SENATE THIRD READING
SB 1216 (Gonzalez)
As Amended August 15, 2022
Majority vote

SUMMARY

This bill, upon appropriation by the Legislature, requires the Secretary of the Government Operations Agency (GovOps) to evaluate specified implications of the proliferation of deepfakes and digital content forgery technologies, as defined, for California's government agencies, businesses, and residents; and requires the Secretary of GovOps to report specified findings and recommendations to the Legislature by October 1, 2024. This bill is sponsored by Adobe, Inc.

Major Provisions

1) Requires the Secretary of GovOps, upon appropriation by the Legislature, for purposes of developing a coordinated plan as described in 2), below, to evaluate all of the following: a) the impact of proliferation of deepfakes on state government, California-based businesses, and residents of the state; b) the risks, including privacy risks, associated with the deployment of digital content forgery technologies and deepfakes on state and local government, California based-businesses, and residents of the state; c) potential privacy impacts of technologies allowing public verification of digital content provenance; d) the impact of digital content forgery technologies and deepfakes on civic engagement, including voters; e) the legal implications associated with the use of digital content forgery technologies and deepfakes, and technologies allowing public verification of digital content provenance; and f) the best practices for preventing digital content forgery and deepfake technology to benefit the state, California-based businesses, and California residents, including whether and how the adoption of a digital content provenance standard could assist with reducing the proliferation of digital content forgeries and deepfakes.

2) Requires the Secretary of GovOps to develop a coordinated plan to accomplish all of the following: a) investigate the feasibility of, and obstacles to, developing standards and technologies for state departments for determining digital content provenance; b) increase the ability of internet companies, journalists, watchdog organizations, other relevant entities, and members of the public to meaningfully scrutinize and identify digital content forgeries and relay trust and information about digital content provenance to content consumers; c) develop or identify mechanisms for content creators to cryptographically certify authenticity of original media and non-deceptive manipulations; and d) develop or identify mechanisms for content creators to enable the public to validate the authenticity of original media and non-deceptive manipulations to establish content provenance without materially compromising personal privacy or civil liberties.

3) Requires the Secretary of GovOps to report to the Legislature on the potential uses and risks of deepfake technology to the state government and California-based businesses on or before October 1, 2024; and requires the report to include the coordinated plan required by 2), above, including recommendations for modifications to the definition of digital content forgery and deepfakes.

COMMENTS

As AI and ML have become increasingly sophisticated, the capacity to manipulate audiovisual media to create realistic representations of fabricated events has grown exponentially. These so-called "deepfakes" can be harmless or even entertaining, but can also have serious social costs if used toward nefarious ends. Though the ability to manipulate digital media has been present since at least the 1990s, the realism made possible by these AI/ML-driven techniques, along with the ability to synthesize realistic media to represent nearly any occurrence, make these recent developments particularly insidious. In support of this bill, the Anti-Defamation League (ADL) explains:

> Deepfakes are an emerging technology that [] combines multiple real images/videos/audio with machine learning technology to create a new, synthetic piece of media (e.g. image, audio or video). This technique has been used to create machine-made media of all kinds, including some with the intention of deceiving audiences. Some examples of deceptive deepfakes include videos of politicians depicted in situations that never happened or fabricated pornographic videos targeting specific individuals. Audio deepfakes could lead to serious forms of fraud and identity theft.
>
> The proliferation of deepfakes and misinformation continue to increase at an alarming rate, and the public policy solutions needed to protect California residents, businesses, and government institutions remain unclear. Policy solutions continue to allude [*sic.*] policy makers across the globe.

