WILMERHALE

Deepfake Legislation: A Nationwide Survey—State and Federal Lawmakers Consider Legislation to Regulate Manipulated Media

SEPTEMBER 25, 2019

By Matthew F. Ferraro

Federal and state lawmakers across the nation are considering legislation to address what they see as the rising dangers of "deepfakes." Deepfakes are false yet highly realistic artificial intelligence (AI)-created video, audio and text. A sophisticated deepfake video can show people saying things they never said and doing things they never did.

About a dozen bills have been introduced in the US Congress and state legislatures in the past year that address deepfakes in one form or another. Two bills have already become criminal law—one in Virginia, criminalizing nonconsensual deepfake pornography, and one in Texas, criminalizing deepfakes that interfere with elections. Two other bills passed by the California legislature in September 2019 await the Governor's signature. They would allow victims of nonconsensual deepfake pornography to sue for damages and give candidates for public office the ability to sue individuals or organizations that create or share election-related deepfakes without warning labels near Election Day.

The proposed and enacted laws share several common characteristics.

1. **Research and Reports**. Six bills pending before the US Congress would require federal agencies to brief lawmakers or write reports on the current state of deepfake technology, deepfake countermeasures, and any changes needed to laws and regulations to respond to the threats posed by such manipulated media (*see* H.R. 2500, H.R. 3600/S. 2065; H.R. 3494; S. 1348.; *see also* H.R. 4355 (requiring a report on research opportunities with the private sector on deepfakes and any policy recommendations that could improve private-public

communication on deepfake-detection technologies); H.R. 3230 (requiring annual reports in addition to imposing new criminal penalties on certain deepfakes)).

2. **Nonconsensual Deepfake Pornography**. One state (Virginia, Va. Code Ann. § 18.2-386.2) has adopted a law, and Congress and a few other states are considering others, to ban the use of deepfake technology to produce or distribute nonconsensual pornography (*see* H.R. 3230; Calif. AB-1280; Calif. AB-602; N.Y. A08155, S0587-B).

3. **Elections**. Texas has adopted a measure outlawing the creation or distribution of deepfake videos of candidates for public office intended to injure the candidate or influence elections (Tex. SB 751). California (Calif. AB-730; Calif. AB-1280) and the US Congress (H.R. 3230) are considering similar bills.

4. **Specific Intent**. Almost without exception, the pending or enacted deepfake-related bills require that, to be liable, a defendant must "intend" for the deepfake he or she produces or distributes to cause a particular result or harm. For example, two bills imposing penalties for nonconsensual deepfake pornography require the defendant to intend to "humiliate or otherwise harass" the victim of the deepfake (*see* H.R. 3230; *see also* Va. Code Ann. § 18.2-386.2; *but see* Calif. AB-602 (not requiring as an element of the offense the intent to humiliate or harass the victim but requiring the intent to create or disclose sexually explicit material that the defendant knew or should have known depicted a nonconsenting individual)). Likewise, laws prohibiting deepfakes that target elections require a perpetrator to create or distribute a deepfake with the "intent to injure a candidate or influence the result of an election" (Tex. SB 751; *see* H.R. 3230; Calif. AB-1280; *see also* Calif. AB-730 (requiring in addition to specific intent a showing of "actual malice")). Including specific-intent requirements may help these bills withstand challenges that they restrict free speech rights.

5. **Private Rights of Action**. Several pending bills would establish a private right of action for those who are victimized by deepfakes, empowering plaintiffs to sue creators and distributors for damages (*see* H.R. 3230; Calif. AB-602; Calif. AB-730).

6. **Liability Shield for Internet Service Providers**. At least one deepfake law (Va. Code Ann. § 18.2-386.2) specifically exempts from liability internet service providers that enable computer access to individuals who create or distribute deepfakes that violate the prohibitions. Internet service providers may, in any event, be immune from liability for information published on their networks by others under Section 230 of the Communications Decency Act.

7. **Policy Innovations**. Proposed deepfake bills contain various pioneering policies to address this new and developing technology. For example, in a first, a bill pending in Congress would allow for in rem civil litigation against a piece of deepfake media itself so that a court could issue a finding that the material is probably a fake (H.R. 3230). The same bill would require the labeling of deepfake videos and establish penalties for failing to do so (H.R. 3230; *see also* Calif. AB-730 (providing private right of action for election-related deepfakes that don't carry a disclaimer that the media was manipulated)). A Massachusetts bill would criminalize the

creation or use of deepfakes to facilitate otherwise criminal or tortious conduct—essentially eliding what constitutes the wrongful use of manipulated media and instead punishing its use in already impermissible conduct (Mass. H. 3366). And in New York, in a bill that has since expired, lawmakers proposed extending protections of one's portrait—including one's digitally manipulated likeness—for 40 years after one's death. The bill would have also created a registry where one's heirs could document their official control over a deceased relative's portrait (N.Y. A08155, S0587-B).

