever is greater |

# Potential Impact of Proposed New York Privacy Act on Businesses and Individuals, and How to Prepare

# Issues Raised During Public Hearings on NYPA Regarding Potential Impact

- June 4, 2019 Joint Hearing held by Committees on Consumer Protection and Internet and Technology
  - Concerns raised that opt-in and data fiduciary requirements will be burdensome for businesses to comply with
  - Concerns that private right of action will create vulnerability to businesses
- November 22, 2019 Hearing held by New York State Senate
  - Business and technology groups:
    - Raised concerns about development of patchwork of state private regulations, and advocated for uniform federal standard
    - Raised concerns about expense associated with compliance
    - Advocated against creation of private right of action
  - Consumer advocacy groups:
    - Lauded efforts by state legislature
    - Discussed clarification of certain definitions
    - Asked about enhanced protections against discriminatory uses of information

# Takeaways from the CCPA

- **Definition of "Private Information."** CCPA class action lawsuits have sought to test the limits of the CCPA's definition of "private information."

- For instance, in *Atkinson v. Minted, Inc.*, 3:20-cv-03869 (N.D. Cal. filed June 11, 2020), the plaintiffs initially alleged that a data breach resulted in the disclosure of consumer names, email addresses, and passwords but did not allege that the breach resulted in the exposure of consumers' names ***in conjunction with*** this sensitive information. The complaint has since been amended to include such an allegation.

- If the NYPA is enacted, plaintiffs will likely bring actions to test the scope of the broad definition of "personal data" (i.e., "information relating to an identifiable natural person"), along with its exceptions (e.g., "publicly available information").

# Takeaways from the CCPA (cont.)

- **Standing.** The CCPA defines a "consumer" as a "California resident," yet several pending CCPA class actions have sought recovery on behalf of non-California residents. *See, e.g.*, *Fuentes v. Sunshine Behavioral Health Grp. LLC*, 8:20-cv-00487 (C.D. Cal. filed Mar. 10, 2020) (Pennsylvania lead plaintiff; voluntarily dismissed on Oct. 21, 2020); *McCoy v. Alphabet Inc.*, 5:20-cv-05427 (N.D. Cal. filed Aug. 5, 2020) (New York lead plaintiff; motion to dismiss pending).

- The NYPA similarly defines a "consumer" as a "New York resident," and thus, as in California, companies would need to be cognizant of class actions that seek to assert claims on behalf of impermissibly broad classes.

# Takeaways from the CCPA (cont.)

- **Limitations on Private Right of Action.** The CCPA's private right of action applies only to "unauthorized access and exfiltration, theft, or disclosure" of personal information resulting from a business's failure to "implement and maintain reasonable security procedures and practice," but many CCPA class actions have asserted claims based on a failure to comply with other requirements, forcing defendants to seek dismissal of those claims. *See, e.g.*, *McCoy*, 5:20-cv-05427; *P. v. Shutterfly, Inc*., 4:20-cv-04960 (N.D. Cal. filed July 23, 2020) (case stayed pending mediation).

- In contrast, the NYPA would grant a private right of action to anyone injured by a violation of the NYPA, making it easier for plaintiffs to avoid dismissal at the pleading stage. Plaintiffs would, however, be required to allege and prove that they were injured as a result of a violation of the NYPA, which would likely be a contested issue in many cases.

# How Businesses Can Prepare

- Assess what personal information and how much is collected from New York residents
  - Limit information collected to what is necessary
  - What can be “de-identified”?
- Prepare notices to consumers that their personal information is being used and of their rights under the NYPA
  - Notice must be reasonably accessible and easily understood
- Develop procedures for how to:
  - Keep track of consumers’ “opt-in” and “opt-out” requests
  - Address consumers’ requests to obtain copies of personal data
  - Ensure no unauthorized use or transfer of data without prior consumer consent
  - Dispose of personal data

# Thank You!

Viola Trebicka
violatrebicka@quinnemanuel.com
212-443-3000
*Los Angeles*

Serafina Concannon
serafinaconcannon@quinnemanuel.com
202-538-8000
*Washington, D.C.*

Sophia Qasir
sophiaqasir@quinnemanuel.com
212-849-7000
*New York*

Dylan Bonfigli
dylanbonfigli@quinnemanuel.com
213-443-3000
*Los Angeles*

quinn emanuel trial lawyers

# The Proposed New York Privacy Act

# STATE OF NEW YORK

5642

2019-2020 Regular Sessions

# IN SENATE

May 9, 2019

Introduced by Sens. THOMAS, CARLUCCI, MYRIE -- read twice and ordered printed, and when printed to be committed to the Committee on Consumer Protection

AN ACT to amend the general business law, in relation to the management and oversight of personal data

**The People of the State of New York, represented in Senate and Assembly, do enact as follows:**

Section 1. Short title. This act may be known and cited as the "New York privacy act".

§ 2. The general business law is amended by adding a new article 42 to read as follows:

**ARTICLE 42**

**NEW YORK PRIVACY ACT**



**§ 1100. Definitions. The definitions in this article apply unless the context clearly requires otherwise:**

**1. "Affiliate" means a legal entity that controls, is controlled by, or is under common control with, another legal entity, where the entity holds itself out as affiliated or under common ownership such that a consumer acting reasonably under the circumstances would anticipate their personal data being provided to an affiliate.**

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD10868-05-9

2. "Consent" means a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

3. "Consumer" means a natural person who is a New York resident. It does not include an employee or contractor of a business acting in their role as an employee or contractor.

4. "Controller" means the natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

5. "Data broker" means a business, or unit or units of a business, separately or together, that earns its primary revenue from supplying data or inferences about people gathered mainly from sources other than the data sources themselves.

6. "De-identified data" means:

(a) data that cannot be linked to a known natural person without additional information not available to the controller; or

(b) data (i) that has been modified to a degree that the risk of re-identification is small as determined by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data, (ii) that is subject to a public commitment by the controller not to attempt to re-identify the data, and (iii) to which one or more enforceable controls to prevent re-identification has been applied. Enforceable controls to prevent re-identification may include legal, administrative, technical, or contractual controls.

7. "Developer" means a person who creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.

8. "Identified or identifiable natural person" means a person who can be identified, directly or indirectly, in particular by reference to specific information including, but not limited to, a name, an identification number, specific geolocation data, or an online identifier.

9. "Minor" means any person under eighteen years of age.

10. "Personal data" means information relating to an identified or identifiable natural person.

