**SENATE JUDICIARY COMMITTEE**
**Senator Thomas Umberg, Chair**
**2021-2022 Regular Session**

SB 1216 (Gonzalez)
Version: February 17, 2022
Hearing Date: April 19, 2022
Fiscal: Yes
Urgency: No
CK

## SUBJECT

Secretary of the Government Operations Agency: working group: deepfakes

## DIGEST

This bill requires the Secretary of the Government Operations Agency to establish the Deepfake Working Group to evaluate the impacts and risks associated with digital content forgery.

## EXECUTIVE SUMMARY

Certain forms of media – audio recordings, video recordings, and still images – can be powerful evidence of the truth. While such media have always been susceptible to some degree of manipulation, until recently, fakes were relatively easy to detect. Advancing technology is making it cheaper and easier to produce so-called "deepfakes": audio, images, and, in particular, video recordings that are not real, but that are so realistic that they are virtually impossible to distinguish from a genuine recording.

This bill requires the Secretary of the Government Operations Agency to establish the Deepfake Working Group to evaluate the impacts and risks associated with digital content forgery. Participants of the group are to be drawn from a variety of fields and represent various interests. The working group will be tasked with developing a coordinated plan to attain its specified goals with the ultimate product being a report for the Legislature on the potential uses and risks of deepfake technology to the state government and California-based businesses.

This bill is sponsored by Adobe, Inc. It is supported by various groups, including the Anti-Defamation League. There is no known opposition. This bill passed out of the Senate Governmental Organization Committee on a 14 to 0 vote.

## PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the Government Operations Agency within the state government to be governed by the Secretary of Government Operations. (Gov't Code §§ 12800, 12803.2.)

2) Authorizes a depicted individual to bring a cause of action against a person who does either of the following:
    a) creates and intentionally discloses sexually explicit material and the person knows or reasonably should have known the depicted individual in that material did not consent to its creation or disclosure; or
    b) intentionally discloses sexually explicit material that the person did not create and the person knows the depicted individual in that material did not consent to the creation of the sexually explicit material. (Civ. Code § 1708.86.)

3) Defines, for the preceding statute, "depicted individual" as an individual who appears, as a result of digitization, to be giving a performance they did not actually perform or to be performing in an altered depiction. (Civ. Code § 1708.86.)

4) Prohibits, until January 1, 2023, a person, committee, or other entity from distributing, within 60 days of an election at which a candidate for elective office will appear on the ballot, with actual malice, materially deceptive audio or visual media of the candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate. (Elec. Code § 20010.)

This bill:

1) Requires the Secretary of the Government Operations Agency, upon appropriation by the Legislature, to establish the Deepfake Working Group to evaluate all of the following:
    a) the impact of the 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) the impact of digital content forgery technologies and deepfakes on civic engagement, including voters;
    d) the legal implications associated with the use of digital content forgery technologies and deepfakes; and

e) the best practices for preventing digital content forgery and deepfake technology to benefit the state, California-based businesses, and California residents.

2) Provides that the group shall consist of 20 participants from specified fields and organizations, including appointees from the technology industry and representatives of privacy and consumer organizations.

3) Requires the working group to take input from a broad range of stakeholders with a diverse range of interests affected by state policies governing emerging technologies, privacy, business, the courts, the legal community, and state government.

4) Requires the group to develop a plan of action and to report to the Legislature on or before July 1, 2024.

5) Provides that it shall only remain in effect until January 1, 2025.

## COMMENTS

1. Combating deepfakes

This bill aims to address the growing concerns associated with what are called "deepfakes," a term drawn from "deep learning" plus "fake." There are various manifestations, but essentially all involve the digital manipulation of audiovisual material to falsely depict an individual engaging in certain conduct. This technology has advanced rapidly in recent years thanks to the use of artificial intelligence to help train the software. Software applications that enable a user to make deepfake videos are now available for easy download. Among the more common apps are TikTok, Snapchat, Wombo, FaceApp, and Zao. Many social media platforms, including Twitter, have committed to combatting the rise of deepfakes with policies aimed at restricting the posting of misleading deepfake content on their platforms.

The Department of Homeland Security issued a report on the increasing threat of deepfakes.[1] It detailed the various scenarios in which this technology can be used nefariously, including:

- inciting violence;
- producing false evidence about climate change;
- falsifying evidence in a criminal case;

[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. All Internet citations are current as of March 27, 2022.

- corporate sabotage;
- corporate and financial institution social engineering attacks;
- stock manipulation; and
- cyberbullying.

