Enforcement Report: The Oregon Consumer Privacy Act, The First Year

ORS 646A.570-646A.589

August 2025

Executive Summary

The Oregon Consumer Privacy Act ("OCPA"), ORS 646A.570-646A.589 is Oregon's comprehensive consumer privacy law, which took effect on July 1, 2024, for business entities and July 1, 2025, for nonprofit entities. In the twelve months since the OCPA took effect, the Oregon Department of Justice ("DOJ") has taken significant steps to educate consumers and businesses and encourage compliance with the law.

The DOJ issued two reports in the first six months of enforcement: a Six-Month Report covering July 1, 2024-January 1, 2025, and a Quarter 1 2025 Report, covering January 1, 2025-March 31, 2025. This enforcement report describes the first year of enforcement and is part of ongoing efforts to be transparent to the public as well as convey the DOJ's compliance expectations to industry.

This updated report provides: (1) a brief recap and overview of the OCPA; (2) a summary of the consumer complaints received under the OCPA; (3) a discussion of the Privacy Unit's enforcement updates; and (4) a summary of recent legislative amendments to the OCPA.

The Oregon Consumer Privacy Act

On June 23, 2023, the Oregon Legislature passed Senate Bill 619, a comprehensive consumer privacy law (the "Oregon Consumer Privacy Act" or "the law"). The Oregon Consumer Privacy Act ("OCPA"), ORS 646A.570-646A.589, passed the Oregon State Legislature with strong bipartisan support and was signed into law by Governor Kotek. The OCPA was based on and shares many commonalities with the consumer privacy laws passed by Colorado and Connecticut (as they were originally drafted).

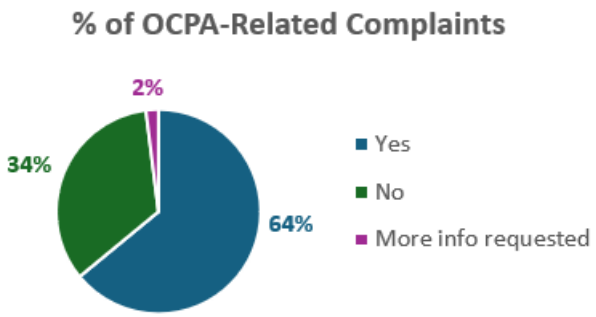
The OCPA took effect on July 1, 2024, for for-profit entities and July 1, 2025, for nonprofit entities. The OCPA is currently in its cure period, which lasts until January 1, 2026, for both businesses and nonprofits. Under the cure period, if the DOJ believes violations of the OCPA are fixable, then the Privacy Unit within the DOJ must give the entity notice and 30 days to remedy or cure the violation(s). If the Attorney General's office determines that there is no cure or remedy for the violation, no such notice is required before the Attorney General brings an enforcement action.

Previous reports have overviewed the OCPA in more depth, and our Consumer Privacy website contains many resources for consumers, businesses, and nonprofits: Consumer Privacy - Oregon Department of Justice : Consumer Protection. This includes tailored FAQs for Nonprofits. This report will now shift to cover the consumer complaints from the last year.

Consumer Privacy Complaints

Oregonians continue to care about their privacy rights. Thanks in part to a concentrated public outreach and education campaign, the Privacy Unit continues to receive a high volume of consumer complaints. The Privacy Complaint Portal is a webform located on the Consumer Privacy Webpage. This portal is designed to allow consumers to make complaints about businesses not honoring a consumer's privacy requests, businesses that lack a privacy notice, or technical issues with submitting a privacy request. The Privacy Unit screens the consumer complaints to ensure that they involve the OCPA and then evaluates whether the named entities may be in violation of the OCPA.

In the first year of enforcement, the DOJ received 214 consumer privacy complaints through the Privacy Complaint Portal. The majority of those – 130 complaints - passed the initial screening process during which DOJ assesses whether the complaint is OCPA-related. Of the 130 OCPA-relevant complaints, DOJ did not take further action on 39, which related to entities or information exempted from the OCPA (ex: government entity, data covered by existing federal law such as HIPAA).