(a) "Personal data" includes:

(i) an identifier such as a real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, unique personal identifier, military identification number, online identifier, Internet Protocol address, email address, account name, mother's maiden name, social security number, driver's license number, passport number, or other similar identifier;

(ii) information such as employment, employment history, bank account number, credit card number, debit card number, insurance policy number, or any other financial information, medical information, mental health information, or health insurance information;

(iii) commercial information, including a record of personal property, income, assets, leases, rentals, products or services purchased, obtained, or considered, or other purchasing or consuming history;

(iv) biometric information, including a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry;

(v) internet or other electronic network activity information, including browsing history, search history, content, including text, photographs, audio or video recordings, or other user generated-content,

non-public communications, and information regarding an individual's interaction with an internet website, mobile application, or advertisement;

(vi) historical or real-time geolocation data;

(vii) audio, electronic, visual, thermal, olfactory, or similar information;

(viii) education records, as defined in section thirty-three hundred two of the education law;

(ix) political information or information on criminal convictions or arrests;

(x) any required security code, access code, password, or username necessary to permit access to the account of an individual;

(xi) characteristics of protected classes under the human rights law, including race, color, national origin, religion, sex, age, or disability; or

(xii) an inference drawn from any of the information described in this paragraph to create a profile about an individual reflecting the individual's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, or aptitudes.

(b) The term personal data does not include publicly available information. "Publicly available information":

(i) means information that is lawfully made available from federal, state, or local government records; and

(ii) does not include biometric information collected by a covered entity about an individual without the individual's knowledge, or information used for a purpose that is not compatible with the purpose for which the information is maintained and made available in government records.

(c) Personal data does not include de-identified data.

11. "Process" or "processing" means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion, or destruction.

12. "Processor" means a natural or legal person who processes personal data on behalf of the controller.

13. "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

14. "Restriction of processing" means the marking of stored personal data with the aim of limiting the processing of such personal data in the future.

15.(a) "Sale", "sell" or "sold" means the exchange of personal data for consideration by the controller to a third party.

(b) "Sale" does not include the following: (i) the disclosure of personal data to a processor who processes the personal data on behalf of the controller; (ii) the disclosure of personal data to a third party with whom the consumer has a direct relationship for purposes of providing a product or service requested by the consumer or otherwise in a manner that is consistent with a consumer's reasonable expectations

considering the context in which the consumer provided the personal data to the controller; (iii) the disclosure or transfer of personal data to an affiliate of the controller; or (iv) the disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller's assets, if consumers are notified of the transfer of their data and of their rights under this article and affirmatively consent to the disclosure and transfer of data.

16. "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained or inferred over time from a consumer's activities across web sites, applications or online services. It does not include advertising to a consumer based upon the consumer's current visit to a web site, application, or online service, or in response to the consumer's request for information or feedback.

17. "Opt-in" means affirmative, express consent of an individual for a covered entity to use, disclose, or permit access to the individual's personal data after the individual has received explicit notification of the request of the covered entity with respect to that data.

§ 1101. Jurisdictional scope. 1. This article applies to legal entities that conduct business in New York state or produce products or services that are intentionally targeted to residents of New York state.

2. This article does not apply to:

(a) state and local governments;

(b) personal data sets to the extent that they are regulated by the federal health insurance portability and accountability act of 1996, the federal health information technology for economic and clinical health act, or the Gramm-Leach-Bliley act of 1999; or

(c) data sets maintained for employment records purposes.

§ 1102. Data fiduciary. 1. Personal data of consumers shall not be used, processed or transferred to a third party, unless the consumer provides express and documented consent. Every legal entity, or any affiliate of such entity, and every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker, in a manner expected by a reasonable consumer under the circumstances.

(a) Every legal entity, or affiliate of such entity, and every controller and data broker to which this article applies shall:

(i) reasonably secure personal data from unauthorized access; and

(ii) promptly inform a consumer of any breach of the duty described in this paragraph with respect to personal data of such consumer.

(b) A legal entity, an affiliate of such entity, controller or data broker may not use personal data, or data derived from personal data, in any way that:

(i) will benefit the online service provider to the detriment of an end user; and

(ii) (A) will result in reasonably foreseeable and material physical or financial harm to a consumer; or

(B) would be unexpected and highly offensive to a reasonable consumer.

(c) A legal entity, or affiliate of such entity, controller or data broker:

(i) may not disclose or sell personal data to, or share personal data with, any other person except as consistent with the duties of care and loyalty under paragraphs (a) and (b) of this subdivision;

(ii) may not disclose or sell personal data to, or share personal data with, any other person unless that person enters into a contract that imposes the same duties of care, loyalty, and confidentially toward the consumer as are imposed under this section; and

(iii) shall take reasonable steps to ensure that the practices of any person to whom the entity, or affiliate of such entity, controller or data broker discloses or sells, or with whom the entity, or affiliate of such entity, controller or data broker shares. Personal data fulfills the duties of care, loyalty, and confidentiality assumed by the person under the contract described in subparagraph (ii) of this paragraph, including by auditing, on a regular basis, the data security and data information practices of any such entity, or affiliate of such entity, controller or data broker.

2. For the purposes of this section the term "privacy risk" means potential adverse consequences to consumers and society arising from the processing of personal data, including, but not limited to:

(a) direct or indirect financial loss or economic harm;

(b) physical harm;

(c) psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;

(d) significant inconvenience or expenditure of time;

(e) adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;

(f) stigmatization or reputational harm;

(g) disruption and intrusion from unwanted commercial communications or contacts;

(h) price discrimination;

(i) effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the controller assessing privacy risk, that:

(A) alters that individual's experiences;

(B) limits that individual's choices;

(C) influences that individual's responses; or

(D) predetermines results; or

(j) other adverse consequences that affect an individual's private life, including private family matters, actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used.

3. The fiduciary duty owed to a consumer under this section shall supersede any duty owed to owners or shareholders of a legal entity or affiliate thereof, controller or data broker, to whom this article apples.

§ 1103. Consumer rights. Any entity subject to the provisions of this article shall provide notice to consumers of their rights under this article and shall provide consumers the opportunity to opt in or opt out of processing their personal data in such a manner that the consumer

must select and clearly indicate their consent or denial of consent. Controllers shall facilitate requests to exercise the consumer rights set forth in subdivisions one through six of this section. 1. On request from a consumer, a controller shall confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data concerning the consumer and the names of third parties to whom personal data is sold or licensed. On request from a consumer, a controller shall provide a copy of the personal data undergoing processing free of charge, up to twice annually. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. Where the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information shall be provided in a commonly used electronic form.

2. On request from a consumer, the controller, without undue delay, shall correct inaccurate personal data concerning the consumer. Taking into account the purposes of the processing, the controller shall complete incomplete personal data, including by means of providing a supplementary statement.

