Calendar No. 197

116TH CONGRESS *1st Session*	SENATE	REPORT 116–93

DEEPFAKE REPORT ACT OF 2019

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 2065

TO REQUIRE THE SECRETARY OF HOMELAND SECURITY TO PUBLISH AN ANNUAL REPORT ON THE USE OF DEEPFAKE TECHNOLOGY, AND FOR OTHER PURPOSES

SEPTEMBER 10, 2019.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
89–010 WASHINGTON : 2019

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
JOSEPH C. FOLIO III, *Chief Counsel*
MICHELLE D. WOODS, *Co-Director and Chief Policy Advisor for Homeland Security*
DAVID M. WEINBERG, *Minority Staff Director*
ZACHARY I. SCHRAM, *Minority Chief Counsel*
MICHELLE M. BENECKE, *Minority Senior Counsel*
JEFFREY D. ROTHBLUM, *Minority Fellow*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 197

116TH CONGRESS *1st Session* | SENATE | REPORT 116–93

DEEPFAKE REPORT ACT OF 2019

SEPTEMBER 10, 2019.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 2065]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 2065) to require the Secretary of Homeland Security to publish an annual report on the use of deepfake technology, 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.

CONTENTS

I. PURPOSE AND SUMMARY

S. 2065, the Deepfake Report Act of 2019, requires the Secretary of Homeland Security to publish an annual report on the extent digital content forgery technologies, also known as deepfake technologies, are being used to weaken national security, undermine our nation's elections, and manipulate media.

II. BACKGROUND AND NEED FOR LEGISLATION

Advances in machine learning algorithms and artificial intelligence capabilities have accelerated the proliferation of digital con-

tent forgery technologies, commonly referred to as "deepfake technologies."[1] Deepfake technologies are used to manipulate audio, video or other media content and have the potential to be used to undermine national security, erode public trust in our democracy and other nefarious reasons.[2] As the software underpinning these technologies becomes easier to acquire and use, policy makers and national security experts are concerned that the continued dissemination of deepfake content across trusted media platforms could increasingly be used to dupe audiences and amplify false narratives about American cultural norms and interests domestically and abroad.[3]

Doctored videos of high-profile politicians and Facebook founder Mark Zuckerberg are prime examples of the disturbing impacts of the use of digital content forgeries.[4] The threat of weaponizing information, even without this powerful technology, becomes clear when considering the Russian influence campaigns carried out in recent U.S. elections.[5] The Intelligence Community concluded that Russia's Internet Research Agency placed false social media advertisements and manipulated content across various highly trafficked and trusted media platforms leading up to the 2016 and 2018 mid-term elections.[6]

In advance of the 2016 and 2018 mid-term elections, Facebook estimated that from January 2015 to August 2017, Russian-backed bots spread fabricated media content to about half of the 250 million eligible voters.[7] Moreover, Twitter discovered approximately "tens of thousands automated accounts" linked directly to Russia.[8] In an effort to limit the flow of disinformation on its platform, Twitter reportedly suspended more than 70 million accounts linked to Russian bots in May and June of 2018 and continued to do so throughout 2018.[9]

As cyber-enabled warfare increasingly becomes the norm, national security experts warn that if the Federal Government does not take swift action to address persistent purveyors of information warfare, deepfake technologies will only continue to become more

---

[1] Kristina Libby, *This Bill Hader Deepfake Video is Amazing. It's Also Terrifying for Our Future,* Popular Mechanics (Aug. 13, 2019), https://www.popularmechanics.com/technology/security/a28691128/deepfake-technology/.

[2] *Id.*

[3] Cuihua Shen, Mona Kasra, Wenjing Pan, Grace A. Bassett, Yining Malloch, and James F. O'Brien, *Fake Images: The Effects of Source, Intermediary, and Digital Media Literacy on Contextual Assessment of Image Credibility Online,* New Media & Society, Vol. 21, 2:pg. 238–463, SAGE Publications (2018), *available at* http://graphics.berkeley.edu/papers/Shen-FIT-2018-09/Shen-FIT-2018-09.pdf [hereinafter *Fake Images*], *The National Security Challenges of Artificial Intelligence, Manipulated Media, and 'Deepfakes': Hearing Before the U. S. House of Representatives, Permanent Select Committee on Intelligence,* 116th Cong., (2019) [hereinafter *HPSCI Hearing*] (statement of Clint Watts).

[4] Allyson Chiu, *Facebook Wouldn't Delete An Altered Video of Nancy Pelsoi. What about one of Mark Zukerberg?,* The Washington Post (June 12, 2019), https://www.washingtonpost.com/nation/2019/06/12/mark-zuckerberg-deepfake-facebook-instagram-nancy-pelosi/.

[5] Susannah George, *"Deepfakes" Called New Election Threat, With No Easy Fix,* Associated Press (June 13, 2019), https://www.apnews.com/4b8ec588bf5047a981bb6f7ac4acb5a7.

