Bipartisan Group of Legislators Unveils Bill to Address Threat of “Deepfake” Videos

JULY 2, 2019

On June 28, 2019, a large bipartisan group of Senators and Representatives introduced a bill to assess the rising threat of “deepfakes”—manipulated videos that can show people saying things they never said and doing things they never did. The bill, the *Deepfakes Report Act of 2019*, would direct the Department of Homeland Security (DHS) to issue a report within 200 days of enactment and every 18 months thereafter on deepfake-technology and to assess the artificial intelligence (AI) technologies used to create and detect deepfakes and the changes that may be needed to the laws governing such technologies. It represents the latest effort by federal and state lawmakers to address rising public concerns about the dangers posed by high-quality disinformation to the electoral process, national security, commercial and financial activity, and personal privacy.

The bill broadly defines deepfakes, or what it calls “digital content forgeries.” Under the bill, the term includes the “use of emerging technologies, including artificial intelligence and machine learning techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead.” The definition is notable because it includes the manipulation not just of audio and video but also of text. It also makes no exception for technology used to produce parodies or satires, which civil liberty organizations have noted could be swept up in attempts to regulate defamatory or injurious videos.

The bill would require DHS to report on three broad categories:

- *assessments* of the underlying technologies used to make deepfakes, who is using them (i.e., foreign or domestic sources), in what contexts (i.e., cyberattacks, pornography, and media), and to what ends. The bill specifically requires assessments of how foreign governments could use deepfakes to “harm national security,” how domestic NGOs could use them, and how deep learning technologies that fabricate content of “events that did not occur” could pose social dangers or benefits. (§ 3(b)(1)-(5))
- *analyses* of methods and technical countermeasures that could be used to detect deepfakes. (§ 3(b)(6)-(7)); and
- *recommendations* regarding what legal authorities could be needed to address the issue. (§ 3(b)(8)).

The bill would direct DHS to consult with many other federal security, intelligence, and regulatory agencies in the preparation of these reports, including the Intelligence Community, the Department of Defense, the Joint Chiefs of Staff, the Department of Justice, the Federal Election Commission, and the Federal Trade Commission (FTC), among others. It would also require DHS to hold public hearings. (§ 3(c)).

The inclusion of the FTC—charged with protecting consumers and competition—is noteworthy because of the rising threat deepfakes and other forms of disinformation pose to businesses. As WilmerHale attorneys have written, disinformation campaigns have harmed businesses by spreading falsehoods about their brands, manipulating stock prices, and undermining confidence in emerging technologies through bogus or grossly misleading "news" reporting. The dangers of disinformation to the private sector will grow as deepfake-technology increases in sophistication, and companies of all sizes can undertake steps to prepare and mitigate the dangers. (For more information on this issue, watch a recent WilmerHale webinar, titled "Hard Truth: Disinformation Threatens Business").

The Deepfakes Report Act was introduced by U.S. Senators Cory Gardner (R-CO), Rob Portman (R-OH), and Martin Heinrich (D-NM), the co-founders 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). The House companion bill was introduced by Representatives Derek Kilmer (D-WA), Peter King (R-NY), Stephanie Murphy (D-FL), and Will Hurd (R-TX).

This bill is one of several proposed in the past few months at the state and federal levels to address deepfakes. Other bills would criminalize the malicious creation and distribution of deepfakes, impose penalties on deepfake creators who use the likenesses of others without their consent, and require anyone creating a piece of synthetic media imitating a person to disclose that the video was altered or generated. On July 1, 2019, Virginia updated its laws to impose criminal penalties on the distribution of non-consensual "deepfake" images and video, what it calls "falsely created videographic or still image[s]."

In coming months and years, deepfakes will attract the interest of policymakers as they continue to grapple with an emerging and difficult technological challenge. WilmerHale will continue to follow developments in this area closely.

Authors

Brent J. Gurney

PARTNER

✉ brent.gurney@wilmerhale.com

☎ +1 202 663 6525

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP