

HOUSE BILL REPORT

HB 1170

As Reported by House Committee On:

Technology, Economic Development, & Veterans

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: Representatives Shavers, Taylor, Ryu, Ramel, Fosse, Wylie, Pollet, Ormsby and Hill.

Brief History:

Committee Activity:

Technology, Economic Development, & Veterans: 1/17/25, 1/28/25 [DPS], 1/14/26, 1/16/26 [DP2S].

Brief Summary of Second Substitute 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.
- Requires providers of certain generative AI systems to include latent disclosures in content created by their systems.

HOUSE COMMITTEE ON TECHNOLOGY, ECONOMIC DEVELOPMENT, & VETERANS

Majority Report: The second substitute bill be substituted therefor and the second substitute bill do pass. Signed by 7 members: Representatives Ryu, Chair; Cortes, Donaghy, Paul, Shavers, Simmons and Thomas.

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.

Minority Report: Do not pass. Signed by 4 members: Representatives Barnard, Ranking Minority Member; Keaton, Penner and Volz.

Staff: Emily Poole (786-7106).

Background:

Artificial intelligence (AI) is defined and understood in different ways. The National Institute of Standards and Technology, 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, recommendations, or decisions influencing real or virtual environments.

In 2024 the Legislature established the Artificial Intelligence Task Force, administered by the Office of the Attorney General. The 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 (Second Substitute):

Definitions.

Definitions are provided for certain terms, including "covered provider," which refers to a person who: (1) has used, or intends to use, a certain threshold of computing power to train a foundation model; (2) uses such foundation model to produce a generative AI system that is publicly accessible within Washington; and (3) 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.

Other terms are defined, including "artificial intelligence," "generative artificial intelligence," and "provenance data," among others.

Provenance Detection Tool.

A covered provider is required to make available a provenance detection tool at no cost to the user. The tool must:

- allow a user to assess whether image, video, or audio content was created or altered by the covered provider's generative AI system;
- output any system provenance data that is detected in the content;
- have results that are publicly accessible, with some exceptions;
- allow a user to upload content or provide a uniform resource locator linking to online content; and
- allow a user to invoke the tool without visiting the covered provider's website.

A covered provider is prohibited from:

- collecting or retaining personal information from users of the tool, with certain exceptions;
- retaining any content submitted to the tool for longer than is necessary to comply with applicable requirements; and
- retaining any personal provenance data from content submitted to the tool by a user.

Disclosures.

A covered provider is required to offer the user the option to include a manifest disclosure in image, video, or audio content created or altered by the covered provider's generative AI system. The disclosure must:

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

A covered provider is required to include a latent disclosure in AI-generated image, video, or audio content created by the covered provider's generative AI system. To the extent it is technically feasible and reasonable, the disclosure must convey:

- the name of the covered provider;
- the name and version number of the generative AI system that created or altered the content;
- the time and date that the disclosure was added to the generated or altered content;
- a unique identifier; and
- personal provenance information only to the extent that a user has affirmatively chosen to add such information.

The latent disclosure must also be detectable by the covered provider's provenance detection tool, consistent with widely accepted industry standards, and difficult to remove or recoverable, to the extent it is technically feasible.

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, television, streaming, movie, or interactive experiences.

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.

Second Substitute Bill Compared to Original Bill:

The second substitute:

- adds an intent section;
- modifies the definition of "artificial intelligence" to generally refer to the use of machine learning and related technologies that use data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, instead of an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments;
- modifies the definition of "covered provider" by:
 - removing the monthly usership threshold;
 - adding thresholds based on both the computing power used to train a foundation model and the person's revenues; and
 - excluding public entities, tribal nations, and business-to-business systems;
- replaces the definition of "generative artificial intelligence system" with a definition of "generative artificial intelligence," defined as an AI system that generates novel data or content based on a foundation model;
- modifies the definition of "personal information" to be the same as the definition in RCW 19.373.010, instead of the definition in RCW 19.255.005;
- modifies the definition of "system provenance data" to include data that contains information that helps a user assess authenticity, instead of information related to content authenticity;
- requires a covered provider to make available a "provenance detection tool" instead of an "artificial intelligence detection tool;"
- removes the requirement that the provenance detection tool must not output any personal provenance data that is detected in content;
- requires the provenance detection tool's results to be publicly accessible, instead of the tool being publicly accessible;
- removes the requirement that the provenance detection tool must support an application programming interface;
- requires a covered provider to consider, instead of incorporate, user feedback;
- establishes that if a covered provider makes available a provenance detection tool for the purpose of complying with another applicable law or regulation, and the tool is reasonably similar to the tool that would otherwise be made available pursuant to the bill, the tool must be deemed to satisfy applicable requirements under the bill;
- requires that when covered providers offer users the option of including manifest disclosures in content, the manifest disclosures must identify the content as AI-

