Published on *The National Law Review* https://natlawreview.com

Nevada's New Privacy Law Will Go Into Effect Next Month: Are You Ready?

Article By:

Ericka A. Johnson

Lydia de la Torre

Elliot Golding

India K. Scarver

The Nevada Privacy of Information Collected on the Internet from Consumers Act (NPICICA) applies to operators of commercial websites and online services. NPICICA was amended in June 2019 through SB-220 to include a requirement to allow consumers to opt-out of certain data disclosures ("Sales"). This new law was inspired by the advent of the most stringent state US privacy law – the California Consumer Privacy Act ("CCPA"). Remarkably, it will leapfrog CCPA as it goes into effect on October 1, 2019.

This post provides a list of steps that should be considered while preparing for new privacy laws such as SB-220 and the CCPA as well as a side-by-side comparison of the obligations under both laws.

What is SB-220 and how is it different from CCPA?

Covered Entities: In effect, the scope of applicability of SB-220 tracks very closely the scope of applicability of the California Online Privacy Protection Act (CalOPPA), a California law that predates the CCPA. Unlike the CCPA (but similar to CalOPPA), SB-220 applies only to persons who own or operate websites or online services for commercial purposes ("Operators") that:

- Collect and maintain "Covered Information" from consumers who reside in Nevada and use or visit the website or online service; and
- Engage in activities that establish a sufficient nexus with the State (including intentionally directing their activities toward Nevada, consummating transactions with the State or a resident thereof, availing themselves of the privilege of conducting business in the State).

In contrast, CCPA imposes most of its obligations on for-profit organizations that process personal information from California residents and meet certain thresholds and is **not** limited to internet activity.

Exempted Entities*:* Service providers are not "Operators" under the new Nevada law. Therefore, a third party that operates, hosts or manages an Internet website or online service on behalf of its owner or processes information on behalf of the owner of an internet website or online service is not directly subject to the requirements of SB-220.[1]In addition, there are limited exemptions for: (a) financial institutions subject to GLBA, (b) entities subject to HIPAA, and (c) manufacturers of motor vehicles and persons who repair or service a motor vehicle (but only with respect to information provided by a consumer to obtain, or retrieve from a motor vehicle in connection with, a motor vehicle technology or service).

The CCPA contains a complex web of exemptions that could be expanded through the ongoing rulemaking process but, in general, does not exempt entities wholesale – only certain types of information. Further, the CCPA will also impact downstream processing by organizations that obtain personal information from businesses subject to CCPA.

Information in Scope: The Nevada law applies to "Covered Information," which means any one or more of the following items of personally identifiable information about a consumer collected by Operators through a website or online service and maintained by the operation in an "accessible form":

- First and last name;
- A home or other physical address which includes the name of a street and the name of a city or town;
- Email address;
- Phone number;
- SSN;
- An identifier that allows a specific person to be contacted either physically or online; and
- Any other information concerning a person collected from the person through the internet website or online service of the Operator and maintained by the Operator, in combination with an identifier in a form that makes the information personally identifiable.

Passively collected online information could be under the scope of the Nevada law if the term "identifier" in the last paragraph is broadly interpreted. Therefore, the scope of the new Nevada law is somewhat narrower than the CCPA's definition of "personal information," but somewhat broader than CalOPPA.

Individuals protected by the law: Both CCPA and NPICICA protect the information of consumers, but the definition of consumer is broader under CCPA. A consumer under the Nevada law is any individual that engages in *commercial activity* with a company and resides in Nevada. In contrast, the CCPA does not limit the definition of "Consumer" to only residents that engage in commercial activities with covered entities and, pending potential modifications being currently considered, should be interpreted to apply even to employee data.

Data sales: A data sale under the Nevada law means the exchange of "covered information "for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons. "Sale" does not include:

- Disclosures to service providers;
- Disclosures at consumer's request;
- Disclosures for purposes which are consistent with the reasonable expectations of a consumer considering the context;

- Disclosure affiliates of the operator; or
- Disclosures in the context of M&A operations and/or bankruptcy proceedings.

Perhaps the most striking difference between SB-220 and the CCPA is the definition of what constitutes a sale. In contrast, under the CCPA, sale is broadly defined as any exchange of personal information for monetary value or other valuable consideration.

Obligations imposed (right to opt-out): The NPICICA has required operators since 2017 to inform consumers of their data management practices by posting a privacy notice. SB-220 adds the additional obligation for operators to provide an opportunity for consumers to opt-out of certain disclosures deemed under the law a "data sale"

Covered entities under SB-220 must now create a "designated request address" (email address, toll-free number, or website) through which a consumer may submit an opt-out request. The CCPA, by contrast, requires more specific opt-out methods, including providing a specific link on company internet homepages and in online privacy statements, entitled "Do Not Sell My Personal Information." Further, companies have to describe consumers' right to opt-out in the online privacy statements.