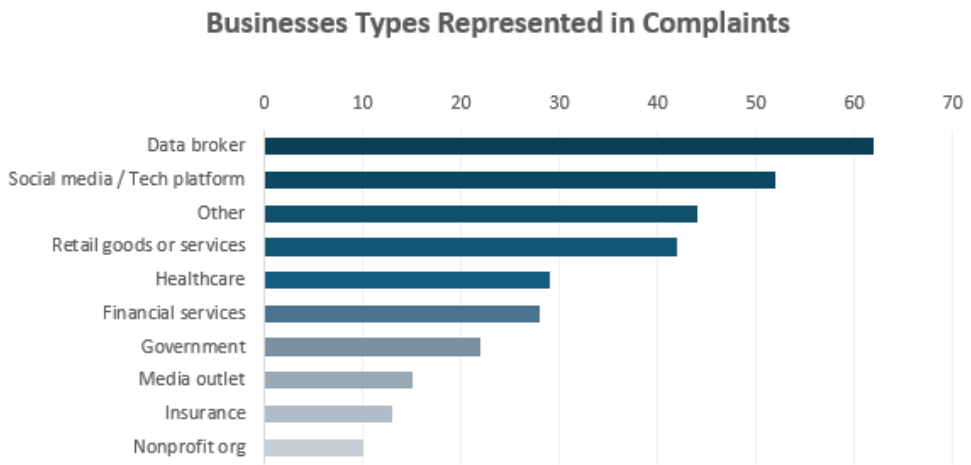


From the remaining 91 OCPA relevant complaints, the Privacy Unit initiated and closed 38

OCPA cure letter matters as of July 1st. As a reminder, the cure notice is a letter mandated by the OCPA until January 1, 2026, if the potential violation(s) are curable, or fixable. Cure letters give entities a chance to correct any compliance issues with the OCPA before additional enforcement steps are taken.

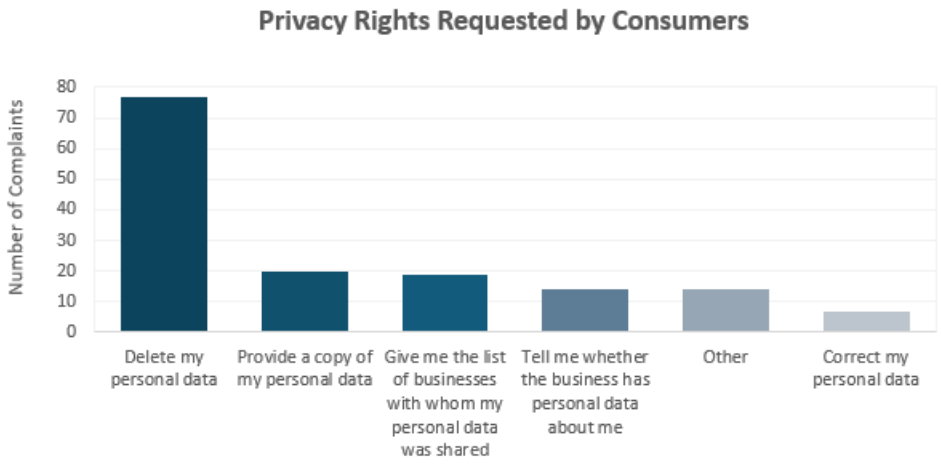
Some additional matters based on complaints remain ongoing and open, therefore confidential. Other complaints were duplicates regarding the same business. Aside from these multiples, there are varying reasons for the rest of the OCPA-related consumer complaints did not result in a cure letter. Sometimes a more informal inquiry letter revealed that the company was already complying. Sometimes an entity did not reach the threshold required for the OCPA to apply.

Data brokers continue to be of chief concern of consumers; 62 of the total consumer complaints involved data brokers.[1] Social media platforms were the second most complained about type of entity/industry.



The right to delete remains the most complained about privacy rights request, with 77 complaints. Oregonians also submitted a substantial number of complaints about the right to request a copy of their data with 20 complaints, and a right to get a list of specific third parties their data was disclosed to, with 19 complaints.

[1] In the privacy complaints form, consumers are asked to identify which type of entity they are submitting a complaint about. Therefore the "business types" are from self-reported consumer statistics.



