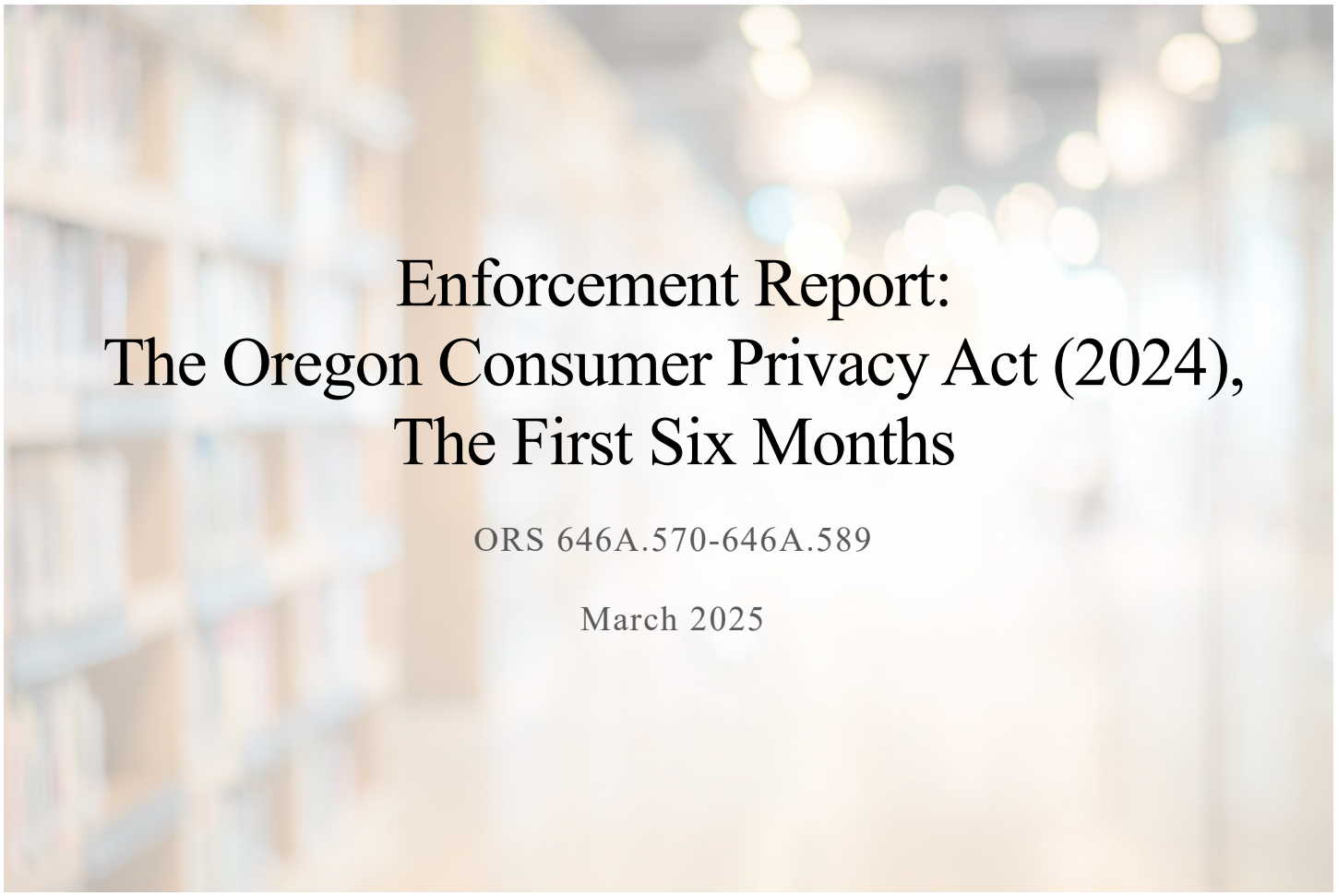


Enforcement Report: The Oregon Consumer Privacy Act (2024), The First Six Months

ORS 646A.570-646A.589

March 2025

Executive Summary

The "Oregon Consumer Privacy Act," or the OCPA, ORS 646A.570-646A.589 is Oregon's comprehensive consumer privacy law, which took effect on July 1, 2024. In the six (6) months since the OCPA took effect, the Oregon Department of Justice ("DOJ") has taken significant steps to educate consumers and businesses about and prompt compliance with the new law. The DOJ has issued over a dozen notices of violation ("cure notices") and inquiry letters. Many companies have taken prompt steps to address issues flagged in cure notices and/or have cooperated with information requests. These efforts are ongoing, as the cure period will not sunset (or expire) until January 1, 2026.

