January 14, 2026

Re: House Bill 1170 - Informing users when content is developed or modified by artificial intelligence.

Dear Honorable Representatives of the House Committee on Technology, Economic Development, & Veterans,

Consumer Reports[1] writes regarding HB 1170. This bill could be an important first step for tackling a growing problem for consumers in Washington: differentiating between authentic and AI-generated content online. Its measured approach is similar to a law passed in California in 2024, SB 942,[2] and as such, passage in Washington state would not create new obligations for companies that operate nationally. It would also build upon voluntary provenance standards that major tech companies are currently developing, such as those proposed by the Coalition for Content Provenance and Authenticity (C2PA). However, in order for the bill to be effective and enforceable, we urge the committee to make some revisions.

The growing problem of deceptive AI content

AI voice and likeness cloning tools have unlocked scammers' abilities to generate deepfake videos falsely depicting celebrities and political figures endorsing products, suggesting investments, and urging citizens to take action. Recent research suggests that consumers struggle to recognize deepfake videos as false, and also overestimate their own ability to detect deepfakes.[3]

AI-powered celeb-bait has proliferated on social media. An investigation by ProPublica identified videos on Meta seemingly depicting President Trump and former president Biden—each with their distinctive tone and cadence—offering cash handouts if people filled out

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] See California Business and Professions Code § 22757

[3] Nils C Köbis et al., Fooled twice: People cannot detect deepfakes but think they can, National Library of Medicine National Center for Biotechnology Information, (2021), https://pubmed.ncbi.nlm.nih.gov/34820608/.

an online form.[4] 404 Media has reported on the spread of AI clones of Joe Rogan, Taylor Swift, Ice Cube, Andrew Tate, Oprah, and The Rock pushing Medicare and Medicaid-related scams on YouTube.[5] Scammers have used an AI deepfake of Taylor Swift to hawk Le Creuset dishware.[6] Elon Musk's likeness has been frequently repurposed by scammers using AI video and voice tools to push fraudulent "investment" schemes. One consumer was reportedly scammed out of $690,000 after seeing a deepfaked Elon Musk endorse an investment opportunity.[7]

By far the most common use of generative AI deepfake technology appears to be creating non-consensual intimate images and pornography. A 2019 review of deepfakes online found that 96% were pornographic.[8] A 2023 analysis of non-consensual deepfakes found that at least 244,625 videos had been added to top websites set up to host deepfake porn videos in the preceding seven years, 113,000 of which were added in 2023, marking a 54% increase over the prior year.[9] Non-consensual intimate images, including of children, were readily found on Google image search and on Microsoft's Bing by NBC News.[10] Apps that promise to create an AI nude image based on an image of a real person are readily found online. Schools across the country, from New Jersey to Washington, have been grappling with students using AI to create non-consensual deepfakes of their fellow classmates.[11] Elected officials have also been targeted, and bad actors have attempted to use such images for blackmail.[12]

Consumer Reports is invested in addressing the issue of deceptive AI content. We've testified before Congress on the issue of deepfakes and AI-driven scams twice.[13] We've also conducted

---

[4] Craig Silverman and Priyanjana Bengani, Exploiting Meta's Weaknesses, Deceptive Political Ads Thrived on Facebook and Instagram in Run-Up to Election, ProPublica, (Oct. 31, 2024), https://www.propublica.org/article/facebook-instagram-meta-deceptive-political-ads-election.

[5] Jason Koelber, Deepfaked Celebrity Ads Promoting Medicare Scams Run Rampant on YouTube, 404 Media, (Jan. 9, 2024), https://www.404media.co/joe-rogan-taylor-swift-andrew-tate-ai-deepfake-youtube-medicare-ads/.

[6] Tiffany Hsu and Yiwen Lu, No, That's Not Taylor Swift Peddling Le Creuset Cookware, New York Times, (Jan. 9, 2024), https://www.nytimes.com/2024/01/09/technology/taylor-swift-le-creuset-ai-deepfake.html.

[7] Stuart Thompson, How 'Deepfake Elon Musk' Became the Internet's Biggest Scammer, New York Times, (Aug. 14, 2024), https://www.nytimes.com/interactive/2024/08/14/technology/elon-musk-ai-deepfake-scam.html.

[8] Tom Simonite, Most Deepfakes Are Porn, and They're Multiplying Fast, Wired, (Oct. 7, 2019), https://www.wired.com/story/most-deepfakes-porn-multiplying-fast/.

[9] Matt Burgess, Deepfake Porn Is Out of Control, Wired, (Oct. 16, 2023), https://www.wired.com/story/deepfake-porn-is-out-of-control/.

[10] Kat Tenbarge, Fake nude photos with faces of underage celebrities top some search engine results, NBC News, (Mar. 1, 2024), https://www.nbcnews.com/tech/internet/fake-nude-photos-faces-underage-celebrities-top-search-engine-results-rcna136828.

[11] Natasha Singer, Teen Girls Confront an Epidemic of Deepfake Nudes in School, New York Times, (Apr. 8, 2024), https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html.