In sum, the Nevada requirement to allow consumers to "opt-out" of sales resembles the CCPA but is much narrower because: (i) only "covered data" is in scope (as opposed to the more comprehensive concept of "personal information" under CCPA and (ii) the definition of sale only includes transfers for monetary consideration where the recipient is authorized to license or sell the information to third parties. Unlike the CCPA, SB-220 does not require opt-in for data of minors and does not contain additional rights (e.g. access, erasure, etc.).

Verifying and honoring requests: Both laws require companies to verify opt-out requests (i.e., confirm the individual is who they say they are).

In Nevada, Covered Entities must respond to the consumer's request within sixty days of receipt but may extend the period by no more than thirty days if reasonably necessary with notice to the consumer. Although not explicitly stated, during that time period, the company should also locate the consumer's personal information and secure the data in such a way as to prevent it from being inadvertently sold. California does not provide an explicit timeline for responding to requests to opt-out, but the language likely requires honoring such requests immediately.

Enforcement: SB-220 permits the Attorney General to seek a temporary or permanent injunction (*e.*, shutdown the internet site) or seek a fine of up to $5,000 per violation. The law does not allow consumers a private right of action. However, even a temporary shutdown of an internet site could have devastating consequences for a company.

The CCPA, on the other hand, provides a private right of action, but only for security breaches. Consumers can seek $750 per consumer per incident or actual damages, whichever is greater. Similar to SB-220, California's Attorney General can seek an injunction and civil penalty of not more than $2,500 per violation or $7,500 for each *intentional*

What should you do to prepare?

Set a "top-down" data management strategy: As more and more laws include requirements regarding data handling practices that need to be disclosed to users, organizations must thoughtfully

design and carefully implement a data management strategy that aligns with their corporate values. Will you disclose to users that some of your activities involve a “sale” as defined under SB-220 or modify your practices to be able to take the position that you do not “sell” data? What kind of contractual obligations that may increase your exposure to liability will you accept if you are a service provider? What jurisdictions will you choose to operate in or avoid? Engaging the C-Suite in these discussions and obtaining their support for the implementation of the strategy will be the key to success.

Know your data: A thorough data inventory to understand how your organization is collecting data and from whom, where it is stored, and how it is used downstream is the first step for compliance. Leveraging any data mapping conducted for compliance with the EU’s General Data Protection Regulation (“GDPR”) can accelerate this process. Given the brief window before the law goes into effect, a viable alternative to a full inventory and data mapping could be a data flow chart overlaid on top a detail map of the technology ecosystem that, at a minimum, identifies the categories of information held and shared.

Design processes to respond to individual rights requests and, where possible, automate: The number and type of opt-out methods that a business puts in place will need to be tailored to the size of the company and the likely demand for the opt-out service. Ideally, organizations should plan on how to automate the processes but, at a minimum, should make sure to have a process that the key stakeholders (consumer services, privacy team, IT team etc.) understand and are able to follow. Companies will also need a thoughtful approach on how to authenticate requests that ensure individuals’ rights are respected while preventing fraudsters from exploiting the new rights to their advantage.

Review your privacy notices: Organizations need to make certain disclosures in their privacy notices and review them for compliance.

Do not forget vendor management!: From reviewing and updating contracts, to ensuring vendors are implementing adequate security measures and are able to assist you in complying with the user’s request, vendor management is key.

Train employees: Employees will need to be trained on the new procedures to receive and process consumer opt-out requests. It is also important for employees that interact directly with users to understand where to direct user privacy inquiries.

Conclusion

As the privacy compliance landscape gets more complex with the new trend towards privacy regulation at the state level, organization should keep an eye on states such Nevada enacting “CCPA lite” laws. Our team is prepared to assist those companies every step of the way.

How we can help?

- Determine applicability of the CCPA and SB-220 to your business.
- Conduct gap assessments of your current practices against the CCPA and SB-220.
- Prepare and execute work plans to achieve compliance in a cost-effective and efficient manner, leveraging existing compliance efforts where possible.
- Interpret nuances in the CCPA and SB-220 provisions, such as identifying business partners as service providers, third parties, or something else under the law.

[1] *See*, NRS Chapter 603A Sec. 330 (2) as amended by NV SB-220.

National Law Review, Volumess IX, Number 256