- generated or -modified content, instead of just AI-generated;
- establishes that manifest disclosures must be difficult to remove, and latent disclosures must be difficult to remove or recoverable, instead of permanent or extraordinarily difficult to remove;
- requires that latent disclosures include the time and date that the disclosure was added, instead of the time and date of the content's creation or alteration;
- requires that latent disclosures include personal provenance information only to the extent that a user has chosen to add such information;
- establishes that a covered provider is not in violation of requirements relating to manifest and latent disclosures solely because such disclosures were unintentionally removed, altered, or rendered unreadable, if the covered provider used commercially reasonable and industry-accepted measures designed to preserve the disclosures;
- specifies that the types of products, services, websites, and applications exempted from the bill's requirements include products, services, websites, and applications that exclusively provide the sale of goods or services directly to consumers through the internet, allowing customers to browse, select, and purchase items virtually;
- modifies the enforcement provisions by:
 - establishing that any waiver of the chapter is contrary to public policy and is void and unenforceable; and
 - limiting the per se violation of the Consumer Protection Act to apply to only actions brought by the Attorney General and establishing that only the Attorney General may bring an action under the Consumer Protection Act to enforce the chapter; and
- establishes an effective date of January 1, 2028.

Appropriation: None.

Fiscal Note: Available.

Effective Date of Second Substitute Bill: The bill takes effect on January 1, 2028.

Staff Summary of Public Testimony:

(In support) There is an urgent need for AI regulation. Popular social media tools operate as deepfake creators, and they can disseminate disinformation, ruin reputations, and cause emotional harm. This bill is modeled on California legislation, and the proposed substitute mirrors work that has been done on this issue in other states. This bill is not heavy-handed, and it does not affect small businesses. Washingtonians need clear borders between real and AI-generated images, because AI is improving and can produce increasingly realistic images.

(Opposed) This bill raises First Amendment concerns. This bill goes beyond legal frameworks that apply to commercial speech. There are problems with implementing this

bill in practice, given variations in accuracy, consistency, and methods used in watermarking content. The bill is modeled on legislation that is already being reconsidered in California. Companies are moving away from watermarking, because there is currently no reliable way of implementing permanent watermarks across different types of content. Watermarks can be removed or manipulated, so relying on watermarking technology will give users a false sense of security. The bill should include a right to cure alleged violations. This bill may be overbroad in its scope.

(Other) This bill attempts to provide users with an understanding of what content is AI-generated. A free tool can help mitigate risks of misinformation. It is good that the proposed substitute does not include a private right of action. Washington should exercise caution before advancing legislation that is based on a California framework that is being actively examined and revised. The technical assumptions in the bill do not reflect how the technology is evolving. The central challenge is that the watermarking solution contemplated has been overtaken by technological developments, because watermarks can be removed. This bill could have unintended consequences on accessibility. The definition of covered provider may cause challenges for enforcement.

Persons Testifying: (In support) Jai Jaisimha, Transparency Coalition.ai; and Yale Moon.

(Opposed) John Coleman, Foundation for Individual Rights and Expression; Max Martin, Association of Washington Business; and Amy Harris, WA TECHNOLOGY INDUSTRY ASSN.

(Other) Rose Feliciano, TechNet; and Sumayo Hassan, Washington State Attorney General's Office.

Persons Signed In To Testify But Not Testifying: None.