The following summarizes each proposed or enacted bill, by legislature.

I. US Congress

Proposed federal bills have largely focused on requiring research and reports on deepfake technology. Five such bills remain pending before Congress, and a sixth bill (H.R. 3230) would require annual reporting and briefing on deepfakes in addition to imposing sweeping regulations on the technology.

The latest bill to be introduced in the US Congress on these issues was the ***Identifying Outputs of Generative Adversarial Networks (IOGAN) Act*** (H.R. 4355). The IOGAN Act was proposed by a bipartisan group of legislators led by Rep. Anthony Gonzalez (R-OH) on September 17, 2019.[1] The bill finds that research gaps exist on the underlying technology needed to develop tools to distinguish authentic media from deepfakes (which it refers to as the content generated by "generative adversarial networks," or GANs, the technology that creates realistic forgeries). The measure would direct the Director of the National Science Foundation (NSF) to support "merit-reviewed and competitively awarded research on the science and ethics of material produced by generative adversarial networks." Such research may include social and behavioral research on the ethics of the technology, fundamental research on generative adversarial networks that are aware of "constraints," and research that supplements the work of certain other government elements on digital media forensic tools. The bill would also direct the Director of the National Institute of Standards and Technology (NIST) to support research to develop measurements and standards that could be used to examine deepfakes. The NIST Director would also be required to conduct outreach to stakeholders in the private, public and academic sectors on fundamental measurements and standards research related to deepfakes and consider the feasibility of an ongoing public and private sector engagement to develop voluntary standards for deepfakes. The Directors of the NSF and NIST would be required to submit a report to Congress no later than a year after the bill's enactment on their findings with respect to the feasibility for research opportunities with the private sector and any policy recommendations the Directors have that could facilitate and improve communication and coordination between the private sector, the NSF, and relevant Federal agencies through the implementation of approaches to detect deepfakes.

[1] H.R. 4355, 116th Cong. (2019).

The bill was referred to the House Committee on Science, Space, and Technology.[2] On September 25, 2019, the Committee accepted an amendment offered to the bill by Rep. Jennifer Wexton (D-VA) that would encourage the NSF to conduct research on the public's awareness of deepfakes and best practices for educating the public on how to spot such forgeries.[3]

Another bipartisan bill, ***the Deepfake Report Act of 2019***, was proposed in the House of Representatives on June 28, 2019 (H.R. 3600) and in the Senate on July 9, 2019 (S. 2065).[4] It would direct the Department of Homeland Security to issue a report within 200 days of enactment and every 18 months thereafter on deepfake technology and to assess the AI technologies used to create and detect deepfakes and the changes that may be needed to the laws governing such technologies. The bipartisan bill was introduced by US Sens. Cory Gardner (R-CO), Rob Portman (R-OH) and Martin Heinrich (D-NM), the cofounders of the Senate Artificial Intelligence Caucus, along with caucus members Joni Ernst (R-IA), Brian Schatz (D-HI), Gary Peters (D-MI) and Mike Rounds (R-SD).[5] The House companion bill was introduced by Reps. Derek Kilmer (D-WA), Peter King (R-NY), Stephanie Murphy (D-FL) and Will Hurd (R-TX).[6]

The House version of the bill has been referred to the House Committee on Energy and Commerce.[7] The Senate version was considered at a business meeting on July 24, 2019, and a substitute amendment by Senator Portman was offered and adopted. As amended, the bill only requires annual reports for five years after the initial report (which is to be completed within a year of the bill's enactment), and the report would be limited to ways that deepfakes are used to commit fraud, cause harm and violate federal civil rights, among other small changes.[8] Both the amendment and the legislation as modified were passed by voice vote and placed on the Senate Legislative Calendar under General Orders.[9]

Two congressional omnibus national security bills currently under consideration include similar reporting and briefing requirements. First, ***the National Defense Authorization Act (NDAA) for Fiscal Year 2020*** (H.R. 2500), introduced by Adam Smith (D-WA) on May 2, 2019, includes a requirement that the congressional defense committees receive briefings "from the Secretary of

---

[2] Actions Overview H.R. 4355.

