Date of Hearing: June 16, 2026

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 1000 (Becker) – As Amended June 9, 2026

SENATE VOTE: 33-1

SUBJECT: California AI Transparency Act

SYNOPSIS

Over the past three years, as generative artificial intelligence (GenAI) technologies have become more realistic and accessible, online content that appears genuine, but is actually false, has flooded social media and other large online platforms. This unmitigated spread of synthetic content threatens to harm Californians in numerous ways, such as through the proliferation of nonconsensual deepfake pornography, scams, and the distribution of targeted political disinformation.

California has sought to tackle the issue of GenAI-produced online content through a three-step plan: label all GenAI content "fake," label a significant portion of real content "real," and prominently display these labels online. Beginning this August, SB 942 (Becker, 2024) requires large GenAI platforms to include machine-detectable "latent disclosures" in their outputs. This bill would update SB 942 to reflect stakeholder feedback prior to that law going into effect on August 2nd.

This bill is supported by Transparency Coalition.ai, Center for AI and Digital Policy, and ForensicVB LLC. California Initiative for Technology & Democracy, TechNet, and Disability Rights California take "support if amended" positions. The bill has no opposition.

EXISTING LAW:

1) Defines the following terms:

   a. "Artificial intelligence" or "AI" to mean 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. (Bus. & Prof. Code § 22757.1. *et seq.*)

   b. "Assistive technology" to mean an item, piece of equipment, or product system, whether acquired commercially, modified, or customized, that is used to increase, maintain, or improve functional capabilities of individuals with disabilities and any service that directly assists an individual with a disability in the selection, acquisition, or use of the item, equipment, or product system. (Welf. & Inst. Code § 19461.)

   c. "Covered provider" to mean a person that creates, codes, or otherwise produces a generative artificial intelligence system that has over 1,000,000 monthly visitors or users and is publicly accessible within the geographic boundaries of the state. (Bus. & Prof. Code § 22757.1. *et seq.*)

d. "Generative artificial intelligence system" or "GenAI system" to mean an artificial intelligence that can generate derived synthetic content, including text, images, video, and audio, that emulates the structure and characteristics of the system's training data. (*Id.*)

e. "Latent" to mean present but not manifest. (*Id.*)

f. "Manifest" to mean easily perceived, understood, or recognized by a natural person. (*Id.*)

g. "Personal provenance data" to mean provenance data that contains either of the following:

1. Personal information.

2. Unique device, system, or service information that is reasonably capable of being associated with a particular user. (Bus. & Prof. Code § 22757.1. *et seq.*)

ii. "Personal provenance data" does not include information contained within a digital signature. (*Id.*)

h. "Provenance data" to mean data that is embedded into digital content, or that is included in the digital content's metadata, for the purpose of verifying the digital content's authenticity, origin, or history of modification. (*Id.*)

i. "System provenance data" to mean provenance data that is not reasonably capable of being associated with a particular user and that contains either information regarding the type of device, system, or service that was used to generate a piece of digital content, or information related to content authenticity. (*Id.*)

2) Beginning August 2, 2026, requires a covered provider to create and make freely available an AI detection tool that can be used to assess whether digital content was created or altered by the covered provider's GenAI system, and that has various specified characteristics.

a. Prohibits a covered provider from collecting or retaining personal information from users of the covered provider's AI detection tool, or retaining personal provenance data from user-uploaded content, except as specified. (Bus. & Prof. Code § 22757.1. *et seq.*)

3) Beginning August 2, 2026, requires a covered provider to offer a user of a GenAI tool the option to include a manifest disclosure in generated content, with various specified characteristics. (*Id.)*

4) Beginning August 2, 2026, requires a covered provider to include a latent disclosure in AI-generated image, video, or audio content, or content that is any combination thereof, created by the covered provider's GenAI system that, to the extent technically feasible and reasonable, conveys the name of the covered provider, the name and version number of the GenAI system that created or altered the content, the time and date of the content's creation or alteration, and a unique identifier, either directly or through a link to a permanent internet website. *(Id.)*

5) Requires that if a covered provider licenses their GenAI system to a third party, the covered provider shall require by contract that the licensee maintain the system's capability to include a latent disclosure.

    a. Requires that if a covered provider knows a licensee has removed the capability of a licensed GenAI system to include a latent disclosure, the covered provider shall revoke the licensee's contract.