This Report provides: an overview of the OCPA; background on the DOJ Privacy Unit, and efforts to prepare for implementation of the OCPA, including a strong focus on outreach; a summary of the consumer complaints received under the OCPA; a discussion of DOJ's early enforcement efforts; and a conclusion.

The Oregon Consumer Privacy Act

Background

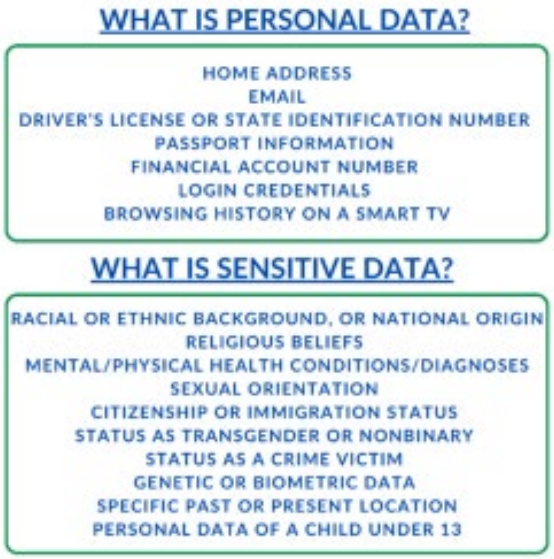
On June 23, 2023, the Oregon Legislature passed Senate Bill 619, a consumer privacy law (the "Oregon Consumer Privacy Act" or "the law"). Senate Bill 619 was developed by former Attorney General Ellen Rosenblum's Consumer Privacy Task Force by working with 150 consumer privacy experts and stakeholders representing consumers and industry. 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. January 1, 2025, marks six months since enactment. The OCPA is currently in its cure period, which lasts until January 1, 2026. Under the cure period, if the DOJ believes violations of the OCPA are fixable, then 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.

Key Provisions

The OCPA applies to any individual or entity that conducts business in Oregon or that provides products or services to Oregon residents if, during a calendar year, that individual or entity controls or processes the personal data of 1) at least 100,000 consumers; or 2) 25,000 or more consumers and derives over 25% of annual gross revenue from the sale of personal data. The individuals or entities that fit that description are called "controllers." The OCPA will go into effect for qualifying non-profits starting on July 1, 2025.

A "sale" is the exchange of personal data for monetary or other valuable consideration between a controller and a third party. Personal data is any information that can be linked to an individual. Personal data also includes any information that can be linked to an individual's device or a household device (like a cell phone or a smart appliance). Sensitive data is a subset of personal data and reveals private information that is generally not public. Certain categories of businesses (ex: banks) and certain types of data (ex: protected health information) are exempt from the OCPA.



Under the OCPA, Oregon consumers have specific privacy rights which allow them to manage the collection, retention, and use/sale of their personal and sensitive information. Consumers are urged to keep it **L.O.C.K.E.D.** They can get a **List** of the specific entities that received their personal data or any data from a controller. They can **Opt-out** (say "no") to a controller selling, profiling, and using their personal data for targeted advertising. They can get a **Copy** of the personal and sensitive data a controller has about them. They can **Know** what data a controller has collected about them. They can **Edit** any inaccuracies in the data about them. Finally, they can **Delete** personal and sensitive data controllers have about them.

