wiley

NEWSLETTER

States Continue to Move Forward on Their Own Privacy and Security Laws: Nevada, Maine, and Oregon Are The Latest

July 2019

Privacy in Focus®

As federal lawmakers consider national privacy legislation, states have moved to implement their own consumer privacy and data security laws. California has led the charge with the passage of the California Consumer Privacy Act of 2018 (CCPA), a broad privacy law that regulates how certain businesses use personal information. On the heels of the CCPA, in September 2018, California also passed legislation addressing security of Internet of Things (IoT) devices, SB 327.

Taking a cue from California's playbook, many other states have introduced various privacy and cybersecurity proposals, and Maine, Nevada, and Oregon have recently enacted such proposals. As further detailed below, the Nevada law covers commercial websites and online services, whereas the Maine law targets one portion of the Internet ecosystem—Internet service providers (ISPs). The new Oregon law – like California's IoT security law – addresses IoT manufacturers.

Nevada Allows Consumers to Opt Out of the Sale of Their Personal Information

On May 29, 2019, Nevada's Governor signed into law SB 220, which updates Nevada's existing law that requires companies to provide a notice regarding the privacy of certain information collected online. SB 220 adds to Nevada law a consumer right to opt out of the sale of covered information by certain online entities. SB 220 is slated to go

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

into effect on October 1, 2019, before CCPA's effective date of January 1, 2020. Accordingly, companies working on CCPA-related compliance measures may need to adjust implementation schedules and practices to account for the new Nevada law.

While the sale opt-out right in the new Nevada law is similar to that of the CCPA, the Nevada law is narrower in scope than the CCPA. In particular:

- The term "consumer" under Nevada law is narrower than the same term in the CCPA, so a more limited set of individuals have opt-out rights. Existing Nevada law defines "consumer" as a "person who seeks or acquires, by purchase or lease, any good, service, money or credit for personal, family or household purposes from the Internet website or online service of an operator,"[1] whereas the CCPA currently defines "consumer" much more broadly, encompassing any California resident.
- Under SB 220, "covered information" is more limited in scope than the CCPA's "personal information." The CCPA applies broadly to *any* information that "relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,"[2] which includes but is not limited to elements as broad as "[a]udio, electronic, visual, thermal, olfactory, or similar information"[3] and "inferences drawn from any ... [personal] information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[4] Nevada's "covered information," on the other hand, is limited to several clearly defined data elements, including name, address, email, phone number, Social Security number, other identifiers that enable a person to be contacted, and information collected online and maintained in combination with an identifier in a form that makes it personally identifiable. Importantly, Nevada also limits "covered information" to data that is "maintained by the operator in an accessible form."[5]
- Nevada similarly takes a narrower view of what constitutes a "sale." SB 220 limits the term "sale" to mean "the exchange of covered information for monetary consideration."[6] Conversely, CCPA's definition of "sale" is broader and encompasses "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."[7]
- The Nevada law is also more limited than the CCPA in that it only imposes opt-out obligations on certain online "operators." SB 220 amends the definition of an operator under existing state privacy law, limiting an "operator" to a person who "owns or operates an Internet website or online service for commercial purposes"[8] and "collects and maintains covered information."[9] Conversely, CCPA, with limited exceptions, extends broadly to any covered business – online operator or otherwise – who "collects" personal information.

As for process, SB 220 requires operators to provide a "designated request address" through which consumers may submit opt-out requests. The "designated request address" may include an e-mail address, toll-free telephone number, or website. Operators must respond to verified requests within 60 days, with the

ability to extend the deadline an additional 30 days where "reasonably necessary"[10] with notice to the consumer.

Even though the Nevada law is narrower in scope than California's approach, companies working on CCPA-related compliance measures can leverage that work to comply with SB 220.