[3] "Amendment to the Amendment in the Nature of a Substitute of H.R. 4355, Offered by Ms. Wexton of Virginia"; *see also* Statement by Congresswoman Jennifer Wexton, via Facebook, Sept. 25, 2019.

[4] H.R. 3600, 116th Cong. (2019); S. 2065, 116th Cong. (2019).

[5] Jonathan Cedarbaum, Matthew F. Ferraro and Brent Gurney, *Bipartisan Group of Legislators Unveils Bill to Address Threat of "Deepfake" Videos*, WilmerHale Client Alert, July 2, 2019; *Gardner, Portman, Heinrich, Ernst, Schatz, Peters, Rounds Introduce Bipartisan Bill to Assess & Address Rising Threat of Deepfakes*, June 28, 2019.

[6] *Reps. Kilmer, King, Murphy, Hurd Introduce Bipartisan, Bicameral Legislation to Assess & Address Rising Threat of Deepfakes*, June 28, 2019.

[7] Actions Overview H.R. 3600.

[8] S. Rep. No. 116-93 (2019).

[9] Actions Overview S. 2065.

Defense on "[e]fforts to counter manipulated media content" (Sec. 256).[10] Specifically, no later than 180 days after the bill's enactment, the Secretary must brief the committees on initiatives of the Department of Defense "to identify and address . . . manipulated media content, specifically 'deepfakes.'" The briefings must include a review of:

- the status of efforts to develop technology that could identify deepfakes that impact national security;
- challenges to the detection, labeling and prevention of the use by foreign actors of deepfakes that impact national security;
- plans to make deepfake detection technology available to other federal agencies and the public;
- efforts of the Department of Defense to engage with academia and industry to combat the use of deepfakes by state and nonstate actors "on social media platforms impacting operations overseas";
- an assessment of adversaries' abilities to generate deepfakes; and
- "[r]ecommendations for a long-term transition partner organization."

The NDAA would also increase by $5 million the funding specifically for media forensics, as part of the special operations forces technology development funding line.

The NDAA, which is Congress's yearly defense funding bill, passed the House on July 12, 2019, and must be reconciled with the Senate's version of the NDAA, which does not contain this provision.[11]

Second, a provision of the ***Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020*** (H.R. 3494), introduced by Rep. Adam Schiff (D-CA) on June 26, 2019, would require the Director of National Intelligence (DNI) to submit a report on the national security impact of deepfakes—specifically machine-manipulated media and machine-generated text—and the use of such technology by foreign governments to spread disinformation.[12]

It would also require the DNI to:

- identify technologies that could be developed to counter deepfakes;

---

[10] H.R. 2500, 116th Cong. (2019).

[11] Actions Overview H.R. 2500.

[12] H.R. 3494, 116th Cong. (2019).

- identify intelligence community offices that should have lead responsibility for monitoring the development of AI-manipulated media;
- describe research and development activities carried out by the intelligence community on machine-manipulated media; and
- provide recommendations on whether the intelligence community requires additional legal authorities or resources to address the national security threat of machine-manipulated media and machine generated text (Sec. 715).

Finally, the Schiff bill would direct the DNI to administer a Deepfake Prize competition to stimulate the research, development or commercialization of technologies to detect deepfakes automatically (Sec. 707). The bill passed the House on July 17, 2019, and has now been referred to the Senate Select Committee on Intelligence.[13]

In May 2019, Sen. Ben Sasse (R-NE) introduced ***A Bill to Require the Secretary of Defense to Conduct a Study on Cyberexploitation of Members of the Armed Forces and Their Families, and For Other Purposes*** (S. 1348).[14] The bill focuses on "cyberexploitation," which it defines as "the use of digital means to knowingly access, or conspire to access, without authorization, an individual's personal information to be employed (or to be used for) with malicious intent." It would require the Secretary of Defense to conduct a study within 150 days of enactment assessing the potential vulnerability of the members of the US armed forces and their families to cyberexploitation. It would also direct the creation of a catalog of past and current efforts by foreign governments and nonstate actors to exploit the personal information and accounts of members of the armed forces and their families, an assessment of the actions undertaken by the Department of the Defense to educate the military about those efforts, and an assessment of the potential for the cyberexploitation of "misappropriated images and videos as well as deep fakes." It also directs the Secretary to develop recommendations for legislative or administrative policy changes to reduce military members' vulnerability to such exploitation.

The bill has been referred to the Senate Armed Services Committee.[15]

Senator Sasse introduced three other bills on deepfake issues in the previous Congress, which have since expired:

- *The Malicious Deep Fake Prohibition Act of 2018* (S. 3805), introduced on December 21, 2018, would have established a new criminal offense for those who create and distribute deepfakes under certain circumstances.[16] First, the bill would have made it illegal to

---

[13] Actions Overview H.R. 3494.