Controllers of personal and sensitive data also have new legal obligations if they are covered by the OCPA. Among other things, controllers must:

1. Provide a clear and accessible privacy notice describing the types of personal data the controller processes, the specific purpose(s) for processing data, whether and why the controller shares personal data with third parties, and information about how consumers can exercise their various rights (e.g. access, deletion) over their personal data.

2. Provide a way for consumers to directly contact the controller about privacy-related issues and rights.

3. Limit their collection of personal data to what is adequate, relevant, and reasonably necessary for the specific purpose(s) for which the data is collected and processed (also known as "data minimization").

4. Obtain consent to process sensitive data, or, in some cases to sell or process data for targeted advertising/profiling. If a consumer is a child under 13, all of their data is sensitive, and parent/guardian permission is needed. For teens 13-16, consent must be given before any of their personal data is sold or used for targeted advertising or profiling.

5. Respond to requests to exercise consumer privacy rights within 45-days.

6. Conduct assessments before processing personal data in a manner that presents a heightened risk of harm to consumers (called "Data Protection Assessments"). This includes processing personal data for the purposes of targeted advertising, sale, or profiling, and any processing of sensitive data.

7. Use reasonable safeguards to secure personal data.[1]

The OCPA was the sixth state comprehensive consumer privacy law to go into effect and Oregon is considered a leader amongst state privacy enforcers. The OCPA is innovative in several ways. First, Oregon is the first state to provide consumers with a right to obtain a list of the specific third parties that their data was disclosed to. Other state laws granted a right to know only the categories of third parties, meaning that consumers could not follow their data downstream. Second, the OCPA expands definitions of sensitive data, encompassing things like gender identity and crime victim status. Third, the OCPA expands protections for the personal and sensitive data for children under 13, as well as teens 13-15. Fourth, the OCPA limits exemptions to ensure that the law's protections would be available more broadly to Oregon consumers.

[1] Oregon's data breach law, ORS 646A.600-646A.628, already mandated that such safeguards be applied to certain categories of information, defined as "personal information." The definition of "personal data" in the OCPA is more expansive.

The Privacy Unit (Antitrust, False Claims, and Privacy Section)

As the OCPA does not include a private right of action, enforcement falls solely to the Attorney General's office. The Privacy Unit is situated within the Civil Enforcement Division, and is housed within the recently formed Antitrust, False Claims, and Privacy Section ("AFCP Section"). The lawyers and professionals in the AFCP section enforce state and federal antitrust laws, prosecute false claims, and enforce federal and state privacy laws, including through the Oregon Unlawful Trade Practices Act ("UTPA").

Given the lack of private rights of action, as well as the increase in enforcement workload, the Oregon Legislature authorized three attorney and two specialized staff positions to enforce the OCPA. The Privacy Unit has expanded significantly in the last six months. The Unit is currently comprised of two Assistant Attorney Generals, one policy analyst, and a technology-oriented research analyst who work full-time on privacy and data security matters.[2] The Privacy Unit is also actively recruiting for a third attorney. These dedicated team members are assisted in this work by the other attorneys and staff within the AFCP Section.

Implementation & Outreach Efforts

After the OCPA passed, the DOJ started working to educate the public and provide resources for Oregon businesses to understand and comply with their new legal obligations.[3] This included building a dedicated Consumer Privacy Webpage[4] on the DOJ website, with materials targeted towards both consumers and businesses. As part of the website implementation, DOJ created a privacy email address for use by the public and businesses for OCPA related questions: "**Contact** – If you have other questions that are not covered by the information above, please reach out to oregonprivacy@doj.oregon.gov**."**

The FAQs for both Businesses[5] and Consumers,[6] which were initially published in May 2024, are a significant part of those outreach efforts. The FAQs provide guidance on issues and questions raised by Oregon businesses and consumers trying to understand and comply with the OCPA. These materials were shared with the Consumer Privacy Task Force listserv to ensure wide distribution among the stakeholders that participated in developing the OCPA.

The FAQs are living documents, and have been revised several times since July 1, 2024, to address new issues that have come up during early enforcement efforts. We are currently working on a separate set of FAQs for non-profit entities, which will be subject to the OCPA on July 1, 2025.