    b. Requires that a licensee cease using a licensed GenAI system after its license has been revoked. (*Id.*)

6) Exempts from the AI Transparency Act any product, service, internet website, or application that provides exclusively non-user-generated video game, television, streaming, movie, or interactive experience. (*Id.)*

THIS BILL:

1) Amends the definitions in Section 22757.1 of the Business and Professions Code as follows:

    a. Adds "assistive technology," defined to have the same meaning as in Welf. & Inst. Code § 19461.

    b. Adds "minor modification," defined to mean any of the following alterations:

        i. A change to brightness, contrast, or color.

        ii. Sharpening.

        iii. Saturating.

        iv. File resizing.

        v. Scaling.

        vi. Cropping.

        vii. File format conversions.

        viii. Denoising and removal of background noise in audio.

    c. Removes "latent," "manifest," and "personal provenance data."

    d. Updates "provenance data" to mean information about the origin of a piece of digital content and the history of modifications to the content that is in a format that is compliant, or interoperable with, widely adopted specifications adopted by an established standards-setting body.

2) Makes various minor adjustments to the AI Transparency Act ahead of its August 2, 2026, implementation, including all of the following:

a. Recasts "AI detection tool" as "disclosure verification tool."

b. Expands the act to cover all GenAI systems, not only those that have over 1 million monthly visitors or users.

c. Clarifies that a disclosure verification tool shall allow users to assess whether content is created or altered, ***except by minor modification,*** by a covered provider's GenAI system.

d. Permits a disclosure verification tool to output personal information only if the user to whom the personal information pertains expressly consents, clearly and conspicuously in plain language, to including personal information specified by the user in the content.

e. Prohibits a covered provider from collecting, using, retaining, selling, sharing, or otherwise making available personal information derived either from a user of the covered provider's disclosure verification tool or from any content processed by the disclosure verification tool beyond what is strictly necessary to comply with the chapter.

f. Prohibits a covered provider from making access to the covered provider's GenAI system or disclosure verification tool contingent upon a user providing personal information beyond what is strictly necessary to comply with the chapter.

g. Allows a covered provider to comply with the requirement to make available a disclosure verification tool by instead directing a user to a third-party tool that complies with the chapter and is compatible with latent disclosures included in the covered provider's GenAI content.

h. Deletes the requirement that a covered provider offer a user the option to include a manifest disclosure in GenAI content.

i. Clarifies that latent disclosures included in GenAI content pursuant to Section 22757.3 are only required to include specified information to the extent "technically feasible."

j. Recasts "version number" as "version information."

k. Adds a requirement for a latent disclosure to include whether or not a GenAI system is "designed to primarily function as assistive technology."

l. Recasts various third-party contracting requirements as "terms of [a] license" that are required to be included by a covered provider. Clarifies that covered providers are only required to respond to violations by an "identifiable" third party licensee and reduces the timeline for responding to 72 hours. Clarifies that a covered provider is not required to "monitor, investigate, or otherwise inquire into a third-party licensee's use or modification of a licensed GenAI system" pursuant to the chapter.

3) Includes an urgency clause.

4) Makes various findings and declarations.

COMMENTS:

1) **Author's statement.** According to the author:

As AI technology advances, distinguishing between human and machine-generated content becomes increasingly challenging. This ambiguity poses significant risks to Californians, exacerbating problems of disinformation, harassment, and fraud while threatening the integrity of the information environment our democracy and economy depend on. In 2024, the legislature passed SB 942, the first bill in the nation to establish disclosure requirements for synthetic content. Since then, content provenance technology has developed in such a way that the leading technologies for embedding provenance are not accurately described by the law. Additionally, some methods of marking content are still in their nascency, and aren't yet robust enough to withstand adversarial exploitation or certain kinds of transformations (e.g. file compression, spoofing attacks, added noise to an image, or file type conversions). The original act also did not address the risk that visible labels create a binary signal implying that unlabeled content is authentic and labeled content is suspect - regardless of whether either inference is warranted. Furthermore, obligations for developers established SB 942 do not require that the information embedded in AI generated or modified content be consistent - or interoperable with - widely adopted standards. Last year, AB 853 (Wicks) established obligations for large online platforms to read provenance data, but only if it was compliant with such standards. This gap risks establishing a fragmented ecosystem where new methods of provenance disclosure that aren't interoperable with current standards are not read by large online platforms, and never subsequently relayed to users. This bill is critical to ensuring California's content labeling laws are effective at providing consumers with consistent information about where the content they see online comes from.