[14] S. 1348, 116th Cong. (2019).

[15] Actions Overview S. 1348.

[16] S. 3805, 115th Cong. (2018).

"create, with the intent to distribute, a deep fake with the intent that the distribution of the deep fake would facilitate criminal or tortious conduct under Federal, State, local, or Tribal law." Second, it would have made it a crime to "distribute" an audiovisual record with "actual knowledge" that it is a deepfake and the "intent" that its distribution "would facilitate criminal or tortious conduct under Federal, State, local, or Tribal law." Under the bill, providers of interactive computer services (such as social media companies) would not be held liable on account of "any action voluntarily taken in good faith to restrict access to or availability of deep fakes" or "any action taken to enable or make available to information content providers or other persons the technical means to restrict access to deep fakes." The bill seemed designed to incentivize platforms to set up reporting systems to flag and notify the platforms of deepfakes so they could then be taken down.[17]

- *A Bill to Require Studies on Cyberexploitation of Employees of Certain Federal Departments and Their Families, and For Other Purposes* (S. 3788), introduced on December 19, 2018, which would have required, within 150 days of enactment, the heads of various federal agencies to conduct a study assessing, among other things, the potential for cyberexploitation of deepfakes of the personal information and accounts of employees of a range of federal agencies and their families.[18]
- *A Bill to Require the Secretary of Defense to Conduct a Study on Cyberexploitation of Members of the Armed Forces and Their Families, and For Other Purposes* (S. 3786), introduced on December 19, 2018, which would have directed the Department of Defense to complete a study on the malicious, unauthorized digital access of the personal information and accounts of members of the armed forces and their families.[19] While this bill expired at the conclusion of the 115th Congress,[20] Senator Sasse reintroduced the same bill in the next Congress, and it remains pending (*see* S. 1348 discussed above).

In addition to bills that primarily require research and reports, Rep. Yvette Clarke, D-NY, introduced in June 2019 the most far-reaching deepfakes-related bill currently under consideration by Congress, the ***Defending Each and Every Person from False Appearances by Keeping Exploitation Subject (DEEP FAKES) to Accountability Act*** of 2019 (H.R. 3230).[21] If passed, the bill would require anyone creating a deepfake image, audio or video imitating a person to label the media with a watermark to disclose that the media has been altered.

---

[17] Kaveh Waddell, *Lawmakers Plunge into "Deepfake" War*, Axios, Jan. 31, 2019.

[18] S. 3788, 115th Cong. (2018).

[19] S. 3786, 115th Cong. (2018).

[20] Actions Overview S. 3788.

[21] H.R. 3230, 116th Cong. (2019).

Knowingly failing to disclose the deepfake—which the bill also calls an "advanced technological false personation record"—would result in a criminal penalty of up to five years' imprisonment. The defendant would be liable if the failure to disclose was done knowingly and with the following intent:

1) to "humiliate or otherwise harass" the target of the altered media if the media contained "sexual content";

2) to cause violence or physical harm;

3) "in the course of criminal conduct related to fraud, including securities fraud and wire fraud, false personation, or identity theft"; and

4) "by a foreign power, or an agent thereof, with the intent of influencing a domestic public policy debate, interfering in a Federal, State, local, or territorial election, or engaging in other acts which such power may not lawfully undertake."

In sum, the DEEP FAKES Accountability Act seeks to protect against the full gamut of deepfake harms, from nonconsensual pornography to foreign interference in elections and public policy debates, from inciting violence to conducting financial fraud and identity theft.

The act would also impose a civil penalty (of up to $150,000 for each record) and provide for injunctive relief for failing to create the required disclosure or for knowingly altering the disclosure. In addition, the bill would establish a right of action for victims of altered media to sue the creators for equitable and injunctive relief. Because many creators and propagators of deepfake material reside overseas, it would also provide for extraterritorial federal jurisdiction over an offense if the defendant or the depicted person is a citizen or permanent resident of the United States.

Notably, the DEEP FAKES Accountability Act would provide several kinds of exceptions to its disclosure requirement. In particular, it would exempt deepfake material that a reasonable person would not mistake as "actual material activity of the exhibited living person, such as parody shows or publications, historical reenactments, or fictionalized radio, television, or motion picture programming." It would also exempt deepfake material produced by a US government employee or under the US government's authority "in furtherance of public safety or national security."