---

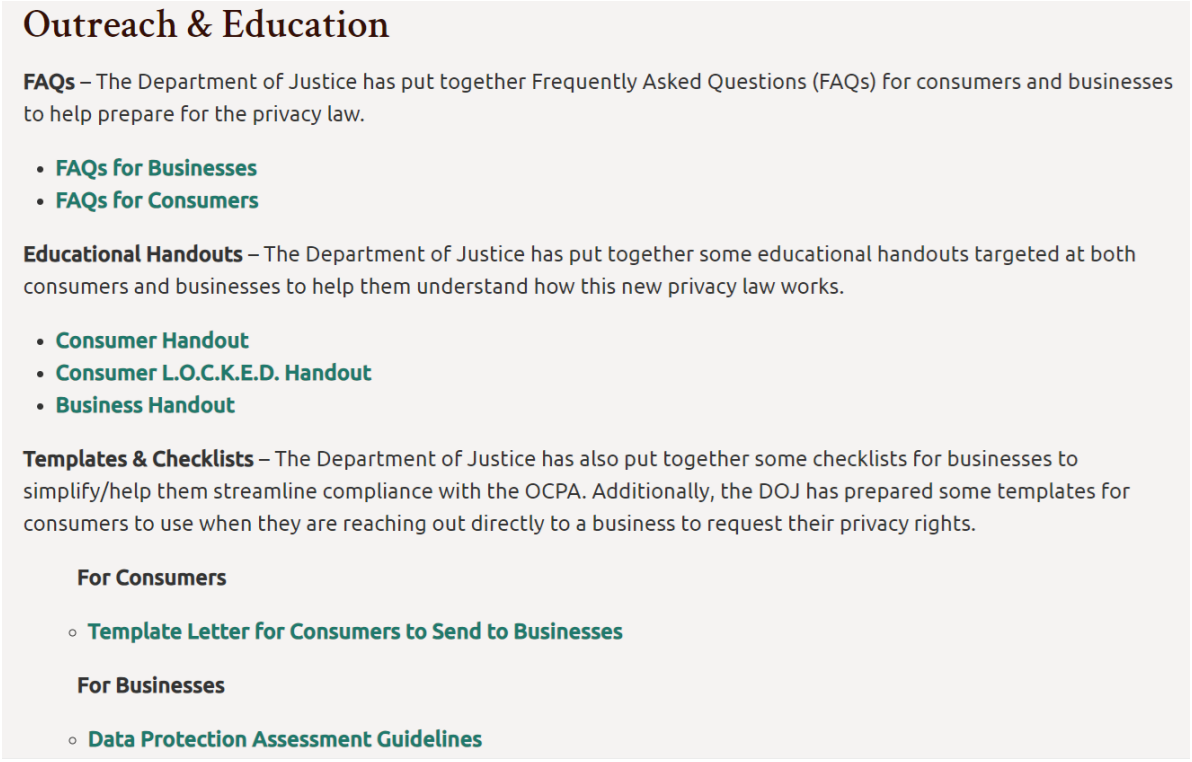
[2] In addition to the OCPA, the AFCP Section enforces the *Oregon Consumer Information Protection Act*, and other state and federal laws governing privacy and data security.

[3] Oregonians Gain Significant New Consumer Privacy Protections.

[4] Consumer Privacy.

[5] Privacy Law FAQs for Businesses.

[6] Privacy Law FAQs for Consumers.



Outreach & Education

FAQs – The Department of Justice has put together Frequently Asked Questions (FAQs) for consumers and businesses to help prepare for the privacy law.

- FAQs for Businesses
- FAQs for Consumers

Educational Handouts – The Department of Justice has put together some educational handouts targeted at both consumers and businesses to help them understand how this new privacy law works.

- Consumer Handout
- Consumer L.O.C.K.E.D. Handout
- Business Handout

Templates & Checklists – The Department of Justice has also put together some checklists for businesses to simplify/help them streamline compliance with the OCPA. Additionally, the DOJ has prepared some templates for consumers to use when they are reaching out directly to a business to request their privacy rights.

