CONCURRENCE IN SENATE AMENDMENTS
CSA1 Bill Id:AB 853¶Author:(Wicks)
As Amended Ver:September 5, 2025
Majority vote

SUMMARY

The bill requires large online platforms to develop a way for users to easily access provenance data of uploaded content. The bill would also require capture device manufacturers to include features on their products that enable users to include provenance data in the content that they capture. These requirements, coupled with SB 942, would create a comprehensive disclosure and detection framework that would enable the large-scale classification of content as either authentic or artificial.

Senate Amendments
Delayed implementation of the requirements for capture device manufacturers until Jan. 1, 2028 and for large online platforms until Jan. 1, 2027.

Delayed implementation of existing statute until Aug. 2, 2026 to align with the AI EU Act.

Narrowed the definition of "large online platforms" to exempt broadband internet access or telecommunications services, and advertising networks.

Refined the obligations placed on large online platforms to include that provenance data detected on their platforms must align with widely adopted specifications, the type of information that must be accessible to users of such platforms, and a prohibition, to the extent feasible, on platforms stripping content of provenance data.

Makes various other technical changes.

COMMENTS

1*) Ctrl+Alt+Deceive: 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. The creation of text, 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 invade privacy and disrupt the lives of Californians. Since its inception, GenAI has been used to create nonconsensual pornography, more accurately referred to by sexual assault experts as image-based sexual abuse, almost entirely against women and girls.

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 abuses, almost always against girls, have been reported across the country and show no sign of abating.[4] In the first six months of 2024, these 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] This provides a potent means of amplifying deepfake nonconsensual pornography, extending the content's reach by, in effect, and crowdsourcing abuse, potentially reaching thousands or even millions of viewers.

2) *What this bill would do.* The challenge of content authentication could theoretically be solved with three steps:

---

[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.

1. Require that all GenAI-derived content be labeled as "fake."

2. Require all content produced by recording devices be labeled as "real."

3. Require social media platforms to clearly present these labels.

Last year, SB 942 (Becker) was chaptered to address concerns around labeling GenAI-produced content as "fake." The bill requires developers of GenAI systems with over one million users to embed latent disclosures within content generated using their systems. Additionally, those developers must provide a publicly accessible and free AI detection tool capable of identifying the embedded disclosures. While SB 942 is prescriptive regarding the type of provenance data that must be detectable by such tools, it allows the industry to establish best practices for ensuring GenAI-produced content can be reliably identified.

This bill would require manufacturers of capture devices, such as cameras, smartphones with cameras, scanners, audio recorders, and other devices capable of storing and transferring digital media, to provide users with the ability to embed provenance data in the content they capture. This approach offers a particularly effective means of content authentication. Unlike GenAI tools, which can produce limitless amounts of synthetic content and are increasingly accessible due to open-source code, capture devices are produced by a limited number of manufacturers. By focusing compliance efforts on these manufacturers, enforcement becomes more feasible. Additionally, the volume of content generated by capture devices is significantly lower than that produced by GenAI systems, further increasing the likelihood that captured content can be reliably authenticated.

This bill would also require large online platforms, such as Instagram and X, to provide users with a readily accessible method for inspecting the provenance data of content shared on their platforms. Given that most individuals engage with digital content through these platforms, it is both practical and impactful to place a duty on them to help users determine the authenticity of the content they encounter. Under current law, the responsibility falls on the viewer to seek out and use AI detection tools to verify content. This bill would shift that burden, establishing a more uniform and accessible framework for identifying content provenance directly within the platforms themselves.

For a full analysis of the issues that this bill is addressing, please see the policy committee analyses.

According to the Author

> New and emerging developments of generative AI (GenAI) tools have made it easier to create, edit, and doctor images, video, and audio. GenAI technologies can create and manipulate content to look realistic and convincing, which allow bad actors to create harmful content and spread disinformation.
>
> AB 853 will help provide more transparency of AI-generated content in the digital information ecosystem and would provide more information to understand the source of content and discern what is real and what is inauthentic. This bill will help mitigate some of the harmful impacts of AI-generated content.

Arguments in Support
California Initiative for Technology & Democracy (CITED) a sponsor of the bill, write in support:

> Last year, the California Legislature passed SB 942, the AI Transparency Act, which created the first-in-the-nation rules requiring generative AI providers to implement content provenance for AI-generated content. When this law takes effect in 2026, the public will be able to use AI detection tools to identify the source of AI-generated content. SB 942 represents an important foundation in our effort to rebuild trust in our information ecosystem.
>
> But more must be done to stem the tide of mis- and dis-information in the age of AI. AB 853 builds upon the framework of the AI Transparency Act by adding several critical interventions, first at the point of content creation and then at the point of dissemination.
>
> At the point of content creation, AB 853 would enable human-created authentic content to be differentiated from AI-generated synthetic content by requiring cameras and recording devices sold in California to include an option to place provenance information on the content that the device produces. This provenance information, together with existing provenance requirements for generative AI under the AI Transparency Act, would allow the public to easily differentiate between human vs. AI-generated content.
>
> Thereafter, at the point of content dissemination, AB 853 would require social media and other online platforms to display the source of the content shared on their platforms by leveraging the underlying provenance data. By requiring clear, factual labeling of the source of online content, AB 853 would equip the public with a tool to make their own judgment about what information they deem to be trustworthy.
>
> With the rapid proliferation of GenAI tools, the public must be equipped with the necessary tools to distinguish the content we see online in order to restore trust in our democracy and our society. For these reasons, CITED is proud to sponsor and support AB 853.