In the context of election campaigns, deepfake technology can be weaponized to distort voters' perception of the truth since deepfakes can be used to deceive people into thinking that a candidate said or did something which the candidate did not. Various incidents, as reported in the media, have highlighted the dangers of the technology in this arena:

- In 2019, a video of U.S. House of Representatives Speaker Nancy Pelosi, sounding and appearing drunk while giving a speech, began circulating on the Internet. Users of Twitter, Facebook and YouTube, among other online platforms shared the video widely. One site recorded that over two million of its users had watched the video. Subsequent investigation revealed that the video had been slowed down to create the appearance that Pelosi was intoxicated at the time. Shown at full speed, the video left no such impression.[2]

- In 2018, suspicions that a video of Gabon's president was a deepfake led members of that nation's military to stage a coup attempt. Before the video came out, Gabonese President Ali Bongo had not been seen in public for months. He was rumored to be in poor health or perhaps already dead.[3]

The problem is particularly serious and widespread in the context of sexual explicit material: "Although political deepfakes are relatively new, pornographic deepfakes have been a problem for some time. These often purport to show a famous actress or model involved in a sex act but actually show the subject's face superimposed onto another woman's body."[4] Given the explicit content of some deepfakes, the consequences can be serious.

> These nonconsensual depictions are not a victimless crime. They cause real harm. Even if it is not really [their] body, an actor depicted as participating in a sex scene may find it difficult to get cast in more family-

---

[2] Drew Harwell, *Faked Pelosi Videos, Slowed to Make Her Appear Drunk, Spread Across Social Media* (May 24, 2019) The Washington Post https://www.washingtonpost.com/technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/?noredirect=on&utm_term=.f6bc368f1590.

[3] Drew Harwell, *Top AI Researchers Race to Detect 'Deepfake' Videos: 'We are Outgunned'* (Jun. 12, 2019) The Washington Post https://www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/?utm_term=.aeb7558380a9.

[4] Nicholas Schmidt, *Privacy law and resolving 'deepfakes' online* (Jan. 30, 2019) IAPP, https://iapp.org/news/a/privacy-law-and-resolving-deepfakes-online/.

> friendly productions. Moreover, [the actor] may endure considerable emotional trauma as a result of being exploited in this horrific way.[5]

The rapid evolution of the underlying technology has only exacerbated these problems:

> Recent improvements in artificial intelligence software have made it surprisingly easy to graft the heads of stars, and ordinary women, to the bodies of X-rated actresses to create realistic videos.
>
> These explicit movies are just one strain of so-called "deepfakes," which are clips that have been doctored so well they look real. Their arrival poses a threat to democracy; mischief makers can, and already have, used them to spread fake news. But another great danger of deepfakes is their use as a tool to harass and humiliate women.[6]

The Legislature has taken action to try and combat this scourge. In the election context, AB 730 (Berman, Ch. 493, Stats. 2019) prohibits a person, committee, or other entity from distributing with actual malice materially deceptive audio or visual media of a candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate within 60 days of an election at which a candidate for elective office will appear on the ballot, as specified and unless certain conditions are met.

AB 602 (Berman, Ch. 491, Stats. 2019) addressed the problem with sexual explicit deepfakes. It provides that a "depicted individual," or an individual who appears, as a result of digitization, to be giving a performance they did not actually perform or to be performing in an altered depiction, has a cause of action against a person who does either of the following:

- creates and intentionally discloses sexually explicit material and the person knows or reasonably should have known the depicted individual in that material did not consent to its creation or disclosure; or
- intentionally discloses sexually explicit material that the person did not create, and the person knows the depicted individual in that material did not consent to the creation of the sexually explicit material.

2. <u>Evaluating the best path forward on deepfakes</u>

This bill aims to address the problem by requiring the creation of a Deepfake Working Group. The group is tasked with evaluating the risks and impacts of this technology.

---

[5] David White, *Deepfake Technology Is an Attack on Consent and Actors' Rights to Control Sex Scenes* (Feb. 21, 2019) The Wrap, https://www.thewrap.com/deepfake-tech-consent-actors-rights-sex-scenes/.
[6] Jeff John Roberts, *Fake Porn Videos Are Terrorizing Women. Do We Need a Law to Stop Them?* (Jan. 15, 2019) Fortune, http://fortune.com/2019/01/15/deepfakes-law/.