For Consumers

- Template Letter for Consumers to Send to Businesses

For Businesses

- Data Protection Assessment Guidelines

DOJ performed extensive outreach over the last year to prepare businesses for the OCPA. Leading up to July 1, Privacy Unit members spoke on panels with other privacy law regulators to discuss the OCPA and presented to lawyers and technology professionals in Oregon. In the last six months, DOJ sent education letters, with links to the Consumer Privacy website, to Oregon trade associations and attorney groups that represent businesses likely to be impacted by the OCPA. The DOJ also generated a list of data brokers and sent "light" cure letters to all data brokers[7] who had not incorporated/addressed the OCPA in their public-facing privacy notices. And we participated in several webinars and in-person trainings targeting businesses (and their advisors) likely to be controllers under the OCPA. That included presenting on OCPA requirements to the Non-Profit Association of Oregon.

DOJ also conducted outreach directly to consumers. Given the nature of the OCPA, it is vital that individual Oregonians know about their new rights under the OCPA, as well as how to report any violations they encounter by using the Consumer Privacy Complaint Portal (discussed in the next section). To that end, we led multiple educational/informational sessions targeted to consumers, including with the following organizations: PDX Privacy/TA3M Webinar, EdTech Webinar, and the PDX Digital Safety Fair.

DOJ also contracted with Gard Communications to run an educational and marketing campaign targeted towards consumers. As part of this campaign, Gard conducted a survey of around 350 Oregonians, to better understand what their attitudes and concerns are around privacy.[8] As a result of information learned from the

[7] Data brokers, which collect and sell consumer's personal data to other organizations (marketing, direct to retail companies, other data brokers, etc.), are subject to the OCPA if they meet either of the numeric thresholds set forth in the law. Some states, including Oregon require data brokers to register with the state and the state maintains a public data broker registry. The Privacy Unit used those state data broker registries to generate a list of which data brokers would likely fall under the OCPA. Data Broker Registry.

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

survey, we created new educational materials and social media graphics, which are on the Consumer Privacy website and available for printing and sharing.

Additionally, we conducted legislative outreach to inform state legislators of DOJ's implementation efforts. On September 24, 2024, Privacy Unit personnel presented on the OCPA to the joint Judiciary Committees during the Fall Legislative Days. The Oregon Consumer Privacy Act (OCPA) (oregonlegislature.gov). At least four state legislators included the OCPA in their newsletter/social media/web posts.

We have also, when appropriate, issued scam alerts notify consumers of trends we are seeing regarding privacy scams.[9] Finally, DOJ has released several press releases[10] to raise consumer and media awareness of the OCPA.

Consumer Privacy 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 that are not honoring their privacy rights requests.[11] The Privacy Unit intakes consumer complaints and evaluates the referenced businesses for potential OCPA violations.



Report a Complaint Under the Oregon Consumer Privacy Act

Consumers wishing to file a report about a suspected violation of the Oregon Consumer Privacy Act can use our online complaint form. (Note, this is a complaint form specifically for the privacy law.)

COMPLAINT FORM

After submitting a complaint, the complaint will be reviewed by a member of the Oregon Department of Justice's consumer privacy team. The Department of Justice may follow up with the consumer for more information, refer the complaint to another government agency if that is most appropriate, or in some cases, follow-up with the business to pursue the complaint.

Why should I report? The Department of Justice enforces the OCPA. Your complaint may be used to monitor industry compliance or to inform an enforcement action. For us to do our job, we need to hear from you! Tell us about any issues you're having with businesses concerning your new privacy rights.

If you have any questions, or aren't sure your complaint is OCPA related, feel free to call the Consumer Hotline at 1-877-877-9392. The Attorney General's Consumer Hotline is open from 8:30 a.m. to 4:30 p.m. and is staffed by dedicated volunteers who field more than 50,000 calls each year on various consumer issues.