[12] Coralie Kraft, Trolls Used Her Face to Make Fake Porn. There Was Nothing She Could Do., New York Times, (Jul. 31, 2024), https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html

[13] Justin Brookman, Consumer Reports testifies before Senate Judiciary on AI-powered deepfakes, Consumer Reports Advocacy, (May 21, 2025), https://advocacy.consumerreports.org/research/consumer-reports-testifies-before-senate-judiciary-on-ai-powered-deepfakes/

original research assessing six voice cloning products to determine whether they employ meaningful safeguards to stop fraud or misuse of their products.[14] That research found that it would be easy to create deepfake voice clones of other people using publicly available audio clips without their consent. Four of the six companies CR evaluated—ElevenLabs, Speechify, PlayAI, and Lovo—did not employ any technical mechanisms to ensure that CR researchers had the speaker's consent to generate a clone or to limit the cloning to the user's own voice. Instead, they only required that users check a box, confirming that they had the speaker's consent to make a clone. Four of the six companies (Speechify, Lovo, PlayHT, and Descript) required only a customer's name and/or email address to make an account.

What HB 1170 does, and suggested revisions

HB 1170 largely does three things. First, it requires generative AI providers with large user bases to provide a free tool to detect whether a piece of content was made or altered with their product. Second, these generative AI providers need to provide an option in their product for users to add a "manifest disclosure"—a label of some kind that is perceptible to a normal consumer, that identifies the content as AI generated, and that is extraordinarily difficult to remove. Lastly, covered generative AI providers must include latent disclosures in the content they generate. These disclosures must include key information, like the name of the covered provider and the name of the genAI system that created the content, without being perceptible to a normal consumer. However, this latent disclosure must be detectable by the provider's own AI detection tool, required by the bill.

Taken together, this bill would provide a means by which consumers could check if a specific piece of content was AI-generated—so long as they know which company's detection tool to use—and would give users the option to make clear that a video, image, or audio clip they are sharing is AI generated.

It's a good start, but it must be paired with additional provisions, such as requiring large online platforms (social media sites, search engines, etc) to also surface information from latent disclosures. This would make it clear to consumers when content is AI generated when scrolling social feeds without them having to chase down the right detection tool. Indeed, after passing legislation similar to HB 1170 in 2024, California passed companion legislation (AB 853) in

---

Justin Brookman, Consumer Reports to testify at Senate Committee hearing on protecting consumers from artificial intelligence enabled frauds and scams, Consumer Reports Advocacy, (November 18, 2024) https://advocacy.consumerreports.org/press_release/consumer-reports-to-testify-at-senate-committee-hearing-on-protecting-consumers-from-artificial-intelligence-enabled-frauds-and-scams/

[14] Grace Gedye, New Report: Do These 6 AI Voice Cloning Companies Do Enough to Prevent Misuse?, Consumer Reports Innovation Lab, (Mar. 10, 2025), https://innovation.consumerreports.org/new-report-do-these-6-ai-voice-cloning-companies-do-enough-toprevent-misuse/.

2025 that enacted these provisions. We urge the committee to review AB 853 and consider passing similar legislation alongside HB 1170.

There are also some changes we'd suggest the legislature make to HB 1170, to ensure it works as intended and is enforceable.

Protecting personal data

Sec. 2 (1) (c) prohibits the detection tool from outputting any personal provenance "to the extent technically feasible." This is too low a standard; consumer's personal data should not be exposed to the public via detection tools against their wishes. This particular language also sets a lower standard than existing law in California.[15] We recommend that the technical feasibility language be removed.

Clarifying content of manifest and latent disclosures

In Sec 3. (1) (a), the manifest disclosure, we suggest adding the following italicized text: "the disclosure identifies content as AI-generated *or modified content*" so that it is consistent with other parts of the legislation. We also suggest clarifying in Sec. 3(2)(a), that the latent disclosure must include the fact that the content was generated or modified by AI. Lastly, we suggest clarifying that the unique identifier required by Sec. 3(2)(a)(iv) should read "A unique identifier *that uniquely identifies each individual piece of content*." Otherwise, this provision may be interpreted as a unique identifier for each covered generative AI provider.

Ensuring that licensing is not a loophole

It is good that the bill requires covered providers to impose some requirements on anyone licensing their product, via contract. However, Sec 3.(3)(a) as currently written does not do enough to ensure that licensees provide the requisite transparency. The bill requires that when genAI providers license their products to third parties, they require the third party by contract to maintain the system's *ability* to include the disclosures required under the law. However, it is important not just that licensees have the ability to comply with the law, but that *they actually do comply*. Therefore, we suggest revising Sec. 3(3)(a) to read "require by contract that the licensee *ensures that* the system includes a disclosure required by subsection (2) of this section in content the system creates or alters."

Tightening exempt product categories

[15] See California Business and Professions Code § 22757.2 (a)(3)

Currently, Section 4 exempts “video game, television, streaming, movie, or interactive experiences.” This exemption is overbroad, and risks undermining the efficacy of the bill. We suggest revising this exemption to cover “any product, service, internet website, or application that provides exclusively *non-user-generated* television, streaming, movie, or interactive experiences.”

In conclusion, we appreciate the legislature’s work on this important topic as well as the opportunity to weigh in. We believe that with the appropriate revisions, this bill would be a reasonable, measured approach to helping consumers differentiate AI-generated content from authentic content online.

Sincerely,

Grace Gedye
Senior Policy Analyst
Consumer Reports