Arguments in Opposition
Technet and the Computers and Communications Industry Association argue:

> Industry-led standards are still being developed by organizations like the Coalition for Content Provenance and Authenticity (C2PA). Locking in rigid mandates at this stage risks undermining those collaborative efforts. Additionally, SB 942, enacted last year, has not yet taken effect. That law already established a framework for synthetic media transparency. Imposing additional prescriptive requirements for watermarking and provenance technology before SB 942 is implemented is premature.
>
> AB 853 requires every new capture device manufactured after 2028 to embed provenance data by default, with opt-out functionality. While the bill now references feasibility and standards-setting bodies, these requirements remain commercially impractical, especially in B2B markets where use cases are distinct from consumer needs. The result could be higher costs for manufacturers and consumers, with little demonstrated benefit.
>
> Recent amendments create new obligations leading to significant compliance burdens The September 5 amendments impose new obligations on "large online platforms" and GenAI hosting platforms, including requirements around latent disclosures that were covered by SB

942. While we support transparency, these provisions are overly broad, lack clarity, and raise serious compliance questions. Furthermore, the bill fails to address how liability attaches when content is modified downstream and could hinder innovation without significantly improving consumer understanding.

AB 853 still doesn't address whether platforms are responsible for third-party or embedded content. This ambiguity poses significant compliance risks and will be particularly challenging

FISCAL COMMENTS

According to the Senate Appropriations Committee:

1) The Department of Justice (DOJ) reports a fiscal impact of approximately $1 million or less (Unfair Competition Law Fund). DOJ notes that implementation of this bill will be dependent upon the appropriation of funds. The DOJ will be unable to absorb the costs to comply with or implement the requirements of the bill within existing budgeted resources. DOJ reports that the Consumer Protection Section (CPS) within the Public Rights Division anticipates increased workloads in investigating and enforcing violations of this bill, beginning on January 1, 2026, and ongoing. CPS will require additional resources consisting of two Deputy Attorneys General (DAGs), one Associate Governmental Program Analyst (AGPA), and one Legal Secretary.

2) Unknown, potentially significant costs to the state funded trial court system (Trial Court Trust Fund, General Fund) to adjudicate civil actions. By expanding a civil penalty with statutory damages, this bill may lead to additional case filings that otherwise would not have been commenced. Expanding civil penalties could lead to lengthier and more complex court proceedings with attendant workload and resource costs to the court. The fiscal impact of this bill to the courts will depend on many unknowns, including the number of cases filed and the factors unique to each case. An eight-hour court day costs approximately $10,500 in staff in workload. While the courts are not funded on a workload basis, an increase in workload could result in delayed court services and would put pressure on the General Fund to fund additional staff and resources and to increase the amount appropriated to backfill for trial court operations.

VOTES:

ASM PRIVACY AND CONSUMER PROTECTION: 11-1-3
YES: Bauer-Kahan, Bryan, Irwin, Lowenthal, McKinnor, Ortega, Pellerin, Petrie-Norris, Ward, Wicks, Wilson
NO: DeMaio
ABS, ABST OR NV: Dixon, Macedo, Patterson

ASM JUDICIARY: 9-0-3
YES: Kalra, Bauer-Kahan, Bryan, Connolly, Harabedian, Pacheco, Papan, Stefani, Zbur
ABS, ABST OR NV: Dixon, Macedo, Sanchez

ASM APPROPRIATIONS: 11-0-4
YES: Wicks, Arambula, Calderon, Caloza, Elhawary, Fong, Mark González, Hart, Pacheco, Pellerin, Solache

ABS, ABST OR NV: Sanchez, Dixon, Ta, Tangipa

ASSEMBLY FLOOR: 58-2-19
YES: Addis, Aguiar-Curry, Ahrens, Alvarez, Arambula, Ávila Farías, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Calderon, Caloza, Carrillo, Connolly, Elhawary, Fong, Gabriel, Garcia, Gipson, Mark González, Haney, Harabedian, Hart, Irwin, Jackson, Kalra, Krell, Lee, Lowenthal, McKinnor, Muratsuchi, Nguyen, Ortega, Pacheco, Papan, Patel, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Ransom, Celeste Rodriguez, Michelle Rodriguez, Rogers, Blanca Rubio, Schiavo, Schultz, Sharp-Collins, Solache, Soria, Stefani, Ward, Wicks, Wilson, Zbur, Rivas
NO: DeMaio, Patterson
ABS, ABST OR NV: Alanis, Bains, Castillo, Chen, Davies, Dixon, Ellis, Flora, Gallagher, Jeff Gonzalez, Hadwick, Hoover, Lackey, Macedo, Sanchez, Ta, Tangipa, Valencia, Wallis

UPDATED

VERSION: September 5, 2025

CONSULTANT: John Bennett / P. & C.P. / (916) 319-2200 FN: 0002079