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

Why Businesses Shouldn't Sleep On Nev.'s Privacy Law

By **Allison Grande**

Law360 (October 18, 2019, 8:42 PM EDT) -- A new law that allows Nevada residents to opt out of the sale of their data isn't garnering as much attention as California's broader looming privacy rules, but attorneys say the risk of regulatory enforcement — including for future data sales — should encourage companies to keep the regulation on their radar.

Nevada's Senate Bill 220, which was signed in May and took effect Oct. 1, requires website operators that collect personal information from state residents to provide these consumers with a way to demand that the operator not sell any covered information that it has or will collect about them.

The law doesn't encompass the sweeping data access and transparency requirements contained in California's landmark Consumer Privacy Act, which is set to go live Jan. 1, and contains much narrower definitions of key statutory terms, including "sale" and "operator."

But that doesn't mean compliance with the law — which allows the attorney general to recover up to $5,000 per violation and covers unanticipated future data sales — should be put on the back burner, according to attorneys.

"No one wants to get on the bad side of an attorney general, and these types of privacy laws are becoming the norm more than the exception, so it's likely in everyone's best interest to tackle these issues head-on and embrace them and not push them off," said Meaghan Pedati, a member of the data privacy and security industry team at McGuireWoods LLP.

In drafting the law, Nevada lawmakers appeared to take inspiration from California, where the Legislature hastily enacted the nation's first comprehensive consumer privacy protections in June 2018 in order to avoid having a more stringent ballot initiative be presented to voters.

The California law gives consumers the right to ask companies what types of personal data they hold about them, to request that their data be deleted and to opt out of the sale of that information. The Nevada law, on the other hand, is limited to the sale component, and the restriction is not as sweeping.

Unlike California, where sale is broadly construed to cover the transfer or disclosure of personal information "for monetary or other valuable consideration," Nevada limits the term to the exchange of covered information for only monetary consideration. Because many online companies derive value from users' information through activities such as targeted advertising — which is not covered by the

Nevada law — and don't engage in traditional sales when it comes to this data, the statute is likely to have a somewhat limited reach, attorneys say.

"The Nevada law defines what is a 'sale' much more narrowly than other state laws we have seen or are seeing," said Gregory Parks, partner and co-leader of Morgan Lewis & Bockius LLP's privacy and cybersecurity practice. "This means the law really applies more to data brokers than it does to retailers or other consumer facing-companies with direct relationships with consumers."

Pedati agreed that the Nevada law's narrower scope makes it "a bit of an easier pill to swallow and seems less burdensome to some extent."

However, as the way that retailers, social media companies and other businesses with an online presence in Nevada use consumers' data continues to evolve, the reach of the law could expand with it.

A top concern with and criticism of the law is its coverage of personal information such as names, Social Security numbers and other identifiers that the company "has or will collect" about a consumer, according to BakerHostetler partner Alan Friel.

That provision leaves the door open for companies that are not currently engaging in traditional sales of consumer data to face liability down the road if the way they deal with this information changes, Friel noted.

"The literal reading of the statute would be, whether you're selling data or not, you have to give people the ability to opt out of even future, not-yet-contemplated, data sales," Friel said. "That's creating a lot of frustration, because companies are first looking at the law and saying, 'That's no problem, I'm not selling covered information,' but then they still have to offer an opt-out for something that they don't do and have no intention of doing in the future."

The California privacy law permits businesses to skip offering an opt-out program if they say in their privacy policy that they don't sell personal data. The state's attorney general elaborated on this provision in recently released regulations for implementing the law. The new regs state that businesses that don't sell personal information must still offer the opportunity to opt out of future sales unless a business states in its privacy policy that it doesn't and won't sell this information and if it treats any data it collects as subject to a validly submitted opt-out, Friel noted.

"That could be an interesting approach for Nevada, too," Friel said.

