Calendar No. 580

116TH CONGRESS *2d Session*	SENATE	REPORT 116–289

IDENTIFYING OUTPUTS OF GENERATIVE ADVERSARIAL NETWORKS ACT

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 2904

NOVEMBER 9, 2020.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
19–010 WASHINGTON : 2020

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

ROGER F. WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD C. YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD J. MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY C. PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

JOHN KEAST, *Staff Director*
DAVID STRICKLAND, *Minority Staff Director*

Calendar No. 580

116TH CONGRESS *2d Session* | SENATE | REPORT 116–289

IDENTIFYING OUTPUTS OF GENERATIVE ADVERSARIAL NETWORKS ACT

NOVEMBER 9, 2020.—Ordered to be printed

Mr. WICKER, from the Committee on Commerce, Science, and Transportation, submitted the following

R E P O R T

[To accompany S. 2904]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 2904) to direct the Director of the National Science Foundation to support research on the outputs that may be generated by generative adversarial networks, otherwise known as deepfakes, and other comparable techniques that may be developed in the future, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

This bill would direct the National Science Foundation (NSF) and the National Institute of Standards and Technology (NIST) to support research on the outputs by generative adversarial networks, commonly referred to as "deepfakes." NSF would be required to support research on manipulated or synthesized content and information authenticity. NIST would be required to support research for the development of measurements and standards necessary to accelerate the development of the technological tools to examine the functions and outputs of generative adversarial networks or other technologies that synthesize or manipulate content.

BACKGROUND AND NEEDS

Generative adversarial networks (GANs) are a type of algorithm that utilize two neural networks to produce synthetic data that appears real.[1] One output of a GAN, commonly known as a deepfake, is a convincing digital video, imagery, or audio of events that never occurred. Most commonly, deepfakes appear in computer-assisted productions of highly believable audio and video in which real people appear to be saying things or doing actions that they never said or did.[2] While the sophisticated manipulation of image and video applications can be solely based in personal amusement or artistic value, other such manipulations are for adversarial purposes such as propaganda and misinformation campaigns.[3] Deepfakes have the potential to be used in information warfare or to manipulate elections.[4] The development of standards for authentication or simply identification is a growing necessity as deepfakes move closer to illegal activities such as copyright infringements and data breaches.[5]

Due to the nature of the internet and the rapid advancement of technology, the production of deepfakes does not require complex processing systems. Academic and industrial researchers and even amateurs are able to acquire the computer resources necessary to create deepfakes. The increase in the prominence of deepfakes has also lead to an increase in quality awareness. Poor quality videos have become easier to detect, exposing inconsistencies such as lighting deficiencies and audio glitches.

Agencies, universities, and private industry have launched research and development initiatives to enhance deepfake detection.[6] Companies such as Amazon, Facebook, Microsoft, and others have joined the Deepfake Detection Challenge (DFDC), which invites people from around the world to build innovative new technologies to help in the detection of manipulated media.[7] The Department of Defense, through the Defense Advanced Research Projects Agency (DARPA) has commissioned researchers across the United States to develop deepfake detection methods. DARPA, in collaboration with the University of Colorado Denver, is working to create convincing videos in order to develop technology to detect the real from the fake.[8] Researchers at the Georgia Tech Research Institute have been working on a grand prize initiative to generate differentially private synthetic data using GANs. This data will then be able to

[1] National Institute of Standards and Technology, "Georgia Tech: The Unlinkable Data Challenge," Public Safety Communications Research Division, press release, updated Jan. 22, 2019 (https://www.nist.gov/ctl/pscr/georgia-tech) (accessed Sep. 3, 2020).

[2] David Chu et al., *White Paper: Deep Fakery—An Action Plan*, 2019 (*available at* https://www.nsf.gov/mps/dms/documents/Deep_Fakery_Workshop_Report.pdf) (accessed Sep. 3, 2020).

[3] Dr. Matt Turek, "Media Forensics (MediFor)," Defense Advanced Research Projects Agency (https://www.darpa.mil/program/media-forensics) (accessed Sep. 3, 2020).