When appropriate, we refer complaints to another department within the DOJ, or to other state agencies such as DCBS. While consumers are not given a case number to track regarding their complaint(s), once an open

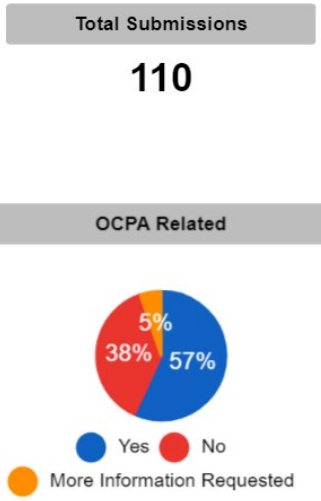
[9] How to Protect Yourself from Privacy Scammers - Oregon Department of Justice: Consumer Protection.

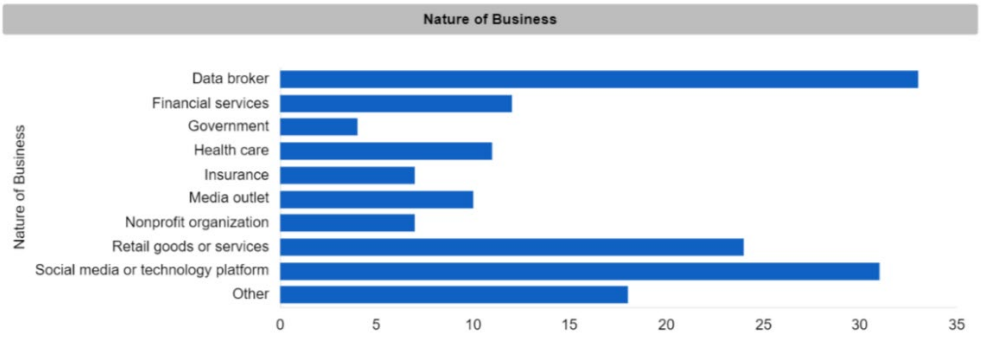
[10] *See* Oregonians Gain Significant New Consumer Privacy Protections; DOJ Survey Finds Most Oregonians Care About Privacy, Curious About New Law; Take action online to protect your privacy rights - Oregon Department of Justice : Media.

[11] This is not the same dispute resolution process that the Consumer Complaint Specialists follow, because there are different legal routes for resolution for those issues. The Privacy Unit is primarily using the complaints to identify potential cure notices at this point in time.

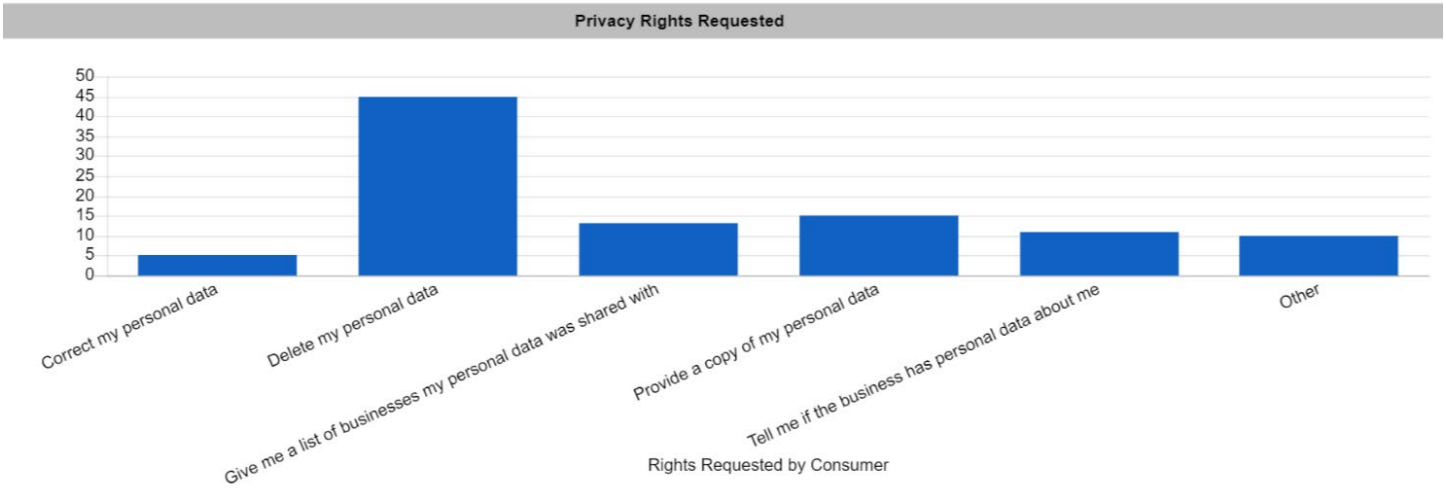
matter is closed, a template email is sent to the consumer confirming that action was taken on their complaint.