Specifically, it will assess the impact of the proliferation of deepfakes, or "digital content forgery," on state government, California-based businesses, residents of the state, and civic engagement. This will include evaluating the grave risks, including on privacy interests, that are associated with these technologies. The groups will look at the legal implications associated with the use of digital content forgery technologies and deepfakes and evaluate best practices.

The group will be made up of a wide variety of participants and will take input from a broad range of stakeholders with a diverse range of interests affected by state policies governing emerging technologies, privacy, business, the courts, the legal community, and state government.

The Deepfake Working Group is required to report to the Legislature, on or before July 1, 2024, on the potential uses and risks of deepfake technology to the state government and California-based businesses. This must include recommendations for modifications to the definition of digital content forgery and deepfakes and recommendations for amendments to other code sections that may be impacted by the deployment of digital content forgery technologies and deepfakes.

According to the author:

> Deepfakes are a type of digital content forgery that use new and emerging technologies like artificial intelligence to create or manipulate audio and video content with the intent to mislead the viewer. These digital forgeries will likely have implications on national security, First Amendment rights, national elections, and even how journalists and media sources verify the provenance or authenticity of a photo or video. This new frontier of technology has created a number of ethical, legal, and policy questions that are not easily answered, and will continue to present complex societal and governmental questions about privacy rights, media accuracy, copyright infringement, and numerous other legal and moral issues that can't easily be addressed without thoughtful dialogue amongst informed stakeholders.
>
> SB 1216 takes the first step in addressing these complex issues by creating the Deepfake Working Group under the GovOps Agency and tasks its members to research, discuss, study, and report on these novel issues and how California can confront them in real time. The working group will evaluate risks, privacy impacts, and legal implications of the proliferation of deepfakes and will develop a coordinated plan to utilize the public, industry, and government to jointly address these threats.

3. Support for the bill

The Anti-Defamation League writes in support:

> 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 policy makers across the globe. SB 1216 is a foundational first step to address the growing threat of deepfakes, by bringing together key experts and stakeholders to study this emerging issue and to develop potential solutions to protect all Californians.
>
> We understand the need for the Deepfake Working Group to evaluate risks, privacy impacts, legal implications of the proliferation of deepfakes, and develop a coordinated plan to address these threats. It is critical that the Working Group include representatives with online hate and harassment expertise.

Adobe, the sponsor of this bill, writes:

> The digitalization of our world has enabled people to connect, create, and communicate like never before. In some cases, it has also made it more difficult for people to discern fact from fiction. Solutions that empower people to make more informed decisions about the content they are seeing online are critical to helping stop the spread of misinformation.

Writing in support, the Silicon Valley Leadership Group states:

> The recent proliferation of deepfakes has harmed the public's ability to discern fact from disinformation. This legislation would wisely bring together a diverse group of experts that represent privacy organizations, consumer advocacy associations, the tech industry, non-tech industry stakeholders, state agency representatives and legal experts to work with the Judicial Council.
>
> The creation of a Deepfake Working Group is a needed step for California to bring together subject matter experts that will combine their perspectives to address the challenges of deepfakes. We support the duties assigned to the Working Group that would include a report to the Legislature and a coordinated plan to reduce the proliferation and impact of deepfakes.

## SUPPORT

Adobe Inc. (sponsor)
Anti-Defamation League
BSA The Software Alliance
California Medical Association
Silicon Valley Leadership Group

## OPPOSITION

None known

## RELATED LEGISLATION

Pending Legislation: AB 972 (Berman, 2022) extends the existing sunset on the provisions implemented by AB 730 to January 1, 2027. This bill is currently pending referral in the Senate.

Prior Legislation:

AB 613 (Christina Garcia, 2021) would have required a social media platform or a user or advertiser to place a tag on a retouched image that has been posted on the social media platform for promotional or commercial purposes. This bill died in the Assembly Privacy and Consumer Protection Committee.

AB 602 (Berman, Ch. 491, Stats. 2019) *See* Comment 1.

AB 730 (Berman, Ch. 493, Stats. 2019) *See* Comment 1.

AB 1280 (Grayson, 2019) would have criminally prohibited a person from preparing, producing, or developing, without the depicted individual's consent, a deepfake that depicts an individual engaging in sexual conduct, under specified circumstances involving the distribution, exhibition, or exchange of the deepfake. A "deepfake" would have been defined as a recording that has been created or altered in a manner that it would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of the individual depicted in the recording. This bill failed passage in the Assembly Public Safety Committee.

## PRIOR VOTES:

Senate Governmental Organization Committee (Ayes 14, Noes 0)

**********