Efforts are underway to lobby either the Nevada Legislature — which only meets in odd-numbered years and doesn't reconvene until February 2021 — to amend the statute or for the state attorney general to issue an advisory opinion to clarify that the opt-out program applies only to companies actively engaged in the sale of data. That push is still in its early stages.

In the meantime, businesses that purposefully direct their services toward and collect covered data from Nevada residents can choose to decline to offer an opt-out on the basis that they don't currently sell consumer data, which could open them up to potential enforcement action. Or, they could take steps similar to what more clear-cut covered entities must do to comply, Friel noted.

These options include offering a full-fledged opt-out program as envisioned by the law — which requires companies to provide consumers with an email address, toll-free phone number or web address to

submit such requests and to verify and respond within 60 days to those demands. Or, it could be a middle ground approach of collecting the contact information of consumers who wish to opt out of future sales and agreeing to notify them if the company decides to sell their data down the road.

"That still means that the company would have to keep a list of consumers' contact information, but it shouldn't be a tremendously difficult burden," Friel said.

Having a plan in place is particularly important in light of the threat for attorney general enforcement, lawyers noted.

"Attorney general enforcement is the main practical risk, and we'll have to wait and see how aggressive the regulator is going to be and whether it has the resources to pursue these actions," O'Melveny & Myers LLP special counsel Scott Pink said. "But I'd imagine companies that are subject to the law would want to be viewed as doing their best to be on the right side of it."

While Nevada Attorney General Aaron Ford hasn't built a reputation as being an aggressive privacy enforcer like his colleagues in California, New Jersey, New York, Illinois and other states, the increased attention being paid to these issues generally coupled with his new enhanced enforcement powers could change that.

"State attorneys general overall are paying as much attention to these issues as the rest of us are," Pedati said.

Given that the new Nevada law doesn't include a provision that requires the attorney general to give companies notice of and a period of time to cure any potential violations, the regulator could technically "just do a website sweep and seek civil penalties on every website that doesn't have the designated opt-out address, even if they're not selling data," Friel noted, although he acknowledged that more nuanced enforcement was likely, especially at the beginning.

"The expectation is that the enforcement priority would be on those selling covered information and not offering an opt-out, and that if the attorney general decides that it's important to offer a prospective opt-out for activity that has yet to occur, that there would be some kind of education effort first without doing a sweep," Friel said.

While the Nevada law doesn't contain a private right of action, claims related to companies' obligation under the statute could still potentially end up in federal court, since the law doesn't bar an alleged violation from being the basis for a claim under any other law.

This could open the door for consumers to claim that a company's failure to adhere to the statute's do-not-sell requirements runs afoul of the state's law prohibiting unfair or deceptive practices, according to Friel. He notes, though, that those claims could be difficult to sustain against companies that aren't actively selling data due to difficulties with establishing any actual harm.

The broader significance of Nevada's law in the growing national data privacy legislative landscape also warrants companies' attention, attorneys noted.

While Nevada's statute was put on the books after California's law, it beat the Golden State to implementation, making it a trailblazer and an important yardstick for how similar laws being considered in New Jersey, New York, Texas and Washington state might play out.

"For companies that thought for a minute that they were going to try to exclude California users or didn't have to follow the opt-out requirements of the California law because they don't have anybody in the state, they might have someone in Nevada and will need to follow those procedures," Baker Botts LLP special counsel Cynthia Cole said. "And it's not going to stop with Nevada, so that's why companies need to be paying attention."

Pedati compared the current state of consumer privacy legislation with the early days of data breach notification legislation. California became the first state in 2003 to enact a law requiring companies to report such incidents, and since then every U.S. state has put a similar law on the books. With a similar trajectory predicted for data privacy, Nevada becomes an important jumping off point to build a more comprehensive compliance program, according to Pedati.

"It's really becoming more of a conversation, less about these individual state laws and really about creating a new compliance structure within an organization that allows for flexibility to incorporate privacy-related laws still to come," Pedati said. "Companies are never off the hook and certainly can't sleep when it comes to privacy issues."

--Editing by Breda Lund and Michael Watanabe.