[4] Donie O'Sullivan, "Lawmakers Warn of 'Deepfake' Videos Ahead of 2020 Election," *CNN*, Jan. 28, 2019 (https://www.cnn.com/2019/01/28/tech/deepfake-lawmakers/index.html) (accessed Sep. 3, 2020).

[5] Ian Sample, "AI-generated Fake Videos Are Becoming More Common (and Convincing). Here's Why We Should Be Worried," *Guardian*, Jan. 13, 2020 (*available at* https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them) (accessed Sep. 3, 2020).

[6] Id.

[7] Deepfake Detection Challenge, "Building Tools to Detect Deepfakes Together," Facebook, 2019 (https://deepfakedetectionchallenge.ai/) (accessed Sep. 3, 2020).

[8] Donie O'Sullivan, "When Seeing Is No Longer Believing: Inside the Pentagon's Race Against Deepfake Videos," *CNN Business*, 2019 (https://www.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/) (accessed Sep. 3, 2020).

be utilized for a variety of analysis efforts, which may include classification, regression, clustering, and answering unknown research questions.[9] These developments have improved understanding of this issue and have shown the opportunity for agency and private partnerships, as well as the need for standards to detect bad actors.

SUMMARY OF PROVISIONS

S. 2904, as amended, would direct NSF and NIST to do the following:

- Support research on generative adversarial networks or deepfakes.
- Support research on manipulated or synthesized content and information authenticity.
- Support research for the development of measurements and standards necessary to accelerate the development of the technological tools to examine the functions and outputs of generative adversarial networks or their technologies that synthesize or manipulate content.
- Report to Congress on the feasibility of utilizing public-private research partnerships to detect manipulated or synthesized content.

LEGISLATIVE HISTORY

S. 2904, the Identifying Outputs of Generative Adversarial Networks Act, was introduced on November 20, 2019, by Senator Cortez Masto (for herself and Senator Moran) and was referred to the Committee on Commerce, Science, and Transportation of the Senate. On May 20, 2020, the Committee met in open Executive Session and, by voice vote, ordered S. 2904 reported favorably with an amendment (in the nature of a substitute), with a first degree amendment.

H.R. 4355, the Identifying Outputs of Generative Adversarial Networks Act, was introduced on September 17, 2019, by Representative Gonzalez [R–OH–16] (for himself and Representatives Stevens [D–MI–11], Baird [R–IN–4], and Hill [D–CA–25]) and was referred to the Committee on Science, Space, and Technology of the House of Representatives. On December 9, 2019, H.R. 4355, as amended, was passed by voice vote in the House of Representatives and was referred to the Committee on Commerce, Science, and Transportation of the Senate.

Hearings

On June 13, 2019, the Permanent Select Committee on Intelligence of the House of Representatives held a hearing entitled "The National Security Challenge of Artificial Intelligence, Manipulated Media, and 'Deepfakes'".[10] This hearing specifically examined deepfakes and other types of AI generated synthetic data.

---

[9] National Institute of Standards and Technology, "Georgia Tech: The Unlinkable Data Challenge," Public Safety Communications Research Division, press release, updated Jan. 22, 2019 (https://www.nist.gov/ctl/pscr/georgia-tech) (accessed Sep. 3, 2020).

[10] U.S. Congress, House Permanent Select Committee on Intelligence, *The National Security Challenge of Artificial Intelligence, Manipulated Media, and "Deepfakes,"* 116th Cong., 1st sess., Jun. 7, 2019, press release and webcast (https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=657) (accessed Sep. 3, 2020).

On January 15, 2020, the Committee on Commerce, Science, and Transportation of the Senate held a hearing entitled "Industries of the Future." This hearing included an examination of the opportunities and issues associated with the development of increasingly sophisticated artificial intelligence capabilities, including deepfakes.[11]

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

S. 2904, Identifying Outputs of Generative Adversarial Networks Act
As ordered reported by the Senate Committee on Commerce, Science, and Transportation on May 20, 2020

By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	6	not estimated

Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2031?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 2904 would require the National Science Foundation (NSF) to support research on manipulated digital content and information authenticity. The bill also would direct the National Institute of Standards and Technology (NIST) to create measurements and standards for the development of technological tools that examine generative adversarial networks (GANs), which are used to produce manipulated content.

