

SENATE BILL REPORT

E2SHB 1170

As of February 20, 2026

Title: An act relating to informing users when content is developed or modified by artificial intelligence.

Brief Description: Informing users when content is developed or modified by artificial intelligence.

Sponsors: House Committee on Technology, Economic Development, & Veterans (originally sponsored by Representatives Shavers, Taylor, Ryu, Ramel, Fosse, Wylie, Pollet, Ormsby and Hill).

Brief History: Passed House: 2/13/26, 56-37.

Committee Activity: Environment, Energy & Technology: 2/20/26.

Brief Summary of Bill

- Requires providers of certain generative artificial intelligence (AI) systems to make a provenance detection tool available to users.
- Requires providers of certain generative AI systems to offer users the option of including disclosures in content created or altered by the systems.
- Provides for enforcement by the attorney general.

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Staff: Alicia Kinne-Clawson (786-7407)

Background: Artificial Intelligence. Artificial intelligence (AI) is defined and understood in different ways. The National Institute of Standards and Technology (NIST), in its AI Risk Management Framework, defines an AI system as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions,

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

recommendations, or decisions influencing real or virtual environments.

Artificial Intelligence Task Force. In 2024, the Legislature established the AI Task Force, administered by the Office of the Attorney General. The AI Task Force is tasked with assessing current uses and trends of AI and making recommendations to the Legislature regarding guidelines and potential legislation for the use of AI systems.

Summary of Bill: Provenance Detection Tool. A covered provider must make available a provenance detection tool that:

- allows a user to assess whether the image, video, or audio content was created or altered by the providers AI system;
- outputs any system provenance data that is detected in the content;
- assures results are publicly accessible;
- allows the user to upload content or provides a tool linking to online content; and
- can be used without visiting the providers website.

A covered provider may not collect or retain personal information from users of the provenance detection tool unless the personal information is collected through the user providing feedback and is used to improve the tool.

Manifest Disclosure. A covered provider must offer a user the option to include a manifest disclosure in image, video, or audio content that was created or altered by the AI system. The disclosure must:

- identify content as AI generated or modified;
- be clear and conspicuous for a reasonable person; and
- difficult to remove, to the extent it is technically feasible.

A covered provider must include a latent disclosure in AI generated image, video, or audio that meets all of the following criteria:

- conveys information including name of the provider, name and version of the AI system, time and date the disclosure was added, a unique identifier, and personal provenance information;
- is detectable by the providers provenance detection tool;
- is consistent with widely accepted industry standards; and
- is difficult to remove.

If a covered provider licenses its generative AI system to a third party, the covered provider must require that the licensee maintain the system's capability to include required disclosures. If a covered provider knows that a third-party licensee modified a licensed generative AI system such that it is no longer capable of including the required disclosures, the covered provider must revoke the license. A third-party licensee must cease using a licensed generative AI system after the license for the system has been revoked.

The requirements regarding provenance detection tools and disclosures do not apply to any

product, service, internet website, or application that provides exclusively video game, or interactive experiences. The requirements also do not apply to systems used solely for upscaling, noise reduction, or compression.

Enforcement. For actions brought by the attorney general, violations of requirements relating to provenance detection tools and disclosures are deemed to affect the public interest and constitute an unfair or deceptive act in trade or commerce for purposes of the Consumer Protection Act. Only the attorney general can bring an action under the Consumer Protection Act pursuant to the bill.

Covered provider is defined as a person who has used, or intends to use, a certain threshold of computer power to train a foundation model; uses such foundation model to produce a generative AI system that is publicly accessible within Washington; and had annual gross revenues in excess of \$500 million in the preceding calendar year. Covered provider does not include public entities, tribal nations, or generative AI systems licensed or sold for business-to-business purposes.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: The bill takes effect on January 1, 2028.

Staff Summary of Public Testimony: PRO: This bill is intended to focus on large users. The scope is limited to high risk products like data and photos. Some people will say this is not technically feasible. AI developers already have the tools required under this bill available. This approach closely appears the version in California that has already passed. This bill is narrow and practical. The bill protects workers from digital impersonation. When deepfakes spread it can jeopardize jobs before people have a chance to respond. We think the bill is completely technically feasible to implement. In fact, people have already begun implementing the California law. This bill creates consistency. This is the kind of thing we do in the consumer protection world all the time and it makes sense to do it here. It helps people distinguish authentic content from manufactured. This is not a government restriction on content. It's a disclosure of truthful content. This assures that the bad actors can't hide behind anonymity of algorithms.

CON: The bill as written is unworkable. The revised language introduces ambiguity for deployers. It introduces new terms that are undefined. The California bill is currently stalled and unworkable. The bill still has significant challenges. Our concern is timing and uncertainty. Stakeholders in California are still working through technical uncertainty. We don't know if California will translate to Washington. This bill can be compared to requiring a nutrition label. This bill instead requires the governments message to be embedded inside

user speech.

Persons Testifying: PRO: Representative Clyde Shavers, Prime Sponsor; Jai Jaisimha, Transparency Coalition.ai; Danica Noble; STEVE WIMMER, Transparency Coalition; Carissa Larsen, Washington State Labor Council, AFL-CIO.

CON: John Coleman, Foundation for Individual Rights and Expression; Amy Harris, Washington Technology Industry Association; Max Martin, Association of Washington Business.

Persons Signed In To Testify But Not Testifying: No one.