Maine's New Law Regulates Broadband Internet Access Service Providers

Approved by Governor Janet Mills on June 6, 2019, Maine's S.P. 275/L.D. 946 is the latest state law aimed at regulating online privacy, and will go into effect on July 1, 2020. Touted as one of the nation's toughest privacy measures, the legislation is modeled on a now-repealed Federal Communications Commission rule – adopted under President Obama's Administration – banning ISPs from using, sharing, or selling a customer's personal data without the customer's consent.

The law requires ISPs – but not other participants in the Internet ecosystem – to obtain express, affirmative opt-in consent before using, disclosing, selling, or permitting access to any customer personal information. The term "customer personal information" is broadly defined, and the opt-in requirement has limited exceptions. The consumer also has the right to revoke his or her consent "at any time."[11] And beyond the substantial consent requirements, the Maine law also establishes nondiscrimination requirements (including prohibiting ISPs from offering discounted rates to customers who agree to give opt-in consent), as well as security requirements to protect customer personal information, among other things.

With its focus on ISPs, Maine's restrictive law is a standout in the state regulatory landscape.

Oregon Requires IoT Manufacturers to Build Protections into Their Devices

Finally, Oregon has joined California as the second state to enact an IoT law requiring manufacturers of Internet-connected devices to equip those devices with "reasonable" security measures. Both the Oregon and the California IoT laws go into force on January 1, 2020.

On its face, Oregon HB 2395 largely tracks the California IoT law. Both bills mandate that manufacturers implement "reasonable" security features, which are features that are "appropriate" to guard against intrusions taking into consideration the nature, function, and data collection capabilities of the Internet-connected device. Moreover, both bills identify two security specifications – both related to authentication – that, if satisfied, would be deemed a "reasonable security feature."[12]

One notable distinction between the two laws is the statutory definitions of a "connected device." The California IoT law defines "connected device" as "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address."[13] Oregon's HB 2395 cabins that definition to devices that are "used primarily for personal, family or household purposes."[14]

Moreover, the California law defines "manufacturer" to mean "the person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California."[15] A "contract with another person to manufacture"[16] excludes "a contract only to purchase a connected device, or only to purchase and brand a connected device."[17] The Oregon law limits manufacturers to "a person that makes a connected device and sells or offers to sell the connected device."[18]

Accordingly, while the Oregon law applies to *fewer* devices and to a *narrower* set of manufacturers, a company doing business in both states will need to comply with the broader California law.

Conclusion

These three recent laws are just the latest examples of the emergence of a fragmented state-by-state approach to data privacy and security, which will continue to impose compliance obligations on U.S. businesses, including obligations that may significantly differ by state. Companies whose products or services deal with consumer data should closely monitor state-level developments, and make decisions about how they manage, share, and protect that data in light of shifting state-level regulatory requirements.

---

[1] 52 Nev. Rev. Stat. ch. 603A.320 (2017).

[2] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.140(1) (2018).

[3] *Id.* § 1798.140(H).

[4] *Id.* § 1798.140(K).

[5] 52 Nev. Rev. Stat. ch. 603A.320 (2017).

[6] S.B. 220, 80th Sess. § 1.6 (Nev. 2019).

[7] California Consumer Privacy Act of 2018 ("CCPA"), CAL. CIV. CODE § 1798.140(t) (2018).

[8] 52 Nev. Rev. Stat. ch. 603A.330 (2017).

[9] *Id.*

[10] S.B. 220, 80th Sess. § 1.8(2) (Nev. 2019).

[11] S.P. 275, ch. 94, § 9301(3)(A) (Me. 2019).

[12] H.B. 2395, Leg. Assemb., 80th Sess. § 1(c) (Or. 2019).

[13] S.B. 327 ("California IoT law"), ch. 886, § 1798.91.05(b) (Cal. 2018).

[14] H.B. 2395, Leg. Assemb., 80th Sess. § 1(A) (Or. 2019).

[15] S.B. 327 ("California IoT law"), ch. 886, § 1798.91.05(c) (Cal. 2018).

[16] *Id.*

[17] *Id* § 1798.91.04(c).

[18] H.B. 2395, Leg. Assemb., 80th Sess. § 1(b) (Or. 2019).