2) Background. *AI and GenAI.* The development of GenAI is creating exciting opportunities to grow California's economy and improve the lives of its residents. GenAI can generate compelling text, images and audio in an instant – but with novel technologies come novel safety concerns.

In brief, AI is the mimicking of human intelligence by artificial systems such as computers. AI uses algorithms – sets of rules – to transform inputs into outputs. Inputs and outputs can be anything a computer can process: numbers, text, audio, video, or movement. AI is not fundamentally different from other computer functions; its novelty lies in its application. Unlike traditional computer functions, AI can accomplish tasks that are normally performed by humans. AI that is trained on small, specific datasets to make recommendations and predictions is sometimes referred to as "predictive AI." This differentiates it from GenAI, which is trained on massive datasets in order to produce detailed text and images. When Netflix suggests a TV show to a viewer, that recommendation is produced by predictive AI that has been trained on the viewing habits of Netflix users. When ChatGPT generates text in clear, concise paragraphs, it uses GenAI that has been trained on the written contents of the internet.

Deepfakes and Disinformation. Image manipulation and video doctoring have existed for nearly as long as photography and recording equipment, but they have historically required great effort and talent. In the past few years, the rapid development of GenAI has drastically reduced those barriers to entry, allowing a vast quantity of convincing, but ultimately fake, content to be generated in an instant. The creation of imagery, video, and audio by GenAI has the potential to change the world by automating repetitive tasks and fostering creativity. When employed by bad actors, however, these capabilities have the potential to destroy lives and destabilize societies.

Deepfake pornography. Since its inception, GenAI has been used to subject women and girls to image-based sexual abuse. While high-profile celebrities were most often targeted when this

technology was first developed,[1] open-source GenAI models have been exploited to make this technology more accessible and affordable. This has led to a proliferation of websites and phone-based apps that offer user-friendly interfaces for uploading clothed images of real people to generate photorealistic nude images of not only adults, but also children. According to a *New York Times* article:

> Boys in several states have used widely available "nudification" apps to pervert real, identifiable photos of their clothed female classmates, shown attending events like school proms, into graphic, convincing-looking images of the girls with exposed A.I.-generated breasts and genitalia. In some cases, boys shared the faked images in the school lunchroom, on the school bus or through group chats on platforms like Snapchat and Instagram, according to school and police reports.[2]

In February 2024, deepfake nude images of 16 eighth-grade students were circulated among students at a California middle school.[3] Similar reports of abuse have been reported across the country and show no sign of abating.[4] In the first six months of 2024, nudification sites had been visited over 200 million times.[5] Meanwhile, a 2024 study from Center on Democracy and Technology reports that 40% of students were aware of deepfakes being shared at school, 15% of which depicted an individual in a sexually explicit or intimate manner. In over 60% of these cases, the images were distributed via social media.[6]

Scams. GenAI-powered speech and video is driving a new era in scamming. These AI tools are often trained on publicly available data, and as a result, the more data a target has online, the easier it is to develop a passable imitation of them or their loved ones. This is especially true of wealthy clients, whose public appearances, including speeches, are often widely available on the internet.[7] For example, a complicated scam utilizing both deepfake video and false audio was

---

[1] Brian Contreras, "Tougher AI Policies Could Protect Taylor Swift—And Everyone Else—From Deepfakes," *Scientific American* (Feb. 8. 2024) accessed at www.scientificamerican.com/article/tougher-ai-policies-could-protect-taylor-swift-and-everyone-else-from-deepfakes/.

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

[3] Mackenzie Tatananni, " 'Inappropriate images' circulate at yet another California high school, as officials grapple with how to protect teens from AI porn created by classmates," *Daily Mail* (Apr. 11, 2024) *accessed at* https://www.dailymail.co.uk/news/article-13295475/Inappropriate-images-California-Fairfax-High-School-AI-deepfake.html.