3. (a) On request from a consumer, a controller shall delete the consumer's personal data without undue delay where one of the following grounds applies:

(i) The personal data is no longer necessary in relation to the purposes for which the personal data was collected or otherwise processed;

(ii) For processing that requires consent under section eleven hundred five of this article, the consumer withdraws consent to processing;

(iii) The personal data has been unlawfully processed;

(iv) To comply with a legal obligation under federal, state, or local law to which the controller is subject; or

(v) The consumer otherwise requests that the data be deleted.

(b) Where the controller is obliged to delete personal data under this section that has been disclosed to third parties by the controller, including data brokers that received the data through a sale, the controller shall take reasonable steps, which may include technical measures, to inform other controllers that are processing the personal data that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation shall take into account available technology and cost of implementation.

(c) This subdivision does not apply to the extent processing is necessary:

(i) for exercising the right of free speech;

(ii) for compliance with a legal obligation that requires processing by federal, state, or local law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(iii) for reasons of public interest in the area of public health, where the processing (A) is subject to suitable and specific measures to safeguard the rights of the consumer; and (B) is processed by or under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;

(iv) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the

deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing; or

(v) for the establishment, exercise, or defense of legal claims.

4. (a) The controller shall cease processing if one of the following grounds applies:

(i) The accuracy of the personal data is contested by the consumer, for a period enabling the controller to verify the accuracy of the personal data;

(ii) The processing is unlawful and the consumer opposes the deletion of the personal data and requests the restriction of processing instead;

(iii) The controller no longer needs the personal data for the purposes of the processing, but such personal data is required by the consumer for the establishment, exercise, or defense of legal claims; or

(iv) The consumer otherwise requests that the controller cease processing.

(b) Where personal data is subject to a restriction or processing under this subdivision, the personal data shall, with the exception of storage, only be processed (i) with the consumer's consent; (ii) for the establishment, exercise, or defense of legal claims; or (iii) for reasons of important public interest under federal, state, or local law.

(c) Where a consumer has taken steps by the online selection of options related to sharing personal data a controller is obligated to adhere to such selections.

5. (a) On request from a consumer, the controller shall provide the consumer any personal data concerning such consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format if (i)(A) the processing of such personal data requires consent under section eleven hundred five of this article, (B) the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or (C) in order to take steps at the request of the consumer prior to entering into a contract; and (ii) the processing is carried out by automated means.

(b) Controllers shall transmit the personal data requested under this subdivision directly from one controller to another, where technically feasible, and transmit the personal data to another controller without hindrance from the controller to which the personal data was provided.

(c) Requests for personnel data under this subdivision shall be without prejudice to subdivision three of this section.

(d) The rights provided in this subdivision do not apply to processing necessary for the performance of a task carried out in the public interest and shall not adversely affect the rights of consumers.

6. A consumer shall not be subject to a decision based solely on profiling which produces legal effects concerning such consumer or similarly significantly affects the consumer. Legal or similarly significant effects include, but are not limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.

(a) This subdivision does not apply if the decision is authorized by federal or state law to which the controller is subject and which incorporates suitable measures to safeguard the consumer's rights and legitimate interests, as indicated by the risk assessments required by section eleven hundred five of this article.

(b) Notwithstanding paragraph (a) of this subdivision, the controller shall implement suitable measures to safeguard consumer's rights and legitimate interests with respect to decisions based solely on profil-

ing, including providing human review of the decision, to express the consumer's point of view with respect to the decision, and to contest the decision.

7. A controller shall communicate any correction, deletion, or restriction of processing carried out in accordance with subdivisions two, three or four of this section to each third-party recipient to whom the personal data has been disclosed, including third parties that received the data through a sale, unless this proves impossible. The controller shall inform the consumer about such third-party recipients, if any, if the consumer requests such information.

8. A controller shall provide information on action taken on a request under subdivisions one through six of this section without undue delay and in any event within thirty days of receipt of the request. That period may be extended by sixty additional days where necessary, taking into account the complexity and number of the requests. The controller shall inform the consumer of any such extension within thirty days of receipt of the request, together with the reasons for the delay. Where the consumer makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the consumer.

(a) If a controller does not take action on the request of a consumer, the controller shall inform the consumer without undue delay and at the latest within thirty days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller.

(b) Information provided under this section must be provided by the controller free of charge to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(c) Where the controller has reasonable doubts concerning the identity of the consumer making a request under subdivisions one through six of this section, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

(d) A controller shall conduct an internal review on any action taken upon request of a consumer under subdivisions one through six of this section.

§ 1104. Transparency. 1. Controllers shall be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that is easily understood and which includes:

(a) the categories of personal data collected by the controller;

(b) the purposes for which the categories of personal data is used and disclosed to third parties, if any;

(c) the rights that consumers may exercise pursuant to section eleven hundred three of this article, if any;

(d) the categories of personal data that the controller shares with third parties, if any; and

(e) the names and categories of third parties, if any, with whom the controller shares personal data.

2. Controllers that engage in profiling shall disclose such profiling to the consumer at or before the time personal data is obtained, includ-

ing meaningful information about the logic involved and the significance and envisaged consequences of the profiling.

3. If a controller sells personal data to data brokers or processes personal data for direct marketing purposes, including targeted marketing and profiling to the extent that it is related to such direct marketing, it shall disclose such processing, as well as the manner in which a consumer may exercise the right to object to such processing, in a clear and prominent manner.

§ 1105. Responsibility according to role. 1. Controllers and brokers shall be responsible for meeting the obligations set forth under this article.

2. Processors and brokers are responsible under this article for adhering to the instructions of the controller and assisting the controller to meet its obligations under this article.

3. Processing by a processor shall be governed by a contract between the controller and the processor that is binding on the processor and that sets out the processing instructions to which the processor is bound.

§ 1106. De-identified data. A controller or processor that uses de-identified data shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the de-identified data is subject, and shall take appropriate steps to address any breaches of contractual commitments.

§ 1107. Exemptions. 1. The obligations imposed on controllers or processors under this article do not restrict a controller's or processor's ability to:

(a) comply with federal, state, or local laws;

(b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(c) disclose personal data to a law enforcement agency if such information:

(i) was inadvertently obtained by the controller or data broker; and

(ii) appears to pertain to the commission of a crime;

(d) cooperate with a governmental entity if the controller or data broker, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure of personal data without delay;

(e) investigate, exercise, or defend legal claims; or

(f) prevent or detect identity theft, fraud, or other criminal activity or verify identities.

2. The obligations imposed on controllers or processors under this article do not apply where compliance by the controller or processor with this article would violate an evidentiary privilege under New York law and do not prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under New York law as part of a privileged communication.

3. A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this article is not in violation of this article, including under section eleven hundred eight of this article, if the third-party recipient processes such personal data in violation of this article, provided that, at the time of disclosing the personal data, the disclosing controller or processor did not have actual knowledge that the third-party recipient intended to commit a violation. A third-party recipient receiving personal data from a controller or processor is likewise not

liable under this article, including under section eleven hundred eight of this article, for the obligations of a controller or processor to whom it provides services.