For this estimate, CBO assumes that the legislation will be enacted in late 2020. Under that assumption, the affected agencies could incur some costs in 2020, but CBO expects that most of the costs would be incurred in 2021 and later.

Using information from the NSF, CBO estimates that implementing the bill would have no significant cost for the NSF because the agency is already carrying out the required activities through its existing grant programs. Using information from NIST, CBO estimates that the agency would require 10 additional employees at an average annual cost of $175,000 each through 2023 to establish a research program on GANs and similar technologies. S. 2904 also would direct NIST and the NSF to report to the Congress on related policy recommendations. Based on the costs of similar tasks, CBO estimates that developing the report would cost less than

[11] U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Industries of the Future*, 116th Cong., 1st sess., Jan. 15, 2020, press release and webcast (https://www.commerce.senate.gov/2020/1/industries-of-the-future) (accessed Sep. 3, 2020).

$500,000. In total, CBO estimates that implementing S. 2904 would cost $6 million over the 2020–2025 period; such spending would be subject to the availability of appropriated funds.

On October 29, 2019, CBO transmitted a cost estimate for H.R. 4355, the Identifying Outputs of Generative Adversarial Networks Act, as ordered reported by the House Committee on Science, Space, and Technology on September 25, 2019. The two pieces of legislation are similar; the differences in CBO's estimated costs in 2020 reflect different assumed dates of enactment.

The CBO staff contacts for this estimate are Janani Shankaran and David Hughes. The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

Number of Persons Covered

S. 2904, as amended, would cover the NSF, NIST, DARPA, Intelligence Advanced Research Projects Activity (IARPA), other relevant Federal agencies, Congress, and public and private academic and scientific stakeholders on forensic science and generative adversarial networks.

Economic Impact

S. 2904, as amended, would have no negative expected impacts on the scientific community. Rather, S. 2904 would assist in accelerating the development of technological tools to examine the outputs of generative adversarial networks and encourage collaboration across public and private sectors.

Privacy

S. 2904, as amended, would have no further impact on privacy.

Paperwork

S. 2904, as amended, in section V would require the Directors of NSF and NIST to submit a joint report to Congress.

CONGRESSIONALLY DIRECTED SPENDING

In compliance with paragraph 4(b) of rule XLIV of the Standing Rules of the Senate, the Committee provides that no provisions contained in the bill, as reported, meet the definition of congressionally directed spending items under the rule.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title.

This section would provide that the bill may be cited as the "Identifying Outputs of Generative Adversarial Networks Act" or the "IOGAN Act".

Section 2. Findings.

This section would establish the current state of affairs regarding artificial intelligence and generative adversarial networks, the cur-

rent work conducted by NSF, and the potential for the development of new credible techniques.

Section 3. NSF support of research on manipulated or synthesized content and information security.

This section would require the Director of NSF, along with other Federal agencies, to support merit-reviewed research on manipulated or synthesized content and authenticity, which may include fundamental research on authenticity and detection technologies, identification technical tools, social and behavioral research, public perception and awareness research, and research awards coordinated with other Federal agencies.

Section 4. NIST support for research and standards on generative adversarial networks.

This section would require the Director of NIST to support research for the development of measurements and standards to examine the function and outputs of GAN or other manipulative technologies. The Director of NIST would be required to receive input from public, private, and academic stakeholders and consider the feasibility of ongoing engagement in the development of standards and measurements.

Section 5. Report on feasibility of public-private partnership to detect manipulated or synthesized content.

This section would require the Directors of NSF and NIST to submit a joint report to Congress, not later than 1 year after the date of enactment, detailing the feasibility for research opportunities with the private sector and any policy recommendations to facilitate and improve communication and coordination among the private sector, NSF, and other Federal agencies with respect to generative adversarial networks or other synthesizing and manipulative technologies.

Section 6. Generative adversarial network defined.

This section would define the term "generative adversarial network" for the purposes of this bill.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the Committee states that the bill as reported would make no change to existing law.

○