The bill would impose several new and novel responsibilities upon the executive branch to support both victims of deepfakes and audiovisual producers in need of legal guidance. The act would require federal authorities to consult, "to the extent practicable," with individuals depicted in prohibited deepfakes "regarding measures such authorities can reasonably undertake to protect their privacy and minimize additional public viewings" of the falsified media. It would also impose on the Attorney General of the United States the responsibility to issue advisory opinions to producers of audiovisual material regarding the legality of their proposed material. The bill would empower the Attorney General to authorize waivers from the disclosure requirements "to additional categories of advanced technological false personation records upon petition of any producer," if the petitioners can show that the law would "impede their ability to engage in otherwise lawful activities protected

by the First Amendment of the Constitution." And the bill would require the Attorney General to designate in each US Attorney's Office two "coordinators," one "for violations directed by foreign nation-states" and one "for false intimate depictions," to receive reports from the public regarding potential violations of the law.

The Attorney General would also be required to publish a report that describes the efforts of Russia, China, and other states or groups "to use deep fake technology to impact elections or public policy debates in the United States or other democracies"; describes the impact "of intimate and sexual deep fakes on women and marginalized communities"; and provides official guidance to federal prosecutors to assist with prosecutions under the act.

The DEEP FAKES Accountability Act would require manufacturers creating software that will be used to produce deepfakes to ensure that the software allows for the insertion of watermarks and disclosures and that the software requires users to acknowledge their legal obligations under the act.

In a novel twist, the bill would also allow for in rem civil proceedings against a deepfake record itself, under certain circumstances. The remedies for such an in rem action would be limited to a court order declaring that there is "a substantial likelihood" that the depicted activity "is false" and lacks the disclosure required by the law.

The act would establish the "Deep Fakes Task Force" under the Secretary of Homeland Security to advance efforts to combat the national security implications of deepfakes, research and develop technologies to detect and counter deepfakes, and, among other tasks, facilitate discussion and appropriate cooperation between the government and the private sector on these issues. The task force would issue an annual report for five years. The Secretary of Homeland Security would also be required to provide an annual briefing on "any known attempts of foreign states to use deep fake technology to influence or otherwise interfere in an official proceeding within the United States, including an election."

Finally, this bill—which would go into effect one year after enactment—would update the definitions of the federal identity theft statute (18 U.S.C. § 1028) to include in the list of prohibited forgeries a "false audiovisual identification record" (defined as a "deep fake" or "advanced technological false personation record"). And it would update the federal false personation statute (18 U.S.C. Ch. 43) to prohibit the use of deepfake technology to impersonate falsely an officer or employee of the United States, among others.

The DEEP FAKES Accountability Act is currently under consideration by the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security.[22]

---

[22] Actions Overview H.R. 3230.

II. California

On Friday, September 13, 2019, lawmakers in California passed two bills related to deepfakes that await Governor Gavin Newsom's signature (*see* Calif. AB-602 and Calif. AB-730). A third deepfake bill (Calif. AB-1280) remains under consideration in the state senate.

The first bill before the Governor would provide victims of nonconsensual, deepfake pornography a private right of action against those who create or share it. The California State Senate adopted the bill on Tuesday, September 10 (by a vote of 40-0). The California State Assembly passed it by a vote of 61-0 on September 13, sending it to the desk of Governor Newsom, who has until October 13 to sign it.[23]

Introduced by Assembly Member Marc Berman (D), the bill—***Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action*** (Calif. AB-602)—would amend Section 1708.86 of the California Civil Code to provide a private right of action against a person who intentionally distributes a pornographic photograph or video of a "depicted individual" without that person's consent, under specified conditions.[24] Notably, the bill defines a "depicted individual" to include someone "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." An "altered depiction" means a performance that the person gave but that was "subsequently altered" to violate the bill's terms. A plaintiff could bring a cause of action if the defendant knew or "reasonably should have known the depicted individual in that material did not consent to its creation or disclosure." It would not be a defense to an action under this bill if a disclaimer is placed on the material acknowledging that it is fake or unauthorized.

The bill would exclude from liability someone who disclosed sexually explicit material under certain circumstances. Those circumstances include when "[r]eporting unlawful activity," when exercising law enforcement duties or in legal proceedings. It would also exempt covered material that relates to a "matter of legitimate public concern," constitutes a "work of political or newsworthy value," or constitutes "[c]ommentary, criticism, or disclosure that is otherwise protected by the California Constitution or the United States Constitution."

A plaintiff could seek economic and noneconomic damages, statutory damages (capped at $30,000, or $150,000 if the unlawful act was committed with malice), punitive damages, and attorneys' fees.