4. This article does not require a controller or processor to do the following:

(a) re-identify de-identified data;

(b) retain personal data concerning a consumer that he or she would not otherwise retain in the ordinary course of business; or

(c) comply with a request to exercise any of the rights under subdivisions one through six of section eleven hundred three of this article if the controller is unable to verify, using commercially reasonable efforts, the identity of the consumer making the request.

5. Obligations imposed on controllers and processors under this article do not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

§ 1108. Liability. Where more than one controller or processor, or both a controller and a processor, involved in the same processing, is in violation of this article, the liability shall be allocated among the parties according to principles of comparative fault, unless such liability is otherwise allocated by contract among the parties.

§ 1109. Enforcement. 1. The legislature finds that the practices covered by this article are matters vitally affecting the public interest for the purpose of providing consumer protection from deceptive acts and practices under article twenty-two-A of this chapter. A violation of this article is not reasonable in relation to the development and preservation of business and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying article twenty-two-A of this chapter.

2. The attorney general may bring an action in the name of the state, or as parens patriae on behalf of persons residing in the state, to enforce this article.

3. In addition to any right of action granted to any governmental body pursuant to this section, any person who has been injured by reason of a violation of this article may bring an action in his or her own name to enjoin such unlawful act, or to recover his or her actual damages, or both such actions. The court may award reasonable attorney's fees to a prevailing plaintiff.

4. Any controller or processor who violates this article is subject to an injunction and liable for damages and a civil penalty. When calculating damages and civil penalties, the court shall consider the number of affected individuals, the severity of the violation, and the size and revenues of the covered entity. Each individual whose information was unlawfully processed counts as a separate violation. Each provision of this article that was violated counts as a separate violation.

§ 1110. Preemption. This article supersedes and preempts laws adopted by any local entity regarding the processing of personal data by controllers or processors.

§ 3. This act shall take effect on the one hundred eightieth day after it shall have become a law.

quinn emanuel trial lawyers

# Inside the Proposed "New York Privacy Act"

# Inside the Proposed New York Privacy Act

New York promises to change the privacy landscape with its proposed New York Privacy Act, which increases consumer protections as well as legal burdens on companies.

By **Viola Trebicka, Serafina Concannon and Sophia Qasir** | September 02, 2020

Step aside, California: the proposed New York Privacy Act (NYPA), S. 5642/A. 8526, 2019-20 Reg. Sess. (N.Y. 2019), if enacted in its current form, will be even more expansive than California's Consumer Privacy Act (CCPA), providing consumers with even greater control over their personal information, while at the same time being much more onerous for businesses to comply with.

The bill was expected to be voted on this legislative term, but due to the shift in priorities for the Legislature as a result of the 2019 coronavirus pandemic, it was set aside. However, the pandemic has also brought to the surface privacy issues in the public health arena, with emerging fears that there is a lag between the protection of individuals' private data and the use of technology. This may revive efforts to enact privacy laws at the state level, or a federal privacy law that may preempt state laws.

Indeed, several federal privacy bills are already under consideration, such as the Consumer Online Privacy Rights Act and the United States Consumer Data Privacy Act. As such, privacy regulation in the United States remains unsettled, but the next year may bring marked changes.

New York has had in place some form of a data breach notification law since 2005. The New York State Information Security Breach and Notification Act, enacted on December 7, 2005, required state entities and persons conducting business who own or license data that includes the private information of New York residents to inform residents, as well as credit reporting agencies, if a breach occurred that compromised such personal information.

In the last few years, however, amidst the European Union's passage of the General Data Protection Regulation 2016/679 (GDPR), as well as the CCPA, which was signed into law in mid-2018 and took effect in January 2020, the New York Legislature has also began contemplating expanding the cybersecurity legislation and enacting additional privacy protections for its own residents.

Some of this legislation has been successfully passed. For example, in the 2018-2019 session, the Legislature passed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), N.Y. Gen. Bus. Law §899-bb, which broadened the scope of the data breach notification law, including by expanding the definition of a data breach, the scope of the information covered by the law, and the data security measures that would be required to protect information to be commensurate with the size of the entity.

Alongside the revised SHIELD Act, Senator Kevin Thomas also introduced the NYPA during the 2018-2019 legislative term, and reintroduced the bill in the 2019-2020 term. The NYPA follows in the footsteps of other recent privacy regulations—notably, the GDPR and the CCPA, but is even more imposing than those regulations. For example, the NYPA establishes a fiduciary obligation on all controllers of (*i.e.*, businesses that have) personal data and requires an "opt-in" consent process.

As such, this law has proven more controversial and has not yet passed. In May 2019, the NYPA was referred to the Consumer Protection Committee of the New York State Senate, and on June 4, 2019, the Committee on Consumer Protection and Committee on Internet and Technology held a Joint Public Hearing on proposed privacy and cybersecurity legislation, including the NYPA.

At the hearing, a number of panelists raised issues with the NYPA in its current form, including concerning the burdens that would be imposed on businesses. Indeed, as discussed further below, the requirements that businesses must serve as "data fiduciaries" to consumers and that consumers must opt-in for entities to be able to collect, use, and sell their data, is more burdensome than the CCPA, and the creation of a private right of action by consumers to sue entities for non-compliance with such provisions will create more vulnerability to businesses in New York.

The New York State Senate held another public hearing on privacy legislation on November 22, 2019 in New York City. Business and technology groups raised concerns about the development of a patchwork of state privacy regulations and advocated for a uniform federal standard. They also raised concerns about the expense associated with compliance and continued to push back against the creation of a private right of action.

Consumer advocacy groups generally lauded the state Legislature's efforts and provided specific commentary on proposed definitions or specific aspects to the regulation, such as addressing the secondary use of personal data, enhanced protections against discrimination, or clarifying certain definitions.

Although the bill may still be revised before it is likely introduced in the next legislative term, and at multiple points before it is ultimately voted on by members of the New York State Legislature (and becomes effective six months after passing), a summary and analysis of the noteworthy aspects of the current draft bill are provided below to help understand the provisions at play.

**No Minimum Threshold on Covered Entities.** The NYPA is broader than the CCPA in not having a minimum revenue or consumer threshold; it would impact all entities "that conduct business in New York state or produce products or services that are intentionally targeted to residents of New York state." NYPA §1101. Some opponents of the NYPA have argued that the compliance costs associated with the NYPA will stifle business, especially start-ups and small businesses.