Enforcement Updates

Many of the DOJ's enforcement efforts referred to in the Six-Month Enforcement Report remain ongoing. The Privacy Unit would like to highlight some updates as well as takeaways we have gleaned from our work in the last year. This includes: (1) compliance issues with a right to know a list of specific third parties; (2) problems with people search sites, which are a subset of data brokers; (3) entities requiring consumers to perform significant effort regarding their privacy rights, which may provide incomplete options for copy, deletion, etc.; (4) a reminder for industry to continue to audit functionality for privacy requests, and (5) some clarifications about the role and extent of legal provisions for authorized agents.

Specific Third Parties

The OCPA was the first comprehensive privacy law to provide its citizens with access to a "list of specific third parties, other than natural persons, to which the controller has disclosed […] The consumer's personal data."[2] In plain language, this provision allows consumers to request a list of entities that their personal data was disclosed to, which includes sales of consumer data. This provision is important, because it helps individuals track to whom their data has been disclosed to, providing them with better understanding of how to follow up potentially with deletion or other privacy rights.

Many of the companies about whom the Privacy Unit have received complaints fail to comply with this requirement in one way or another, even more than a year after the OCPA went into effect. Not only are consumers concerned by companies that fail to list this as a right available for consumers to exercise, 19 of the consumer complaints received by the Privacy Unit describe that companies who claim to provide this right do not handle such requests correctly.

[2] ORS 646A.574 (1)(a)(B).

The right to a list of specific third parties is an enforcement concern for the DOJ, as it represents an important tool for consumers to monitor and understand how their data has been disclosed downstream and makes data practices more transparent. As other states consider adding this right to their comprehensive privacy laws,[3] the Privacy Unit expects companies to focus on better compliance with this provision.

People Search Sites

People search sites are a subset of data broker websites. While these sites do not generally collect large amounts of consumer data themselves, they do purport to provide unofficial background profiles on significant numbers of consumers. These background profiles can vary in depth, but they are generally comprised of a mix of public records and purchased data.

Sites that provide lists of public records associated with names generally do not pose OCPA concerns because that information is not personal data. However, some of these people search sites combine public records with purchased data to compile detailed profiles of individuals. These profiles are extensive and often inaccurate.

Self-Help Requests

The Privacy Unit has also encountered some common issues with entities that require consumers to do "self-help" to effectuate their privacy rights requests.

First, the approach is often not comprehensive. When consumers are directed to their own accounts to copy their data, delete their data, etc., it often only relates to data that is consumer-facing. Back-end personal data kept on consumers, such as marketing profiles or shopping patterns, are not included in this data and, therefore, this approach does not comply with the OCPA. When a consumer requests a copy of their data, deletion of their data, or other privacy rights granted by the OCPA, it is the controller's obligation to provide all personal or sensitive data, including derived data that is not exempted by law.

Second, this "self-help" approach does not always provide a mechanism for non-account holders to access their OCPA rights. Similarly, authorized agents are also often not given a "self-help" mechanism to opt-out on a consumer's behalf, as required by the OCPA.

Companies should make sure to review their existing privacy rights mechanisms to make sure that any self-help approaches to privacy requests comply with the OCPA.

Technical Issues

In reviewing numerous privacy complaints and assessing the relevant Privacy Notices, the Privacy Unit also noted a trend of technical problems resulting in compliance issues. Specifically, many entities have issues ensuring that any electronic form is functioning as intended. Additionally,

[3] Since the passage of the OCPA, Minnesota, Connecticut, and Delaware have included a similar provision in their comprehensive consumer privacy laws.

companies should ensure that if there is an email address, that it is checked on a regular basis for privacy related concerns or requests from consumers.

The Privacy Unit looks at a number of characteristics of an electronic form to determine whether it is sufficiently accessible to consumers to meet the requirements of the OCPA: does it allow consumers to list their state, if rights are limited to states with comprehensive privacy laws? Does the list of states include Oregon? Are all of the rights provided by the webform? Oftentimes, a right to a list of specific third parties is not addressed.

Finally, companies should have some non-automated option for consumers to reach out to with any technical issues. For example, one consumer mistyped their birthdate when opening an account, marking them as a very young minor. The company's automated help/privacy options made it so that the consumer was unable to correct their birthdate, even though a right to correction is granted by the OCPA. The DOJ expects entities to have some human intervention versus completely automated handling of privacy issues.