Echoing the concerns raised by ADL, a recent report published by the United States Department of Homeland Security outlines several scenarios in which the use of deepfakes could be extremely dangerous, including: inciting violence; producing false evidence undermining scientific consensuses such as climate change and vaccine efficacy; falsifying evidence in a criminal case; corporate sabotage; social engineering attacks targeting corporate and financial institutions; stock manipulation; and cyberbullying.[1]

Since 2019, this Legislature has demonstrated recognition of the risks inherent to deepfake technology. Specifically, by passing AB 730 (Berman), Chapter 493, Statutes of 2019, and AB 602 (Berman), Chapter 491, Statutes of 2019), respectively, California has taken decisive action to address the sensitive circumstances in which deepfakes can be weaponized to influence political outcomes in elections or to manufacture explicit content that could harm the reputation of those falsely depicted.

Still, regulating the use of deepfakes in all but the most egregious of circumstances is extraordinarily complex. Doing so requires technical literacy with respect to the technology itself, a sociocultural understanding of the media environment in which both problematic and legitimate uses may arise, and an in-depth understanding of the legal constraints surrounding such regulation, including potential impositions on First Amendment rights related to free expression.

[1] Department of Homeland Security, "Increasing Threats of Deepfake Identities", https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf [as of Jun. 12, 2022].

Recognizing this complexity, SB 1216 seeks to provide the Legislature with recommendations from the Secretary of GovOps spanning various facets of the issues arising from deepfakes. Doing so has the potential to better inform future policy in order to effectively balance the myriad considerations thoughtful policymaking in this space must address.

In 2018, this Legislature passed, and the Governor signed into law, AB 2658 (Calderon, Ch**.** 875, Stats. 2018), which tasked the Secretary of GovOps with appointing a Blockchain Working Group to evaluate several facets of blockchain technology, including: uses of blockchain in state government and business; risks, including privacy risks, associated with the use of blockchain; benefits associated with the use of blockchain; legal implications associated with the use of blockchain; and best practices for enabling blockchain technology to benefit the state of California. AB 2658 also required the Blockchain Working Group to report to the Legislature on its findings, and on July 1, 2020, the Blockchain Working Group submitted its report, recommendations from which have generated several Legislative proposals in the years since. This bill is modelled after AB 2658, mirroring its structure and repurposing several of its provisions nearly verbatim.

Rather than proposing the establishment of a Deepfake Working Group to carry out the required evaluation and reporting, however, the bill has been amended to instead require similar evaluation and reporting to be conducted independently by the Secretary of GovOps, in an effort to reduce anticipated costs. As it is currently in print, this bill would task the Secretary of GovOps with exploring certain impacts and implications of the proliferation of digital content forgery technologies, as defined, and deepfakes, as defined, including: impacts on state government, California-based businesses, and residents of the state; risks, including privacy risks, associated with the deployment of digital content forgery technologies and deepfakes; potential privacy impacts of technologies allowing public verification of digital content provenance; impacts of digital content forgery technologies and deepfakes on civic engagement, including voters; legal implications associated with the use of digital content forgery technologies, deepfakes, and technologies allowing public verification of digital content provenance; and best practices for preventing digital content forgery and deepfake technology, including whether and how the adoption of a digital content provenance standard could assist with reducing the proliferation of digital content forgeries and deepfakes.

The bill in print would also define the term "digital content forgery" to mean the use of technologies, including AI and ML techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead; would define the term "digital content provenance" to mean the verifiable chronology of the original piece of digital content, such as an image, video, audio recording, or electronic document; and would define the term "deepfake" to mean audio or visual content that has been generated or manipulated by AI which would falsely appear to be authentic or truthful and which features depictions of people appearing to say or do things they did not say or do without their consent.

This bill would further require the Secretary of GovOps to develop a coordinated plan to accomplish several goals, including: investigating the feasibility of, and obstacles to, developing standards and technologies for state departments for determining digital content provenance; increasing the ability of various entities, including members of the public, to meaningfully scrutinize and identify digital content forgeries, and to relay trust and information about digital content provenance to content consumers; developing or identifying mechanisms for content creators to cryptographically certify authenticity of original media and non-deceptive manipulations; and developing or identifying mechanisms for content creators to enable the public to validate the authenticity of original media and non-deceptive manipulations to establish content provenance without material compromising personal privacy or civil liberties. Finally, the bill in print would require the Secretary of GovOps to report to the Legislature on or before October 1, 2024 regarding potential uses and risks of deepfake technology to the state government and California-based businesses, including the required coordinated plan, and recommendations for modifications to the definition of digital content forgery and deepfakes.