**Broad Definition of Personal Data.** The NYPA applies to any "information relating to an identified or identifiable natural person," and includes but is not limited to identifiers such as real name, gender identity, alias, signature, email address, employment history, financial information, commercial information such as income and assets, biometric

information, internet activity information, geolocation data, education records, political information, and protected class characteristics such as religion, age, race, and natural origin. *id.*§1100(10). This definition of "personal data" has been criticized by opponents of the NYPA as very broad.

It has also been criticized by certain consumer groups, who advocate for a narrower definition of "de-identified" data, such that the definition would only exempt personal data that "companies believe in good faith … could not be reassociated with unique individuals."

**Fiduciary Obligation.** The NYPA imposes a fiduciary duty on controllers, data brokers, and every entity (or affiliate of any entity) that "collects, sells or licenses personal information of consumers." *Id.* §1102(1). The NYPA defines "controller" as someone who "determines the purposes and means of the processing of personal data" and "data broker" as a business that "earns its primary revenue from supplying data or inferences about people gathered mainly from sources other than the data sources themselves." *Id.* §§1101(4)-(5).

These entities must "exercise the duty of care, loyalty, and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act *in the best interests of the consumer, without regard to the interests of the entity*, controller or data broker." *Id.* §1102(1) (emphasis added).

The fiduciary obligation is imposed regardless of any consent provided by a consumer. The seriousness of this obligation is highlighted by the requirement that the fiduciary duty owed to a consumer under this regulation "shall supersede any duty owed to owners or shareholders of a legal entity or affiliate thereof, controller or data broker." *Id.* §1102(3). For example, the NYPA states that entities that possess personal data may not use that data in a way that "will benefit the online service provider to the detriment of an end user." *Id.* §1102(1)(b)(i).

Furthermore, any entity subject to these regulations may not disclose, sell or share personal data with any other person or entity, unless that other person or entity assumes the same fiduciary obligations. *Id.*§1102(1)(c)(ii). This fiduciary obligation is a novel concept in the privacy regulation sphere, and may put officers and directors, who owe a duty to shareholders as well as, if the NYPA is enacted in its current form, a duty to consumers, into an untenable position of having to breach their duty to one of these two groups.

**Opt-In Requirement.** Unlike the CCPA, which gives consumers the right to "opt-out" from the sale of their personal data, the NYPA requires consumers to "opt-in" for the use of their personal data, and not just with respect to selling and sharing personal data, but even in the collection and processing of it. The "opt in" process requires the consumer to make—and the company to record—"a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of the agreement to the processing of personal data relating to the consumer." *Id.* §1100(2).

However, certain language elsewhere in the statute suggests that New York's opt-in framework will effectively operate in a manner similar to that of opt-in regimes. *See id.* §1103. However, the distinction between an "opt in" and "opt out" framework may create additional hurdles for companies depending on the documentation requirements imposed on businesses. This requirement can also more significantly disadvantage start-ups and small businesses that rely on the use of personal data for advertising and sales and are not as well-equipped to maintain records of consent.

**Private Right of Action.** In addition to permitting the attorney general to bring an action in the name of the state or on behalf of residents, the NYPA creates a private right action for consumers who were injured by reason of a violation of the NYPA to pursue civil remedies. Unlike the CCPA, which allows for the recovery of statutory damages or actual damages, whichever are greater, Cal. Civ. Code §1798.150, the NYPA limits recovery for violations of the Act in the form of injunctive relief and "actual damages." NYPA §1109(3).

This may be one of the few ways in which the NYPA is less onerous than the CCPA, as actual damages may be difficult to prove with respect to a data breach. On the other hand, whereas the CCPA limits the private right of action to where an individual's personal information was compromised in a data breach, the NYPA has no such restriction,

stating that a right of action can be brought by "any person who has been injured by reason of a violation of this article." NYPA §1109(3).

Thus, as long as actual damages can be proven, a private right of action can be brought for *any* violation of the Act. This can range from violations for an entity's sale of personal data without obtaining a consumer's consent, to an entity's failure to provide a transparent notice to a consumer containing all the information required by the NYPA.

Furthermore, while the CCPA actually restricts the private right of action to only certain personal information—namely, an individual's name, social security, identification card number, credit or debit card or account number with code or password, or medical or health insurance information, *see* Cal. Civ. Code. §1798.81.5(d)(1)(A), the NYPA has not such restrictions, thus applying to all personal data as defined in the Act. In addition, a successful plaintiff may recover attorney fees. NYPA §1109(3).

Viola Trebicka *is partner at Quinn Emanuel Urquhart & Sullivan.* Serafina Concannon *and* Sophia Qasir *are associates at the firm.*

quinn emanuel trial lawyers

# A Developing Patchwork Of Privacy Legislation In Washington

**Portfolio Media. Inc.** | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# A Developing Patchwork Of Privacy Legislation In Washington

By **Viola Trebicka and Olga Slobodyanyuk** (April 15, 2020, 5:15 PM EDT)

Viola Trebicka

Olga Slobodyanyuk

The Washington Legislature considered this session a series of bills on data privacy, facial recognition and artificial intelligence. All save one failed to pass. As a result, the California Consumer Privacy Act remains unmatched despite the efforts of many other states to pass far-reaching consumer privacy legislation.

However, the sponsors of the Washington privacy legislation indicated their willingness to renew the efforts to push through privacy legislation in the next legislative session, which starts in 2021. Staying informed of the developing patchwork legislation in the various states will continue to be vital for businesses.

This is so despite the efforts to pass federal privacy legislation, given that it remains a point of discussion as to whether federal law would displace or leave untouched stricter state legislation. If the (eventual) federal legislation lacks a sweeping preemption clause, states will continue to experiment with their own privacy statues with which businesses will have to comply.

**The Washington Privacy Act (PSSB 6281)**

Out of the proposed set of Washington state bills, the Washington Privacy Act, or WPA — a revival of a draft 2019 legislation — generated the most discussion in part because of the far-reaching privacy provisions.

The stated aim of the WPA was to provide Washington consumers the right to access, correct and delete personal data, as well as the right to opt out of the collection and use of personal data for certain purposes. It imposed affirmative obligations on certain companies to safeguard personal data and provide clear, understandable and transparent information to consumers about how their personal data is used, required data protection assessments in the collection and use of personal data, and empowered the state attorney general to obtain and evaluate a company's data protection assessments, to impose penalties where violations occur, and to prevent against future violations.[1]

The bill came very close to passing, as both the House and the Senate passed their own versions. The Senate version passed in the state Senate, by a vote of 46-1. The bill's sponsors said that the new version of the bill more clearly articulates consumers' rights, has tighter definitions, and clearer lines around enforcement.[2]

Microsoft Corp., an important player in Washington state, has publicly expressed its support

for the WPA.[3] It has received praised from industry commentators and privacy advocates for its comprehensive approach and thoughtful incorporation of CCPA and General Data Protection Regulation concepts.[4]

Advertising trade groups opposed this bill, and, among other things, argued for a narrower definition of what constitutes a "sale" that consumers would be allowed to opt out of under the privacy legislation.[5] Certain civil liberties organizations of Washington state, including the American Civil Liberties Union of Washington, did not support the WPA based on the bill's lack of moratorium against facial recognition technologies.