Authorized Agents

Authorized agents can be individuals, but are more commonly businesses, to whom a consumer gives the legal authority to act on the consumer's behalf. In the context of the OCPA, consumers have the right to use authorized agents to exercise their right to opt out of targeted advertising and profiling. Ideally, an authorized agent takes some of the workload from a consumer.[4]

Many authorized agents who operate as businesses charge a subscription fee for this service. A problem arises when authorized agents say that they can guarantee additional privacy rights to paid users, mainly a right to delete.

While a controller can *choose* to honor a deletion request or other privacy request from an authorized agent on behalf of a consumer, the controller is not obligated to. The only type of request submitted by authorized agents that controllers are required to grant under the OCPA is an opt-out request. Authorized agents should be careful in how they represent their services to consumers, and particularly should avoid using misleading language to engage consumers in subscription models.

[4] ORS 646A.576(4) ("A consumer may designate another person to act on the consumer's behalf as the consumer's authorized agent for the purpose of opting out of a controller's processing of the consumer's personal data, as provided in ORS 646A.574 (1)(d). The consumer may designate an authorized agent by means of an internet link, browser setting, browser extension, global device setting or other technology that enables the consumer to opt out of the controller's processing of the consumer's personal data. A controller shall comply with an opt-out request the controller receives from an authorized agent if the controller can verify, with commercially reasonable effort, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.").

Legislative Amendments to the OCPA

The Oregon Legislature recently wrapped up its 2025 Legislative Session. The Legislature enacted several key pieces of legislation which amended the OCPA. As one of the first states to enact a comprehensive consumer privacy law, Oregon is at the forefront of privacy protection and enforcement. These amendments ensure that the OCPA remains updated to meet new and emerging threats to Oregonians' privacy.

Expanded Protections for Children and Teens

In the statewide survey the DOJ conducted last year, children's privacy was identified by respondents as a top priority and concern.[5] This mirrors national concern for the safety and the long-term impacts of social media and lack of privacy for children online. Following in the footsteps of other states, in the 2025 Legislative Session, the Legislature decided to add additional protections for children and teens by amending the OCPA.

The amendment, HB 2008, does several things to reinforce protections for children and teens. First, processing the data of children under 13 still requires compliance with the recently updated and strengthened federal protection of the Children's Online Privacy Protection Act, broadly known as COPPA.

Second, controllers, or entities that control consumers' personal data, are banned from selling or sharing for value, the personal or sensitive data of a child under 16. This applies to children or teens that a controller knows, or *should* have known, are under 16.

Third and relatedly, neither the child themselves nor their parent/guardian can consent for that data to be sold/shared. This should not impact a child or teens' ability to use any connected services, but it limits what entities can do with the personal and sensitive data they have collected about a child or teen.

These provisions on the ban on the sale or exchange of personal or sensitive data for children under 16, and consent, go into effect on January 1, 2026.

Geolocation Data

With HB 2008, the Oregon Legislature also banned the sale of all Oregonians' precise geolocation data. Precise geolocation data is defined as data that identifies a consumer or their device's past or present location with a 1,750-foot radius. This restriction applies to geolocation data exchanged for monetary or valuable consideration. This might potentially impact the sale of location-based advertising.

The ban on the sale or exchange of geolocation data goes into effect on January 1, 2026.

[5] DOJ Survey Finds Most Oregonians Care About Privacy, Curious About New Law.

Auto Manufacturer Thresholds

While the general threshold numbers for entities that must comply with the OCPA remains unchanged, one industry must comply with the OCPA regardless of how many Oregonians' data they possess: car manufacturers. HB 3875 extends OCPA requirements to all automakers, explicitly addressing concerns around reports that cars are the worst for privacy.

This reduction of OCPA threshold requirement goes into effect September 26, 2025.

Conclusion

The DOJ is dedicated to staying at the forefront of privacy rights for Oregonians. Since the passage of the OCPA, the Privacy Unit has worked hard to provide consumer education and outreach to industry and nonprofits alike. Aside from robustly enforcing existing provisions of the law, the Privacy Unit will be rolling out additional materials to educate consumers and businesses of the new amendments that passed in 2025.

The Privacy Unit remains dedicated to education, enforcement, and transparency in topics relating to privacy.