The Screen Actors Guild-American Federation of Television and Radio Artists (SAG-AFTRA) strongly supports AB-602 and is urging Governor Newsom to sign it to protect actors from

---

[23] *See* Melody Gutierrez, *Victims of Fake Sex Videos Could File California Lawsuits Under Proposed Law*, L.A. Times, Sept. 13, 2019.

[24] AB-602 (California), Sept. 6, 2019, version.

exploitation, calling it "an opportunity for California to be a global leader on the rapidly escalating threat of 'deepfake' videos."[25] In April 2019, when the California State Senate was considering a very similar Senate bill (*Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material* (Calif. SB-564), introduced by State Sen. Connie Leyva (D)), SAG-AFTRA had encouraged its members to support its passage with the hashtag #ProtectMyImage.[26]

The second bill awaiting the Governor's signature[27]—***Elections: Deceptive Audio or Visual Media*** (Calif. AB-730)—would amend Section 20010 of the California Elections Code to prohibit a person, committee or other entity, within 60 days of an election, from distributing, "with actual malice, materially deceptive audio or visual media" of a candidate for election "with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate," unless the media carried a disclosure that it had been manipulated.[28]

Introduced by Assembly Member Berman in February 2019 and amended as recently as September 10, the bill overcame objections from the California News Publishers Association and the California Cable and Telecommunications Association that it was a threat to free speech.[29] The bill was adopted by the California Senate on Friday, September 13, 2019, by a vote of 29-7 and by the California Assembly the same day by a vote of 67-4.[30]

While the bill does not address "deepfakes" per se, it defines "materially deceptive audio or visual media" to capture the same material: images, audio, or video of a candidate's appearance, speech or conduct "that has been intentionally manipulated." To fall under this definition, the media must meet the following conditions:

1) The media "would falsely appear to a reasonable person to be authentic"; and

2) The media "would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were hearing or seeing the unaltered, original version of the image or audio or video recording."

---

[25] Dave McNary, *SAG-AFTRA Urges Gavin Newsom to Sign Law Punishing 'Deep Fake' Videos*, Variety, Sept. 13, 2019.

[26] *ACTION ALERT: Support California Bill to End Deepfake Porn*, SAG-AFTRA, Apr. 29, 2019. The Senate Appropriations Committee voted on May 13 to hold SB-564 in suspense so that AB-602, of which Senator Leyva is the principal coauthor, could proceed to a vote. *See* "Hearing Results," California Senate Appropriations Committee, May 13, 2019.

[27] Alexei Koseff and Dustin Gardiner, *California Lawmakers Vote for 8:30 a.m. Starting Time for High schools*, San Francisco Chronicle, Sept. 14, 2019.

[28] AB-730 (California), Sept. 10, 2019 version.

[29] *See* Nick Cahill, *California Senate Approves Anti-Deepfake Bill Despite Free Speech Concerns*, Courthouse News Service, Sept. 13, 2019.

[30] *Id.*

The bill would provide exemptions from liability for broadcasting stations and internet websites that carry the altered media so long as the media is labeled to show that its authenticity is questionable. Outlets would not be held liable for airing paid political advertisements that contained materially deceptive audio or video. And, in an apparent response to concerns by free speech advocates, the revised bill exempts from liability "materially deceptive audio or visual media that constitutes satire or parody."

The bill's provisions would sunset on January 1, 2023, unless extended by a later statute.

Finally, a third bill still under consideration in the California legislature—***Crimes: Deceptive Recordings*** (Calif. AB-1280)—would go further than AB-602 and AB-730, which would impose only civil liability, by criminally prohibiting the creation or distribution of nonconsensual pornographic deepfakes and deepfakes used to deceive voters before an election.[31]

The bill defines a "deepfake" as "any" audio or visual media in an electronic format "that is 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."

First, it would criminalize the preparation, production, development or distribution of a deepfake that depicts a person "engaging in sexual conduct" without that person's consent. The law would impose harsher penalties on a sexually explicit deepfake of a minor. Second, the bill would criminalize the preparation, production and development of any deepfake created with the intent to "coerce or deceive any voter into voting for or against a candidate or measure" in an election occurring within 60 days.