An amended version of the WPA was passed in the Washington House of Representatives on March 6. The House amended the bill by adding a private right of action for the enforcement of consumer data privacy rights, and changing the Senate's proposals for facial recognition provisions. The vote in the House was 56 to 41.

***Liability and Enforcement***

The Senate version of the WPA did not create a private right of action. Instead, the attorney general has exclusive authority to enforce the WPA by bringing an action. Each violation is subject to an injunction and a civil penalty of up to $7,500 per violation.

By contrast, the House version of the WPA contained a private right of action. It allowed Washington residents to bring claims under the state Consumer Protection Act, which authorizes litigants to seek an injunction, actual damages, treble damages, costs of suit, and attorney fees. This was, by all accounts, the major sticking point that caused the bill to fail.

***Jurisdictional Scope***

Both versions of the WPA covered legal entities "that conduct business in Washington or produce products or services that are targeted to residents of Washington" and either (a) control or process personal data of 100,000 or more consumers or (b) derive over a percentage of their gross revenue from the sale of personal data and process or control personal data of 25,000 or more consumers.

The Senate version of the WPA set this percentage at 50% of gross revenue. The version of the WPA that passed in the House changed the requirement to 25%.

***Facial Recognition***

The WPA contained a provision for processors that provide facial recognition services. These processors must make available an API or other technical capability, chosen by the processor, to enable controllers or third parties to conduct legitimate, independent and reasonable tests of those facial recognition services for accuracy and unfair performance differences across distinct subpopulations (defined by visually detectable characters).

If the results of independent testing show unfair performance differences and processor is able to reproduce the results using the methodology and data provided, then the processor needs to implement a plan to mitigate the identified performance differences.

The House version of the WPA contained a number of changes from the Senate version in the facial recognition portion of the bill. It had stricter consent and training requirements, and permitted disclosure in response to a court-ordered warrant.

**Facial Recognition (S.B. 6280)**

The Washington Legislature passed a bill governing use of facial recognition services by state and local government agencies. This bill requires that a state or local government agency that uses or intends to use a facial recognition service must produce an accountability report

that discloses the intent to use such a service and the purpose for using that service.[6]

The bill also identifies the criteria for the accountability report. The accountability report must include the name of the facial recognition service, the type of data it uses, its proposed use, a clear data management policy, testing procedures, potential impacts of service, and procedures for receiving feedback.[7]

Prior to finalizing the accountability report, the agency that intends to use the facial recognition service must allow for a public review and comment period and hold at least three community meetings.[8] The accountability report needs to be updated every two years.[9] It must also be communicated to the public at least 90 days before the facial recognition services goes into operational use.[10] The accountability report needs to be updated if the service is to be used for a new purpose.[11]

S.B. 6280 also mandates that state or local government agencies using facial recognition services to make decisions regarding individuals must ensure that these decisions are subject to meaningful human review.[12] The bill also contains provision regarding the testing, access, training and disclosure requirements for the facial recognition service.[13] It forbids the use of facial recognition services by government agencies for ongoing surveillance or real-time identification absent a warrant, court order or exigent circumstances.[14]

Finally, it establishes a facial recognition task force in order to provide recommendations on potential abuses and threats posed by the use of facial recognition services, the adequacy of applicable Washington state laws, and to study the quality, accuracy and efficacy of the service.[15] This bill was successfully passed by the Washington Legislature and will now head to governor's office.

**Other Potential Legislation**

In addition to the WPA, the Washington Legislature considered a number of other bills related to technology and privacy, as identified and summarized below. Some of these proposals are significant and noteworthy because they would have expanded consumer protection and enforcement of digital rights in Washington — particularly the Management and Oversight of Personal Data House Bill, Personal Data Rights House Bill, and the Biometric Data Ownership House Bill.

Of these bills, there was strong industry objection to the Management and Oversight of Personal Data House Bill, which would have imposed high penalties for violations and, similar to the House version of the WPA, created a private right of action.

***Management and Oversight of Personal Data (SHB 2742)***

This bill would have made Washington state among the first tier of states giving consumers the ability to protect their own rights to privacy and requiring companies to be responsible custodians of data as technological innovations emerge. This act would do so by explicitly providing consumers the right to access, correct and delete personal data, as well as the right to opt out of the collection and use of personal data for certain purposes.

Additionally, this act would impose affirmative obligations upon companies to safeguard personal data and provide clear, understandable and transparent information to consumers about how their personal data are used. It would also strengthen compliance and accountability by requiring data protection assessments in the collection and use of personal data.

Finally, it would empower the state attorney general to obtain and evaluate a company's data protection assessments, to impose penalties where violations occur, and to prevent against future violations. The penalties under this bill are $50,000 per violation or $100,000

per intentional violation. This bill also contains a provision that would create a private right of action. At the end of the 2020 legislative session, this bill was still in the House committee.

***Personal Data Rights (H.B. 2364)***

This proposed bill enumerates specific rights that individuals residing in Washington state have with respect to their personal data. The bill, if enacted, would require businesses to provide privacy policies to consumers, minimize the collection of personal data, avoid secondary use, secure personal data from unauthorized use, act in good faith and diligence, and not discriminate against the exercise of personal data rights.

It would empower the attorney general to enforce the proposed bill, with penalties of up to $10,000 per violation. Any individual whose rights have been violated may also bring a civil action for "declaratory relief, injunctive relief, and actual damages, but not less than statutory damages of ten thousand dollars per violation." At the end of the 2020 legislative session, this bill was still in the House committee.

***Biometric Data Ownership (H.S. 2363)***

This proposed bill affirms each person's exclusive property right in the person's biometric identifiers and instructs the office of the attorney general, in consultation with the Office of Privacy and Data Protection, to "convene a task force to examine the issues related to infringement by biometric surveillance technology on the biometric identifiers ownership rights" that would be created by the act. At the end of the 2020 legislative session, this bill is still in the House committee.

***Connected Devices (H.B. 2365)***

The proposed bill requires the Office of Privacy and Data Protection to "develop a user data transmission sticker" in order to notify Washington consumers that a device can transmit data. This sticker would need to include a graphic that is "easily identifiable and understandable to children and adults." The bill then proposed that, effective January 1, 2022, connected devices need to bear this sticker. At the end of the 2020 legislative session, this bill was still in the House committee.