As of January 1, 2025, the Privacy Unit had received 110 complaints, the majority of which came directly through the Privacy Complaint Portal. This is a significant number compared to other similarly sized states, showing that Oregonians care about their privacy rights, and that they are engaged with the process. Connecticut, for example, received only 30 complaints in the first six months of the effective date of their privacy law.[12]





The DOJ has received the most complaints about data brokers (specifically "background" websites purportedly providing in-depth background reports on individuals for a fee), and social media/technology platforms. According to our metrics, the number one right consumers have requested and been denied, is the right to delete their data.



[12] *See* PURSUANT TO PUBLIC ACT 22-15, "AN ACT CONCERNING PERSONAL DATA PRIVACY AND ONL INE MONITORING.

Six Months of Enforcement- Cure Period

The cure notice is the primary method by which the Privacy Unit enforces initially identified violations under the Oregon Consumer Privacy Act. The cure notice is a letter mandated by the OCPA until January 1, 2026, if the potential violation(s) are curable, or fixable. The Privacy Unit has been busy with enforcement. Those efforts have already resulted in significant changes to privacy notices, to provide more transparency regarding data practices, and better reflect consumer rights between companies and individuals.

In the last six months, the Privacy Unit has initiated and closed 21 OCPA cure letter matters. Those matters included sending inquiry letters (to obtain more information needed to assess OCPA compliance) and letters with both inquiry and cure components. In addition, some businesses received "light" cure letters, including 20 data brokers, who did not address the OCPA in their privacy notices. These letters are called "light" because they only asked companies to incorporate the law in their online privacy notice and did not cite specific deficiencies in those notices.

Some of the common deficiencies identified in the notices included:

- **Lacking disclosures** (e.g., failure to incorporate notice of consumer rights under the OCPA);
- **Inadequate disclosures** (e.g., failure to sufficiently inform Oregon consumers about their rights under the law, specifically the list of third parties their data has been sold to);
- **Confusing privacy notices** (e.g., notices that are not clear or accessible to the average consumer);
    - **For example:** notices that name one or two states in the "your state rights" section but not Oregon, giving consumers the impression that privacy rights are only available to people who live in those named states.
- **Lacking or burdensome rights mechanisms** (e.g., failure to include a clear and conspicuous link to a webpage enabling consumers to opt out, request their privacy rights, or inappropriately difficult authentication requirements).

The OCPA gives companies a 30-day window to cure identified violations. Overall, the responses we have received to date have been positive. Most companies updated privacy notices and/or improved consumer rights mechanisms quickly upon receiving cure notices.

Conclusion

Looking forward, starting July 1, 2025, the OCPA will be extending to cover qualifying nonprofit entities. The Privacy Unit has already performed outreach to some of Oregon's nonprofits and is preparing nonprofit-specific support materials for the Consumer Privacy Webpage, such as FAQs for Nonprofits.

The cure period remains in place until January 1, 2026, meaning that the Privacy Unit will continue to issue warnings via cure letters until that date has passed. Such letters provide ongoing learning opportunities for businesses and nonprofits, while still allowing the DOJ to safeguard the privacy rights of Oregonians. After January 1, 2026, the Privacy Unit can focus on other implementation tasks including enforcing the OCPA's universal opt-out mechanism requirements that go into effect at the beginning of next year.