The bill would also appropriate $25 million to the University of California for research to identify and combat the inappropriate use of deepfake technology. Introduced in the California General Assembly in February 2019 by Assembly Member Tim Grayson (D), it failed its first attempt at passage and has been re-referred to the Committee on Public Safety.[32]

III. Massachusetts

In Massachusetts, in January 2019, Rep. Jay D. Livingstone introduced ***An Act to Protect Against Deep Fakes Used to Facilitate Criminal or Torturous Conduct*** (Mass. H. 3366), which would expand the state's definition of identity fraud to criminalize the creation or distribution of deepfakes intended for use in otherwise criminal or tortious conduct.[33]

---

[31] AB-1280 (California), Apr. 22, 2019, version.

[32] California AB1280, TrackBill.

[33] Bill H. 3366 (Massachusetts).

The bill defines deepfakes with a reasonable person standard, as "an audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual."

The bill would make it a crime for someone either to "create[], with the intent to distribute, a deep fake and with the intent that the distribution of the deep fake would facilitate criminal or tortious conduct," or for someone to "distribute[]" a deepfake "with actual knowledge that the audiovisual record is a deep fake and with the intent that the distribution of the audiovisual record would facilitate criminal or tortious conduct."

Note that liability turns on the intent that the deepfake be used to facilitate already prohibited conduct. In this way, the bill is nearly unique because it avoids defining additional purposes for deepfakes (whether revenge porn or inappropriate electoral influence) by essentially piggybacking deepfakes onto already prohibited conduct. (As discussed above, the Malicious Deep Fake Prohibition Act of 2018 (S. 3805), which expired in the US Senate last year, would have similarly established a new criminal offense for deepfake creators and propagators if they had the "intent" to "facilitate criminal or tortious conduct under Federal, State, local, or Tribal law.")

Punishments could include a fine not to exceed $5,000 and imprisonment of up to two and a half years. The bill would exclude from liability "any activity protected by the Massachusetts Constitution or by the First Amendment to the Constitution of the United States."

A hearing on the bill was held in May 2019, and it remains pending in the state Committee on the Judiciary.[34]

IV. New York

New York lawmakers considered in 2018 an innovative law to combat deepfake pornography. While it has since expired, the bill garnered significant attention.[35] Introduced by State Assembly Rep. Joseph Morelle (D, now a member of the House of Representatives) and State Sen. Diane Savino (D), the bill—***An Act to Amend the Civil Rights Law, in Relation to the Right of Privacy and the Right of Publicity*** (N.Y. A08155, S0587-B)—would have amended existing civil rights law to establish the right of privacy and the right of publicity for both living and deceased individuals by providing that an individual's persona is the personal property of the individual and is freely transferable and descendible.[36] It would have extended protections of one's likeness for 40 years

[34] Jay Livingstone - (D) Massachusetts, Bill Track 50.

[35] Jennifer Rothman, *Only Robin Wright Should Own Robin Wright*, Volokh Conspiracy, May 9, 2018; Eriq Gardner, *Disney Comes Out Against New York's Proposal to Curb Pornographic "Deepfakes,"* Hollywood Reporter, June 11, 2018.

[36] A08155/S05857-B (New York).

past death and would have created a registry where heirs could document their official control over a deceased relative's name and image.

Importantly in this context, it included in the definition of someone's persona a person's "digital replica," defined as "a computer-generated or electronic reproduction of a living or deceased individual's likeness or voice that realistically depicts the likeness or voice of the individual being portrayed." The bill would have established that the use of a "digital replica" of a person without his or her consent in any kind of performance (scripted, musical, athletic, pornographic and so on) constituted a violation of the law.

The actors' guild SAG-AFTRA supported the bill, saying it would give "families the right to prevent unwanted commercial exploitation of their deceased loved ones" while protecting "individuals from unwanted image and voice manipulation and unauthorized advertisements," "prohibiting deepfake pornography, and clarifying the digital replica rights of entertainers."[37] The bill was opposed by media companies including the Motion Picture Association of America, Getty Images, the New York State Broadcasters Association, the Electronic Frontier Foundation, the Digital Media Licensing Association, the Entertainment Software Association, the Media Coalition, Disney, NBCUniversal, Viacom, Warner Bros. and others.[38]

The bill passed the New York State Assembly but expired at the end of the term while under consideration in the state senate.[39]

V. Texas

On Sept. 1, Texas became the first state in the nation to prohibit the creation or distribution of deepfake videos intended to harm candidates for public office or influence elections.[40] Amid rising fears of the dangers of hyperrealistic, computer-altered fake photos and videos, Texas is now only the second state to impose penalties on the creation and propagation of deepfakes in certain circumstances. As discussed above, other state houses around the country, as well as Congress, may adopt additional, comparable measures targeting deepfake technology over the next year.

