OR AG Issues Guidance Regarding OR State Laws and AI

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On December 24, 2024, the Oregon Attorney General published AI guidance, "What you should know about how Oregon's laws may affect your company's use of Artificial Intelligence," (the "Guidance") that clarifies how existing Oregon consumer protection, privacy and anti-discrimination laws apply to AI tools. Through various examples, the Guidance highlights key themes such as privacy, accountability and transparency, and provides insight into "core concerns," including bias and discrimination.

Consumer Protection – Oregon's Unlawful Trade Practice Act ("UTPA")

The Guidance emphasizes that misrepresentations, even when they are not directly made to the consumer, may be actionable under the UTPA, and an AI developer or deployer may be "liable to downstream consumers for the harm its products cause." The Guidance provides a non-exhaustive list of examples that may constitute violations of the UTPA, such as:

- failing to disclose any known material defect or nonconformity when delivering an AI product;
- misrepresenting that an AI product has characteristics, uses, benefits or qualities that it does not have;
- using AI to misrepresent that real estate, goods or services have certain characteristics, uses, benefits or qualities (e.g., a developer or deployer using a chatbot while falsely representing that it is human);
- using AI to make false or misleading representations about price reductions (e.g., using AI generated ads or emails indicating "limited time" or "flash sale" when a similar discount is offered year-round);
- using AI to set excessively high prices during an emergency;
- using an AI-generated voice as part of a robocall campaign to misrepresent or falsify certain information, such as the caller's identity and the purpose of the call; and
- leveraging AI to use unconscionable tactics regarding the sale, rental or disposal of real estate, goods or services, or collecting or enforcing an obligation (e.g., knowingly taking advantage of a consumer's ignorance or knowingly permitting a consumer to enter into a transaction that does not materially benefit them).

Data Privacy – Oregon Consumer Protection Act ("OCPA")

In addition, the Guidance notes that developers, suppliers and users of AI may be subject to OCPA,

given generative AI systems ingest a significant amount of words, images and other content that often consists of personal data. Key takeaways from the Guidance regarding OCPA include:

- developers that use personal data to train AI systems must clearly disclose that they do so in an accessible and clear privacy notice;
- if personal data includes any categories of sensitive data, entities must first obtain explicit consent from consumers before using the data to develop or train AI models;
- if the developer purchases or uses another data's company for model training, the developer may be considered a "controller" under OCPA, and therefore must comply with the same standards as the company that initially collected the data;
- data suppliers and developers are prohibited from "retroactively or passively" altering privacy notices or terms of use to legitimatize the use of previously collected personal data to train AI models, and instead are required to obtain affirmative consent for any secondary or new uses of that data;
- developers and users of AI must provide a mechanism for consumers to withdraw previously-given consent (and if the consent is revoked, stop processing the data within 15 days of receiving the revocation);
- entities subject to OCPA must consider how to account for specific consumer rights when using AI models, including a consumer's right to (1) opt-out of the use of profiling in decisions that have legal or similarly significant effects (e.g., housing, education or lending) and (2) request the deletion of their personal data; and
- in connection with OCPA's requirement to conduct data protection assessments for certain processing activities, due to the complexity of generative AI models and proprietary data and algorithms, entities "should be aware that feeding consumer data into AI models and processing it in connection with these models likely poses heightened risks to consumers."

Data Security – Oregon Consumer Information Protection Act

The Guidance clarifies that AI developers (as well as their data suppliers and users) that "own, license, maintain, store, manage, collect, acquire or otherwise possess" personal information also must comply with the Oregon Consumer Information Protection Act, which requires businesses to safeguard personal information and implement an information security program that meets specific requirements. The Guidance also notes that to the extent there is a security breach, AI developers, data suppliers and users may be required to notify consumers and the Oregon Attorney General.

Anti-Discrimination – Oregon Equality Act

The Guidance explains that AI systems that "utilize discretionary inputs or produce biased outcomes that harm individuals based on protected characteristics" may trigger the Oregon Equality Act. The law prohibits discrimination based on race, color, religion, sex, sexual orientation, gender identity, national origin, marital status, age or disability, including in connection with housing and public accommodations. The Guidance also includes an illustrative example regarding how the law applies to the use of AI. Specifically, the Guidance notes that a rental management company's use of an AI mortgage approval system that consistently denies loans to qualified applicants based on certain neighborhoods or ethnic backgrounds because the AI system was trained on historically biased data may be considered a violation of the law.

Source URL:https://natlawreview.com/article/or-ag-issues-guidance-regarding-or-state-laws-and-ai