According to the Author

> Deepfakes are deceptive life-like videos and recordings that can effectively make it appear as though an individual said or did something that never actually took place. This type of manufactured media can have entertaining and innocent uses such as viral TikToks; or nefarious uses like the dissemination of forged sexually explicit material, or videos of influential political leaders that incite political violence. The potential of these digital forgeries is far reaching and will have implications for national security, influence on elections, and even how journalists and media sources verify the provenance of videos before they report them as factual news.
>
> This new frontier of technology has created a number of ethical, legal, and policy questions that are not easily answered and creates numerous complex implications for privacy rights, governmental communication, media accuracy, copyright infringement, and many other legal repercussions that can't be easily addressed without thoughtful dialogue amongst informed stakeholders. This bill will allow for the exploration and examination of best practices being used to reduce digital content forgeries, help in identifying mechanisms to certify the authenticity of original content, and evaluate the impact of deepfakes throughout the state.

Arguments in Support

Adobe, Inc., who sponsor this bill, argue:

> SB 1216 [] represents an important step toward increasing public and private sector collaboration in combatting the unique threat that digital content forgeries and misinformation campaigns pose to our state and our democracy. As studies have shown, we will continue to consume content digitally and we must find ways to protect against the dangers of falsely manipulated digital content. There could be 100 times more visual content by 2027, according to one study. One expert [] estimates that synthetic video may account for as much as 90% of online video in just three to five years. […] We are encouraged to see this bill recognize the need to evaluate risks, privacy impacts, and legal implications of the proliferation of deepfakes, and to develop a coordinated plan to […] address these threats. Furthermore, the bill provides a unique opportunity for the state of California to take the lead in addressing the impact of misinformation on consumers and to explore the development and deployment of a "digital content provenance" open standard to counter the spread of deepfakes and misinformation.

Arguments in Opposition

None on file.

FISCAL COMMENTS

According to the Assembly Appropriations Committee, "[c]osts (General Fund) possibly in the hundreds of thousands of dollars ongoing to the Government Operations Agency (GovOps) in additional staff and infrastructure to study the risks of deepfakes."

VOTES

SENATE FLOOR: 39-0-1
YES: Allen, Archuleta, Atkins, Bates, Becker, Borgeas, Bradford, Caballero, Cortese, Dahle, Dodd, Durazo, Eggman, Glazer, Gonzalez, Grove, Hueso, Hurtado, Jones, Kamlager, Laird, Leyva, Limón, McGuire, Melendez, Min, Newman, Nielsen, Ochoa Bogh, Pan, Portantino, Roth, Rubio, Skinner, Stern, Umberg, Wieckowski, Wiener, Wilk
ABS, ABST OR NV: Hertzberg

ASM PRIVACY AND CONSUMER PROTECTION: 9-0-2
YES: Gabriel, Bauer-Kahan, Berman, Choi, Cunningham, Mike Fong, Irwin, Valladares, Wilson
ABS, ABST OR NV: Bennett, Wicks

ASM ACCOUNTABILITY AND ADMINISTRATIVE REVIEW: 7-0-0
YES: Petrie-Norris, Patterson, Gray, Lackey, Medina, Rodriguez, Wilson

ASM APPROPRIATIONS: 12-0-4
YES: Holden, Bryan, Calderon, Arambula, Mike Fong, Gabriel, Eduardo Garcia, Levine, Quirk, Robert Rivas, Akilah Weber, McCarty
ABS, ABST OR NV: Bigelow, Megan Dahle, Davies, Fong

UPDATED

VERSION: August 15, 2022

CONSULTANT: Landon Klein / P. & C.P. / (916) 319-2200 FN: 0003382