---

[37] *SAG-AFTRA Statement on the Passing of New York Assembly Bill A.8155-B*, June 18, 2018.

[38] Judy Bass, *New York Right of Publicity Bill Passage Drama Ends With No Action by State Senate*, N.Y. State Bar, June 25, 2018; *Memorandum in Opposition to New York Assembly Bill A.8155B (Morelle, Right of Publicity)*, Motion Picture Association of America, June 8, 2018; Daniel Nazer, *Once Again, New York State Considers a Terrible Right of Publicity Law, Electronic Frontier Foundation*, June 8, 2018; Gardner, Hollywood Reporter, June 11, 2018.

[39] Bass, N.Y. State Bar, June 25, 2018.

[40] Matthew Ferraro, *Texas Law Could Signal More State, Federal Deepfake Bans*, Law 360, Sept. 6, 2019; Chuck Lindell, *800 New Laws Take Effect Sunday*, Glen Rose Reporter, Aug. 29, 2019.

The new Texas law (Tex. SB 751) defines a "deep fake video" as a video "created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality."[41] It makes it a Class A misdemeanor,[42] punishable by up to a year in the county jail and a fine of $4,000,[43] for a person to "create[]" a deepfake video and "cause[]" that video "to be published or distributed within 30 days of an election," if the person does so with the "intent to injure a candidate or influence the result of an election."

Analysis by the Texas Senate Research Center acknowledged that deepfake technology "likely cannot be constitutionally banned altogether," but concluded that "it can be narrowly limited to avoid what may be its greatest potential threat: the electoral process."[44] The law, originally introduced by Texas Sens. Bryan Hughes, a Republican, and Royce West, a Democrat, was signed by Texas Governor Greg Abbott on June 14 and amends Section 255.004 of the Texas Election Code.

VI. Virginia

In June 2019, an app developer released and then quickly ceased distribution of "DeepNude," a program that used AI to make images of clothed women appear to be realistic nudes.[45] Concern that such software has made it remarkably easy to use deepfake technology to create convincing nudes or sexual imagery that could be used to harass or exploit nearly anyone led Virginia to became the first state in the nation to impose criminal penalties on the distribution of nonconsensual deepfake pornography.

The Virginia law—***Unlawful Dissemination or Sale of Images of Another Person*** (Va. Code Ann. § 18.2-386.2, HB 2678, SB 1736)—went into effect on July 1, 2019. It made the distribution of nonconsensual "falsely created" images and videos a Class 1 misdemeanor,[46] punishable by up to a year in jail and a fine of $2,500. Originally introduced in January 2019 in the Virginia House of Delegates by Del. Marcus B. Simon (D) and in the Virginia State Senate by Sen. Adam P. Ebbin (D) and signed into law in March, the new law amends Section 18.2-386.2 of the Code of Virginia.[47] It imposes criminal penalties on

> "[a]ny person who, with the intent to coerce, harass, or intimidate, maliciously disseminates or sells any videographic or still image created by any means whatsoever, *including a falsely created videographic or still image*, that depicts

---

[41] SB 751 (Texas).

[42] Bill Analysis, C.S.S.B. 751, Texas Senate Research Center.

[43] Tex. Penal Code Ann. § 12.21.

[44] Bill Analysis, C.S.S.B. 751, Texas Senate Research Center.

[45] Timothy B. Lee, *Author Pulls Software that Used Deep Learning to Virtually Undress Women*, ARS Technica, June 28, 2019.

[46] 2019 Session, HB 2678, Virginia's Legislative Information System.

[47] Va. Code Ann. § 18.2-11.

another person who is totally nude," or in a state of undress "where such person knows or has reason to know that he is not licensed or authorized to disseminate or sell such videographic or still image . . ." (emphasis added).[48]

The law specifically exempts from liability internet service providers that enable computer access to others committing such acts.

VII. Conclusion

Laws in this area are changing rapidly as legislatures at both the state and federal levels grapple with emerging technologies that could have far-reaching implications for individuals, companies and society at large. State legislatures have thus far taken the lead on legislation in this area, while Congress is considering bills that are limited to studying and reporting on the issue, with one notable exception. We can expect further legislative activity as lawmakers attempt to draft laws that abide by constitutional free speech requirements while protecting against present harms and anticipating inchoate ones.

[48] HB 2678 (Virginia).

I gratefully acknowledge former summer associate Courtney Murray and Research and Reference Specialist Karen Rutherford for their research assistance.

For more information on this or other deepfake matters, contact:

Matthew Ferraro | +1 202 663 6562 | matthew.ferraro@wilmerhale.com.