[4] Tim McNicholas, "New Jersey high school students accused of making AI-generated pornographic images of classmates," *CBS News* (Nov. 2, 2023), https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/; Lauraine Langreo, "Students Are Sharing Sexually Explicit 'Deepfakes.' Are Schools Prepared?" *Ed Week* (Sept. 26, 2024), https://www.edweek.org/leadership/studentsare-sharing-sexually-explicit-deepfakes-are-schools-prepared/2024/09; Gabrielle Hunt and Daryl Higgens "AI nudes of Victorian students were allegedly shared online. How can schools and parents respond to deepfake porn?," *The Guardian* (June, 12, 2024), https://www.theguardian.com/australia-news/article/2024/jun/12/ai-nudes-of-victorian-students-were-allegedly-shared-online-how-canschools-and-parents-respond-to-deepfake-porn.

[5] *People of the State of California v. Sol Ecom, Inc, et al.* (2024) Case No. CGC-24-617237, p. 2, https://www.sfcityattorney.org/wp-content/uploads/2024/08/2024-08-16-First-Amended-Complaint_Redacted.pdf

[6] Elizabeth Laird, Maddy Dwyer and Kristin Woelfel, "In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools," *Center for Democracy & Technology* (Sept. 26, 2024), https://cdt.org/wp-content/uploads/2024/09/FINAL-UPDATED-CDT-2024-NCII-Polling-Slide-Deck. Pdf.

[7] Emily Flitter and Stacy Cowley, "Voice Deepfakes Are Coming for Your Bank Balance", *New York Times (*Aug. 30, 2023), www.nytimes.com/2023/08/30/business/voice-deepfakes-bank-scams.html.

recently performed in Hong Kong. A multinational company lost $25.6 million after employees were fooled by deepfake technology, with one incident involving a digitally recreated version of its chief financial officer ordering money transfers in a video conference call. Everyone present on the video call, except the victim, was a fake representation of real people. The scammers applied deepfake technology to turn publicly available video and other footage into convincing versions of the meeting's participants.[8]

In December 2024, the FBI issued a public service announcement warning about the potential dangers posed by GenAI.[9] Among the concerns highlighted was the technology's ability to significantly lower the barrier for producing counterfeit documents, such as fake IDs, passports, and other fraudulent government-issued identification, which could greatly facilitate identity theft. Additionally, GenAI enables the creation of entirely fictitious profiles on social media and dating platforms, which can be used to exploit individuals both financially and emotionally.

Elections. Deepfake technology is being used around the world to spread disinformation and propaganda. This has already been observed in Slovakia, where deepfake audio influenced an election in 2023:

> Days before a pivotal election in Slovakia to determine who would lead the country, a damning audio recording spread online in which one of the top candidates seemingly boasted about how he'd rigged the election. And if that wasn't bad enough, his voice could be heard on another recording talking about raising the cost of beer. The recordings immediately went viral on social media, and the candidate, who is pro-NATO and aligned with Western interests, was defeated in September by an opponent who supported closer ties to Moscow and Russian President Vladimir Putin.[10]

Similar deepfakes surfaced in the United States ahead of the 2024 presidential election. In July 2024, Elon Musk shared a video featuring an AI-generated voice clone of then-Vice President Kamala Harris, in which the fabricated voice claimed she was a "diversity hire" due to being a woman of color and that she "did not know the first thing about running a country."[11] Although Musk admitted two days after posting that the video was intended as satire, the potential impact of such content on political campaigns remains a serious concern. In 2023, the Legislature enacted a trio of bills aimed at addressing elections deepfakes: AB 2655 (Berman, Ch. 261, Stats. 2024), which imposes removal and disclosure obligations on large online platforms during the four months leading up to an election; AB 2839 (Pellerin, Ch. 262, Stats. 2024), which prohibits the distribution of election materials containing certain types of deceptively altered digital content; and AB 2355 (Carillo, Ch. 260, Stats. 2024), which requires AI-altered campaign

---

[8] Harvey Kong, "'Everyone looked real': multinational firm's Hong Kong office loses HK$200 million after scammers stage deepfake video meeting," *South China Morning Post* (Feb. 4, 2024), www.scmp.com/news/hong-kong/law-and-crime/article/3250851/everyone-looked-real-multinational-firms-hong-kong-office-loses-hk200-million-after-scammers-stage.

[9] Department of Justice Federal Bureau of Investigations, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud" (Dec. 3, 2024) , https://www.ic3.gov/PSA/2024/PSA241203.

[10] Curt Devine, Donie O'Sullivan, Sean Lyngass, "A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning," *CNN* (Feb. 1, 2024), www.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html.