***Chief Privacy Officer (H.B. 2366)***

This proposed bill would make the chief privacy officer within the Office of Privacy and Data Protection an elected position. At the end of the 2020 legislative session, this bill was still in the House committee.

***Bot Communications (H.B. 2396)***

This proposed bill regulates bot communication (i.e., communications through "an automated online account where all or substantially all of the actions or posts ... are not the result of a [natural person or corporation]") on public-facing websites, making it illegal to use a bot to communicate with a Washington resident "for the purpose of knowingly deceiving the other person about the content of the communication to incentivize a purchase or sale of goods or services in a commercial transaction," without prior disclosure that the communicator is a bot. At the end of the 2020 legislative session, this bill was still in committee in the Senate after being passed by the House.

***Connected Devices With Voice Feature (H.B. 2399)***

This proposed bill would forbid the operation of a voice recognition feature in a connected device without informing the users. The bill also forbids the voice recording from being used in advertising, disclosed to third parties, or retained anywhere other than the connected

device without prior consent. At the end of the 2020 legislative session, this bill was still in the House committee.

***Privacy Assessment Surveys of State Agencies (H.B. 2400)***

This proposed bill requires the office of privacy and data protection to conduct an annual privacy review of state agencies, provide privacy training, and otherwise coordinate data protection. At the end of the 2020 legislative session, this bill was still in committee in the Senate after being passed by the House.

***AI in Job Applications (H.B. 2401)***

This proposed bill states that if an employer uses artificial intelligence for applicant-submitted video interviews, the employer needs to provide notice to the applicants that AI will be used and obtain consent. At the end of the 2020 legislative session, this bill was still in the House committee.

***AI Enabled Profiling (H.B. 2644)***

This proposed bill prohibits the use of "artificial intelligence-enabled profiling in any place of public resort, accommodation, assemblage, or amusement," and in decision-making that produces legal effects or similarly significant effects concerning Washingtonians. It would also create a private right of action, with recovery of actual damages, statutory damages of at least $1,000 for a negligent violation and at least $5,000 for an intentional or reckless violation, in addition to attorney fees and costs. At the end of the 2020 legislative session, this bill was still in the House committee.

***Digital Equity (H.B. 2414)***

The stated purpose of the bill is to create a "digital equity capacity grant program and a digital equity competitive grant program to promote the expansion of digital equity across the state by supporting digital inclusion activities and building capacity for local jurisdictions to spur greater adoption of broadband among covered populations throughout Washington." At the end of the 2020 legislative session, this bill was still in the House committee.

Some or all of the above privacy bills are bound to be considered again in the new legislative session, which starts in 2021. It is important for businesses to remain aware of the developing patchwork of state legislation.

As the experience of the 2020 Washington legislative session demonstrates, there is currently a strong push for legislation in the privacy area — but the success of these efforts is all but guaranteed. Legislators are considering a wide array of diverse topics, not just limited to consumer data privacy, but also biometric rights, Internet of Things, bots, AI, and digital equity.

These legislative proposals also use a variety of enforcement tools, such as private rights of actions, moratoriums on certain technologies, and a wide range of statutory penalties. This results in a lot of uncertainty for businesses who need to monitor these developments. Absent federal privacy legislation with a strong preemption clause, the uncertain and patchwork situation will continue to proliferate.

---

*Viola Trebicka is a partner and Olga Slobodyanyuk is an associate at Quinn Emanuel Urquhart & Sullivan LLP.*

*article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] See § 2, ¶ 5.

[2] Monica Nickelsburg, "Sneak peek: How Washington state lawmakers plan to regulate data privacy and facial recognition," GeekWire, Nov. 18, 2019, available at https://www.geekwire.com/2019/sneak-peek-washington-state-lawmakers-plan-regulate-data-privacy-facial-recognition/.

[3] Julie Brill, "The new Washington Privacy Act raises the bar for privacy in the United States," Microsoft, Jan. 24, 2020, available at https://blogs.microsoft.com/on-the-issues/2020/01/24/washington-privacy-act-protection/.

[4] See, e.g., Pollyanna Sanderson, "It's Raining Privacy Bills: An Overview of the Washington State Privacy Act and other Introduced Bills," Future of Privacy Forum, Jan. 13, 2020, available at https://fpf.org/2020/01/13/its-raining-privacy-bills-an-overview-of-the-washington-state-privacy-act-and-other-introduced-bills/.

[5] See, e.g., Allison Grande, "Ad Groups Want Lawsuit Threat Cut From Wash. Privacy Bill," Law360, Feb. 11, 2020, available at https://www.law360.com/cybersecurity-privacy/articles/1242893/ad-groups-want-lawsuit-threat-cut-from-wash-privacy-bill?nl_pk=a86c7962-76e8-49b8-bd54-1ed6336ff41e&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy.

[6] See § 3.

[7] See § 3, ¶ 2.

[8] See § 3, ¶ 3.

[9] See § 3, ¶ 4.

[10] See § 3, ¶ 5.

[11] See § 3, ¶ 7.

[12] See § 4.

[13] See §§ 5, 6, 7, 8.

[14] See § 11.

[15] See § 10.

quinn emanuel trial lawyers

# Overview: California Privacy Rights Act (Proposition 24)

# Overview: California Privacy Rights Act (Proposition 24)

On November 3, 2020, Californians passed Proposition 24, also known as the California Privacy Rights Act of 2020 (CPRA). The proposition amends the California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100–1798.199. Among other things, the CPRA (1) changes existing consumer data privacy laws, (2) provides new consumer privacy rights, (3) changes existing penalties, and (4) creates a new state agency to oversee and enforce consumer data privacy laws. All of the changes discussed below will take effect on January 1, 2023, see CPRA § 31(a), with the exception of the creation of the new state agency, which will take effect when the election results are certified in November or December 2020, *see* CPRA § 31(b). Before these changes take effect, businesses should determine whether they will be subject to the CCPA as amended, and if so, they should modify their policies and procedures to ensure compliance. Those businesses that fail to do so could face lawsuits, administrative enforcement actions, and ultimately significant liability, especially in light of the changes to the CCPA's penalty provisions. This article summarizes some of the CPRA's most important changes.

## Changes Which Businesses Must Meet Data Privacy Requirements

The CPRA changes which businesses are subject to the CCPA. Currently, to qualify as a "business" for purposes of the CCPA, a business must satisfy at least one of three threshold requirements: (1) have an annual gross revenues in excess of $25 million, (2) annually buy, receive for the business's commercial purposes, sell, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices, or (3) derive 50 percent or more of its annual revenues from selling consumers' personal information. Cal. Civ. Code § 1798.140(c)(1). Notably, the CPRA narrows the second requirement by (1) no longer counting devices and (2) increasing the annual threshold from 50,000 to 100,000 or more consumers or households. CPRA § 14. The CPRA also amends the first requirement by specifying that "annual gross revenue" is that of the "preceding calendar year" and broadens the third requirement by covering "selling *or sharing*" consumers' personal information. CPRA § 14. Businesses, and particularly those that are subject to the CCPA by virtue of the second threshold requirement, should assess whether they will be subject to the CCPA when these changes take effect.

