GT GreenbergTraurig

# Alert | Data, Privacy & Cybersecurity

August 2019

# Preparing for Nevada, California, and New York's New Privacy Laws

As state legislatures across the country adjourn for summer recess, privacy legislation has stalled in many states. Nevertheless, organizations should be aware of several developments on the horizon, including:

- Nevada's new opt-out law is effective October 1, 2019, less than six weeks from today;
- California's legislature is set to finalize proposed amendments to the California Consumer Privacy Act (CCPA) in the next month, and the CA Attorney General's Office (AG) will be publishing proposed regulations this fall; and
- New York passed expanded data breach and security legislation effective March 21, 2020.

## Nevada's Opt-Out Privacy Law Is Effective October 1, 2019

In May 2019, Nevada passed SB 220, providing consumers with the right to opt out of the "sale" of their personal information to data brokers by website operators or anyone who runs an online service. Nevada's law comes into effect three months before the CCPA, on October 1, 2019. For more information, see GT's prior article on Nevada's new law.

## CCPA's Pending Amendments Progress Through Senate & AG Rulemaking Comments Released

Although the CCPA will be effective in just a few months, on January 1, 2020, there are several proposed amendments pending before the California Senate that could alter the application of the CCPA. On August 12, the California Legislature reconvened, and the Senate is scheduled to consider the following six Assembly Bills: AB 25, AB 846, AB 874, AB 1146, AB 1355, and AB 1564. These bills have all been ordered to a third reading, during which the author will explain the bill, and the Senate will discuss and vote on the bill.

The California Senate has until September 13 to pass the bills. Unless the Senate amended the bill, the bill then proceeds to the governor for approval. Senate-amended bills will need to be approved on a favorable Assembly concurrence vote before proceeding to the governor for approval. The governor has until October 13 to sign the bills into law.

Below is a summary of the six bills still under consideration:

| Name/Bill#/Status | Date / Sponsor | Status as of August 21, 2019 |
|---|---|---|
| **Employment Information, AB 25** | December 3, 2018, Senate amended July 11, 2019 / Chau (D) | Ordered to Third Reading |
| • Provides a temporary, partial exception for compliance with CCPA requirements with respect to the personal information of job applicants, employees, directors, officers, medical staff members, and contractors ("employment information"), which sunsets on January 1, 2021.<br>• On January 1, 2020, businesses will still have to comply with the following CCPA requirements with respect to employment information: (1) obligation to provide notice at or before collection of personal information, and (2) private right of action for data breaches. | | |
| **Customer Loyalty Programs, AB 846** | February 20, 2019, amended July 11, 2019 / Burke (D) | Ordered to Third Reading |
| • Clarifies that the financial incentives exception to the non-discrimination provision allows businesses to offer customer loyalty programs (such as rewards, coupons, points, etc.).<br>• Recent amendment bans the sale of information collected by a business through a customer loyalty program.<br>• On August 14, 2019, Senate Floor Analyses suggests California AG's office may provide additional guidance on financial incentives. | | |
| **Publicly Available information, AB 874** | February 20, 2019, amended March 25, 2019 / Irwin (D) | Ordered to Third Reading |
| • Clarifies that personal information does not include de-identified or aggregate consumer information. | | |

| | | |
|---|---|---|
| **Vehicle Information Exemptions, AB 1146** | February 21, 2019, amended June 28, 2019 / Berman (D) | Ordered to Third Reading |
| • Exempts from CCPA requirements "vehicle information" (VIN, make, model, year, odometer reading) and "ownership information" (registered owners, contact info) when it is shared between a motor vehicle dealer and the manufacturer for repair, warranty, or recall purposes.<br>• Recent amendment bans the sale of the exempted vehicle information. | | |
| **Personal information, AB 1355** | February 22, 2019, amended April 12, 2019 / Chau (D) | Ordered to Third Reading |
| • Makes several technical, corrective, and clarifying amendments to address drafting errors and duplicative language. | | |
| **Consumer privacy request for disclosure methods, AB 1564** | February 22, 2019, Senate amended July 11, 2019 / Berman (D) | Ordered to Third Reading |
| • Provides a limited exception for businesses that operate exclusively online and have a direct relationship with the consumer. The exception allows such businesses to provide only an email address as the method for submitting consumer requests, instead of mandating they have two designated methods (including at least a toll-free number). | | |

In fall 2019, the California AG's office is expected to release its Notice of Proposed Regulatory Action, to provide guidance to businesses on how to comply. The AG's preliminary rulemaking activities between January and March concluded with the release of over 1,300 pages of public comments from organizations, nonprofits, and academic institutions on a variety of topics. These submissions, and the feedback gathered during the public hearings will inform the Proposed Regulatory Action, which will address the following topics:

- The definition of Unique Identifiers and other **categories of personal information** in order to address changes in technology and data collection practices,
- Clarifying **exemptions to the CCPA**, including those relating to trade secrets and intellectual property rights,
- Establishing rules to facilitate and govern **consumer requests to exercise rights**, including requirements for verifying a consumer request,
- Requirements for **uniform opt-out button** for consumers, and
- Establishing rules for **consumer-friendly notices** and information.

After the AG publishes its Notice of Proposed Regulatory Action, there will be additional public hearings, and the public will have at least 45 days to provide comments. Based on the comments received, the AG will then determine if material changes are needed. To the extent material changes are necessary, there will be a new 15 or 45-day comment period. If no material changes are made, the AG will publish the final text of the CCPA regulations.

### New York Strengthens Data Breach Law and Establishes Reasonable Security Requirements for Computerized Data

On July 25, 2019, New York's governor signed into law New York's "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act), which comes into effect on March 21, 2020, and is enforceable by the state attorney general.

Under New York's current data breach notification law, the unauthorized acquisition of "private information" constitutes a data breach triggering a business's obligation to notify an individual of the breach. Under New York's current law, "private information" is defined as "personal information" (or "any information concerning a natural person which . . . can be used to identify such natural person") in combination with a "data element." Data elements include: social security number; driver's license number or non-driver ID card number; and account number, credit or debit card number, with any other data necessary to access a financial account. The SHIELD Act expands the definition of "private information" to include the following data elements: (a) account number, credit or debit card number, where no other data is necessary to access a financial account; (b) biometric information (such as fingerprint, voice print, retina or iris image); and (c) user name or email address with a password or security question that would permit access to an online account.

The Act also broadens the definition of "breach of the security system," which triggers notification obligations and liability, to include unauthorized "access," rather than require unauthorized "acquisition of" computerized data.

Finally, the SHIELD Act also establishes a "reasonable security requirement," which requires a business or person that owns or licenses data to implement "reasonable safeguards to protect the security, confidentiality, and integrity" of private information. Small businesses and regulated entities (entities demonstrating compliance with the Gramm-Leach Bliley Act, the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, New York's Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500), and any other New York data security statutes, rules and regulations) are exempted from the "reasonable security requirement."

Penalties may include damages for actual costs or losses incurred, including consequential financial losses. Where a business is found to have acted recklessly, a court can award civil penalties of the greater of $5,000 or $20 per instance of failed notification, provided the latter amount does not exceed $250,000.

## Authors

This GT Alert was prepared by **Gretchen A. Ramos** and **Cathy C. Shyong**. Questions about this information can be directed to:


- Gretchen A. Ramos | +1 415.655.1319 | ramosg@gtlaw.com
- Cathy C. Shyong | +1 415.655.1276 | shyongc@gtlaw.com
- Or your Greenberg Traurig attorney

Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.