[11] Ken Bensinger, "Elon Musk Shares Manipulated Harris Video, in Seeming Violation of X's Policies", *The New York Times* (July 27, 2024), https://www.nytimes.com/2024/07/27/us/politics/elon-musk-kamala-harris-deepfake.html

materials to include clear disclosures. The first two bills, however, have been blocked from being enacted by legal proceedings.

Content Provenance. Many of the issues associated with deepfakes could be resolved, if only there were a reliable way to identify GenAI content. While at present no single solution exists, there are ongoing efforts to embed information related to "content provenance," the verifiable history of a piece of content, into both GenAI products and the products of real-life recorders, such as digital cameras. Under this framework, the users of social media platforms would be able to rely on provenance data to identify trustworthy content.

Metadata. The Merriam-Webster Dictionary defines metadata as "data that provides information about other data." In practice, metadata is a structured set of descriptors attached to digital content. A photograph's metadata might include information about the camera used to take the photo, the time and date the photo was taken, and the photo's precise geolocation. A written document's metadata may include details about its author, its creation date, and the number of times the document has been edited. Metadata can be used to verify content authenticity, helping to combat fake news by providing a traceable history of content creation and modification. But metadata can also contain personal information about the individual who creates or modifies a piece of content.

Watermarking. Watermarking is the process of embedding an identifiable marker into digital content. This "watermark" can be visible, such as a logo or text overlay, or it can be invisible, data embedded into a file in a manner that does not noticeably alter the content. As a technology, watermarking is in its infancy. Watermarks can be stripped from content relatively easily by common screenshotting tools, file compression software, and image editing programs like Photoshop. They can also be faked by treating a GenAI system like a copy machine: a real image or video can be fed into a GenAI system and spit back out, unaltered except for the addition of a watermark. The system's user receives a piece of authentic content that has been incorrectly marked as inauthentic, ready to be posted online to create confusion and sow discord. Furthermore, while progress has been made towards developing standards for watermarking images and video, how text should be watermarked is far less clear.

SB 942. Seeking to enact a comprehensive content provenance framework to combat the rapid online proliferation of AI-generated content, the Legislature passed SB 942 (Becker, Ch. 291, Stats. 2024). The resulting "AI Transparency Act" applies to "covered providers" – developers of publicly-accessible GenAI systems with over one million monthly users – requiring them to provide a free, publicly accessible tool that allows users to detect whether audio, image, or video content was generated or altered by their systems. The act permits visible disclosures and requires latent, machine-detectable provenance data to be embedded into content generated by these providers' GenAI systems, effectively requiring GenAI developers to disclose that content generated by their systems is "fake" beginning in mid-2026.

3) What this bill would do. SB 1000 would amend the AI Transparency Act in response to stakeholder concerns. Major changes include:

a. Expanding the bill to cover all GenAI systems, not only those that have over 1 million monthly visitors or users.

b. Removing the requirement for GenAI providers to allow users to include manifest disclosures in outputs.

c. Allowing GenAI providers to direct users to a third-party disclosure verification tool that meets specified requirements.

d. Clarifying the bill does not apply to "minor modifications" of content by GenAI systems, as defined.

e. Clarifying the bill's latent disclosure requirements apply only to the extent they are technically feasible.

f. Updating third-party licensing language to ensure compatibility with common licensing practices, specifying that GenAI providers only have to act on violations by identifiable licensees, reducing the response window from 96 hours to 72 hours, and clarifying that the bill's third-party licensing provisions do not require GenAI providers to monitor third party use.

Writing in support, TransparencyCoalition.ai explains the need for this measure:

> As AI technology advances, distinguishing between human and machine-generated content becomes increasingly challenging. This ambiguity poses significant societal and democratic risks, exacerbating problems such as disinformation, harassment, and fraud while threatening academic and journalistic integrity. At the same time, content provenance and disclosure technology is still in development, and researchers across both academia and industry are working to ensure methods of embedding information in content are scalable and capable of withstanding adversarial exploitation. It is therefore critical that provenance disclosure methods provide clear information to users to allow them to discern the trustworthiness and probable origin of content.

The bill contains an urgency clause allowing the AI Transparency Act to be updated immediately if the bill passes and the Governor signs it.