## Changes Existing Data Privacy Requirements

The CPRA changes the data privacy requirements that businesses must meet and, in some cases, adds new requirements.

*Disclosures Regarding Sensitive Personal Information*. Currently, the CCPA requires that businesses inform consumers of the types of personal information collected and the purposes for which that information is collected. Cal. Civ. Code § 1798.100. This requirement remains largely the same, *see* CPRA § 4, but the CPRA also creates a new category of information referred to as "sensitive personal information," which means: (1) a consumer's social security, driver's license, state identification card, or passport number; (2) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (3) a consumer's precise geolocation; (4) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; or (5) the contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication, CPRA § 14. The CPRA requires that businesses disclose the types of sensitive personal information collected, the purposes for which that information is collected, and whether that information is sold or shared. CPRA § 4. Existing CCPA notices and disclosures will need to be revised in light of these requirements.

*Retention of Personal Information.* The CPRA requires that businesses inform consumers of the length of time the business intends to retain each category of personal information, or if that is not possible, the criteria used to determine that period. CPRA § 4. The CPRA also specifies that a business cannot retain personal information "longer than reasonably necessary." CPRA § 4. Before these change takes effect, businesses will need to review their policies and procedures for retaining personal information, such as their retention schedules, to determine how best to comply with this requirement.

*Agreements with Third Parties.* The CPRA requires businesses that disclose personal information to third parties to include certain terms in their agreements with those third parties. CPRA § 4. Specifically,

their agreements must (1) specify that the personal information is sold or disclosed by the business only for limited and specified purposes; (2) obligate the third party to comply with the relevant obligations under the CCPA and to provide the level of privacy protection that is required by the CCPA, (3) grant the business the right to take reasonable and appropriate steps to ensure that the third party uses the personal information in a manner consistent with the business's obligations under the CCPA; (4) require the third party to notify the business if it determines that it no longer meets the obligations under the CCPA; and (5) grant the business the right, upon notice, to take reasonable steps to stop and remediate unauthorized use of personal information.

*Reasonable Security Procedures and Practices.* The CPRA requires that businesses implement "reasonable security procedures and practices" to prevent unauthorized or illegal access, destruction, use, modification, or disclosure of consumers' personal information. CPRA § 4. Businesses will need to evaluate and update their security procedures and practices to ensure that they are reasonable in light of the personal information collected.

## New Limits on Use of Personal Data and Right to Correction

The CPRA provides consumers with a number of new privacy rights.

*Limit Sharing of Personal Data.* Currently, the CCPA gives consumers the right to prevent businesses from selling their personal information. Cal. Civ. Code § 1798.120(a). The CPRA expands this right by giving consumers the right to prevent sharing, in addition to selling, of their personal information. CPRA § 9.

*Correct Personal Data.* The CPRA gives consumers the right to request that inaccurate personal information be corrected. CPRA § 6. The CPRA requires that businesses inform consumers of this right and requires that businesses use "commercially reasonable efforts to correct the inaccurate information as directed by the consumer." CPRA § 6. To comply with these requirements, businesses will need to establish policies and procedures to allow consumers to request corrections to personal information along with policies and procedures for investigating and responding to such requests.

*Limit Use of "Sensitive" Personal Data.* The CPRA gives consumers the right to limit businesses' use of their sensitive personal information to certain enumerated purposes, such as using the information in the manner "reasonably expected" by consumers based on the goods or services provided. CPRA § 10. To comply with this provision, businesses will need to put policies and procedures in place to ensure that they are able to segregate sensitive personal information from other personal information so that they can appropriately limit the use of consumers' sensitive personal information when consumers make such a request.

## Stricter Penalty Structure and Elimination of Cure Period

Currently, a business is in violation of the CCPA if it fails to cure any noncompliance within 30 days of being notified of such noncompliance, and the CCPA provides for civil penalties of $2,500 for each violation or $7,500 for each intentional violation. Cal. Civ. Code § 1798.155(b). These penalties are assessed in a civil action brought in the name of the people of the State of California by the Attorney General. Cal. Civ. Code § 1798.155(b). The CPRA eliminates the 30-day cure period and permits a new penalty of $7,500 for violations involving the personal information of consumers whom a business knows is under 16 years of age. CPRA § 17. And, as discussed below, the CPRA allows for the initial imposition of these penalties in administrative proceedings. CPRA § 24.10.

Currently, a consumer may bring suit under the CPPA if the consumer's nonencrypted and nonredacted personal information is "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices," Cal. Civ. Code § 1798.150(a)(1), and the consumer gave the business 30 days to cure the violation, Cal. Civ. Code § 1798.150(b). The CPRA expands this right of action to cover data breaches of email addresses along with information that would permit access to the account (e.g., a password or security question). CPRA § 16. And the CPRA clarifies that implementing reasonable security procedures and practices following a breach "does not constitute a cure with respect to that breach." CPRA § 16.

These changes add significant litigation risk, particularly for email service providers and businesses that target persons under the age of 16. Businesses will need to take steps to ensure that reasonable security procedures and practices are in place to prevent data breaches, or they run the risk of facing significant liability. And early compliance will be critical as there is no longer a guaranteed opportunity to remedy noncompliance before facing administrative penalties.

## Creates New State Enforcement Agency

The proposition creates a new agency, the California Privacy Protection Agency (CPPA), which "is vested with full administrative power, authority, and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018." CPRA § 24.1. The agency will have broad authority to "investigate possible violations" of the CCPA. CPRA § 24.8. And if the agency determines that a violation has occurred, then it may require that the violator cease and desist violation of the CCPA and/or pay an administrative fine of up to $7,500 per violation, depending on the circumstances. CPRA § 24.10. An interested party may seek review of the agency's decision in the state trial courts, subject to an abuse of discretion standard of review. CPRA § 24.16. The California Department of Justice was previously responsible for enforcing the CCPA but was only able to handle a few cases per year due to limited resources. Given that the CPPA will be funded with at least $10 million annually to oversee and enforce the CCPA (in conjunction with the Department of Justice), it is likely that there will be an uptick in government enforcement actions, increasing the importance of early and effective compliance.

## Summary

Proposition 24 effects a number of changes to the California Consumer Privacy Act, most of which will become effective on January 1, 2023. Before then, businesses will need to evaluate their policies procedures and make changes to ensure compliance. Businesses that fail to do so could face significant liability, including administrative fines and monetary damages.