Proskauer

Oregon Strengthens Geolocation Data Privacy and Children's Personal Data Protections, Adding to Compliance for Data Brokers and Others

New Media and Technology Law Blog on **July 23, 2025**

On June 3, 2025, Oregon Governor Tina Kotek signed HB 2008 into law to amend the Oregon Consumer Privacy Act,[1] the state's comprehensive data privacy law. Among other items, effective January 1, 2026, the "sale" of two categories of personal data will be prohibited

- Precise geolocation information that can pinpoint an individual or device with a 1,750-foot radius, absent some specific communications or utility-related exceptions
- Personal data of anyone under sixteen years of age, provided that the data controller "has actual knowledge that, or willfully disregards whether, the consumer is under 16 years of age"[2]

The location data provision echoes a similar prohibition that was passed in Maryland last year.[3]

Location data is considered "sensitive" because it can be readily collected from mobile devices or web browsing activities and can reveal a great deal about an individual's habits, interests and movements. Beyond targeted advertising, anonymized location data can be a valuable source of alternative data for businesses gathering insights on competitors or consumer foot traffic or migration patterns and population growth.

As a result, the Oregon law – and the possibility of other similar state enactments that could restrict the sale of precise location data – represents an important development affecting data brokers and entities that use such data for location-based advertising and profiling and to create other data products and insights from location data. HB 2008's definition of "sale" may potentially affect not just direct sales of precise location data but bundling and other licensing arrangements, subject to certain exceptions and uses. The new law will also add to customers' due diligence process examining their data vendors' collection practices.

Location Data Generally

Generally speaking, location data is collected from users via mobile apps, often with the user's consent, in exchange for more personalized or optimized services. While this data is often anonymized, a device's movement patterns can sometimes be predictable enough to derive the possible identity of its owner, making the data susceptible to "de-anonymization." For example, a phone will usually spend its overnight hours at the owner's home address, and regular commuting patterns can be deciphered and cross-referenced with other databases.

In light of the foregoing, public and private access to location data has earned the attention of both federal and state regulators and legislatures – particularly with the expanding use of such data by government bodies, such as law enforcement, the military, and intelligence agencies, which might seek to access or license commercially available datasets or services. Though, it should be noted that public agencies might also use location data for environmental protection purposes, traffic analysis and city planning, uses that may not implicate consumer privacy in the same ways as others.

Oregon HB 2008 and Compliance

Under HB 2008, companies may no longer sell a consumer's precise location data if the data in question: "accurately identifies within a radius of 1,750 feet a consumer's present or past location, or the present or past location of a device that links or is linkable to a consumer by means of technology." The statute includes an exception for the "content of communications" or data related to advanced "utility metering infrastructure systems or equipment for use by a utility." The definition of "sale" in HB 2008 cites to the meaning under the Oregon privacy law and is not limited to monetary transactions. Under ORS 646A.570(17), "sale" means "the exchange of personal data for monetary or other valuable consideration by the controller with a third party."

Most other state data privacy laws that regulate the sharing of sensitive data require data controllers to post certain disclosures and obtain consumer consent before the data collector may sell or share such data, and to provide consumers with certain opt-out rights. Oregon's law, however, is now more stringent with respect to location data. HB 2008, on its face, imposes a blanket ban on the sale of precise location data that can accurately identify a consumer or device. This broad provision is expected to have ripple effects across the online advertising and data industry, from web publishers and app developers to ad tech and data providers.

Still, it should be noted the Oregon privacy law's definition of "sale" includes its own exceptions,[4] such as for disclosures of personal data to a processor or a controller's affiliate to provide the requested product or service. The definition of "sale" also exempts a "disclosure of personal data that occurs because a consumer…directs a controller to disclose the personal data" or when a consumer otherwise intentionally discloses such data on "mass media" or when directing a data controller to interact with a third party. These statutory exceptions introduce some nuance to data collection and compliance practices, often requiring the involvement of legal counsel. Thus, despite being a "ban," the definition of "sale" under the statute leaves certain uses outside the prohibition and will likely prompt providers to revise data collection and consent practices and monitor future guidance by courts or the state attorney general.

In addition, although the law prohibits the sale of location data, it applies only to precise location data. Sales of general location data – such as that derived from an IP address, which might narrow a user's whereabouts to a broad neighborhood (beyond the 1,750-foot zone) or city – remain permissible.

In practice, there are several steps that data brokers and others might take to comply with the Oregon law. Such measures might include segregating and tagging Oregon (and Maryland) location data collected, storing such data in separate databases or partitions and applying restricted processing rules. A data broker, for example, might remove or obfuscate precise geolocation data for Oregon residents to show aggregated neighborhood-level data for sale, but not the exact locations visited by consumers. Overall, compliance might include a multi-step filtering and data governance and audit process to comply with HB 2008 and similar laws.

By following Maryland's lead, Oregon has highlighted a potential shift at the state level towards expanding data privacy protection for highly sensitive digital information like location data. Legislators in California, Maine, Massachusetts, and Vermont are considering similar geolocation privacy measures. As data privacy laws continue to evolve at the state level, business need to stay informed of new requirements, adjust their policies, and regularly reassess their compliance posture.

View original.

---

[1] The Oregon Consumer Privacy Act is codified at ORS 646A.570-646A.589. Specially, HB 2008 amends ORS 646A.578.

[2] As to the additional restrictions on the sale of data of minors, Oregon's amendments go beyond the federal Children's Online Privacy Protection Act (COPPA) which apply only to children under thirteen (though, a bipartisan bill that would strengthen COPPA's protections, named "COPPA 2.0," has been reintroduced in the U.S. Senate).

[3] It should be noted that last year, Maryland enacted the "Maryland Online Data Privacy Act," which regulates the ways in which a data controller or processor may process the consumer's personal data and which contains a provision that bans the sale of "sensitive data," including precise location data. The Maryland law becomes effective later this year in October 2025. Other states are also considering similar restrictions on location data sharing. Meanwhile, the FTC has in recent years continued its enforcement focus on the sharing of location data without informed consumer consent.

[4] "Sale" or "sell" means the exchange of personal data for monetary or other valuable consideration by the controller with a third party.

(b) “Sale” or “sell” does not include:

(A) A disclosure of personal data to a processor;

(B) A disclosure of personal data to an affiliate of a controller or to a third party for the purpose of enabling the controller to provide a product or service to a consumer that requested the product or service;

(C) A disclosure or transfer of personal data from a controller to a third party as part of a proposed or completed merger, acquisition, bankruptcy or other transaction in which the third party assumes control of all or part of the controller’s assets, including the personal data; or

(D) A disclosure of personal data that occurs because a consumer:

(i) Directs a controller to disclose the personal data;

(ii) Intentionally discloses the personal data in the course of directing a controller to interact with a third party; or

(iii) Intentionally discloses the personal data to the public by means of mass media, if the disclosure is not restricted to a specific audience.