Accessibility Concerns. Disability Rights California has raised concerns about unintended consequences of the bill for individuals with disabilities. According to a June 9th letter to this Committee:

> [The] bill as currently drafted does not adequately account for situations in which generative AI is used as an assistive technology by individuals with disabilities, particularly those with disabilities that impact their ability to communicate verbally . . . For individuals with conditions such as ALS, cerebral palsy, or other communication-related disabilities, AI-driven voice tools function as a substitute for natural speech. These tools are used in everyday contexts, including communicating with service providers, participating in professional or public discourse, and engaging in personal interactions. Applying AI-generated content labeling requirements to these communications risks mischaracterizing human-authored speech as synthetic content and may inadvertently disclose a person's disability status.

Disability Rights California goes on to suggest exempting audio-based assistive technologies from the bill. Concerned that an outright exemption could enable bad actors to avoid disclosure

requirements, the author instead recently amended SB 1000 to require that latent disclosures specify "whether [a] GenAI system is designed to primarily function as assistive technology." Going forward, the author may wish to delay implementation of this requirement to give existing latent disclosure technologies time to adjust accordingly.

Video games. The AI Transparency Act includes the following exemption, meant to address concerns raised by the video game industry in response to SB 942:

> *"This chapter does not apply to any product, service, internet website, or application that provides exclusively non-user-generated video game, television, streaming, movie, or interactive experiences."*

An earlier version of SB 1000 would have modified the language of this exemption to more narrowly focus on video games incapable of outputting highly realistic content. Following further negotiations with industry and this committee, the author recently amended this bill such that it no longer changes the scope of this exemption.

ARGUMENTS IN SUPPORT:

Writing in support, the Center for AI and Digital Policy explains the need for this measure:

> SB 1000 is an appropriate expansion of the rights laid out in California' AI Transparency Act. Specifically, it removes the 1,000,000 user threshold from the definition of 'covered provider', expands the latent disclosure requirement to include whether content is generated or modified by AI, and replaces the 'AI detection tool' with a 'disclosure verification tool', shifting the obligation from passive detection to active and embedded disclosure. Taken together, these provisions establish meaningful protections for California consumers.

TechNet takes a "support if amended" position, writing the following:

> The recent amendments to SB 1000 represent a notable improvement, and we value the author's commitment to refining the legislation. Given the necessity of addressing outstanding concerns with SB 942 prior to its August 2, 2026, activation, these updates are vital. The present version successfully harmonizes consumer safety, security, and technological progress by prioritizing latent disclosures over unfeasible manifest labeling requirements.
>
> However, we maintain specific concerns regarding the bill as amended on June 9. Our feedback is intended to refine the legislation to ensure scalable compliance and avoid unintended consequences, rather than to oppose its primary goals. We recommend additional clarity on the following points:
>
> - We would like to see a clear exemption for business-to-business uses, because without it, covered providers that distribute or make available a generative artificial intelligence system to businesses or for business purposes face potential liability for content generated by downstream customers using their platforms—even though the provider has no knowledge of, control over, or intent regarding the specific content produced…

- Matching data minimization rules with practical tool functionality: The bill presently restricts the use of limited operational data needed to maintain and improve disclosure tools, relying too heavily on user feedback…

- Establishing direct compliance for third-party licensees: While we support uniform transparency protections, the bill currently places the burden of policing downstream compliance on model developers…

The California Initiative for Technology & Democracy takes a "support if amended" position, writing the following:

> SB 1000 makes several improvements to the AI Transparency Act. First, it expands the coverage of the law by ensuring that all creators of generative AI systems are responsible for maintaining a functioning system to embed latent disclosures, underscoring the foundational importance of attaching content provenance to all AI-generated content. Second, the bill clarifies the exceptions to the bill to eliminate vague terms, including the undefined "interactive experiences."
>
> […]
>
> While CITED applauds the improvements outlined above, we believe there are still continued refinements that deserve attention. For instance, the bill excludes the listing of "minor modifications" in provenance information, a term defined by a listing of editing techniques.
>
> […]
>
> Additionally, CITED objects to the elimination of the requirement for Gen AI Providers to provide users with the *option* to place manifest disclosures on the bill. Manifest disclosures remain the most accessible way a consumer can quickly discern the origins of digital content.

REGISTERED SUPPORT / OPPOSITION:

Support

Center for Ai and Digital Policy (CAIDP)
ForensicVB LLC
Transparency Coalition.ai

Opposition

None on file.

Analysis Prepared by: Slater Sharp / P. & C.P. / (916) 319-2200