[6] *HPSCI Hearing, supra* note 3; Madeline Purdue, *Deepfake 2020: New Artificial Intelligence is Battling Altered Videos Before Elections,* USA Today (Aug. 14, 2019), https://www.usatoday.com/story/tech/news/2019/08/14/election-2020-company-campaigns-against-political-deepfake-videos/2001940001/.

[7] Oren Etzioni, *How Will We Prevent AI-Based Forgery,* Harvard Business Review (March 1, 2019), https://hbr.org/2019/03/how-will-we-prevent-ai-based-forgery.

[8] *Id.*

[9] Craig Timberg and Elizabeth Dwoskin, *Twitter is Sweeping Out Fake Accounts Like Never Before, Putting User Growth at Risk,* The Washing Post (July, 16, 2018), https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/.

sophisticated and widely used in disinformation campaigns launched by our nation's foreign adversaries, most notably China and Russia.[10] In June 2019, the U.S. House of Representatives Permanent Select Committee on Intelligence held a hearing entitled, "The National Security Challenges of Artificial Intelligence, Manipulated Media, and 'Deepfakes'".[11] During this hearing, witness Clint Watts, Distinguished Research Fellow, Foreign Policy Institute, stated that China and Russia will continue to use deepfake technologies to "discredit domestic dissidents and foreign detractors, incite fear and promote conflict inside Western-style democracies, and distort the reality of American audiences and audiences of American allies."[12] Mr. Watts further explained the dangers of the continued proliferation of deepfake technologies:

> Over the long term, deliberate development of false synthetic media will target U.S. officials, institutions and democratic processes with an enduring goal of subverting democracy and demoralizing the American constituency. In the near and short term, circulation of "Deepfakes" may incite physical mobilizations under false pretenses, initiate public safety crises and spark the outbreak of violence. The recent spate of false conspiracies proliferating via WhatsApp in India offer a relevant example of how bogus messages and media can fuel violence. The spread of "Deepfake" capabilities will likely only increase the frequency and intensity of such violent outbreaks.[13]

Federal entities, such as Defense Advanced Research Projects Agency, and academic institutions are conducting research on how to identify doctored media and counter deepfake technologies.[14] However, national security experts have identified a series of interim actions Congress and the private sector can take to counter the proliferation of deepfake media content and its adverse effects. Proposed actions to counter deepfake technologies and content include: implementing legislation prohibiting public figures from disseminating deepfake content, public-private partnerships to develop standards for content accountability, encouraging social media companies to develop digital signatures, and launching public awareness campaigns about deepfake content.[15]

The Federal Government should proactively identity the tools and techniques used by our adversaries to develop deepfake technologies and content, and develop countermeasures and tools to identify and counter deepfake content.

S. 2065 requires the Department of Homeland Security, in coordination with other Federal agencies, to develop a report on the use of digital content forgery technologies, and recommend actions and identify countermeasures to mitigate the impacts of these technologies on national security. The report is to include, among other things, an assessment of the technologies used to create or propagate digital content forgeries, a description of the types of digital

---

[10] *HPSCI Hearing, supra* note 3 (statement of Clint Watts); *Fake Images, supra* note 3.
[11] *HPSCI Hearing, supra* note 3.
[12] *Id.* (statement of Clint Watts).
[13] *Id.*
[14] Kristina Libby, *This Bill Hader Deepfake Video is Amazing. It's Also Terrifying for Our Future,* Popular Mechanics, (Aug. 13, 2019), https://www.popularmechanics.com/technology/security/a28691128/deepfake-technology/.
[15] *Id.; HPSCI Hearing, supra* note 3 (statement of Clint Watts); *Fake Images, supra* note 3.

content forgeries, how such technologies are being or could be used to undermine national security, and a description of the technological countermeasures that are, or could be, used to address concerns with digital content forgeries. In addition, the Secretary may consult with other Federal agencies and conduct public hearings to gather relevant information to assist with the production of the report.

The first report is due one year after the bill's enactment, and annually thereafter for five years. The report is to be provided in unclassified form, but may include a classified annex. Existing information and public disclosure exemptions under the Freedom of Information Act apply to the reports required by this bill. The bill also includes an exemption from the Paperwork Reduction Act.

III. LEGISLATIVE HISTORY

S. 2065, the Deepfake Report Act of 2019, was introduced on July 09, 2019, by Senator Rob Portman. Senators Martin Heinrich, Brian Schatz, Cory Gardner, Mike Rounds, Joni Ernst, and Gary Peters cosponsored the bill. Senator Margaret Wood Hassan later joined as a cosponsor. The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 2065 at a business meeting on July 24, 2019. During the business meeting, a substitute amendment by Senator Portman was offered and adopted. The substitute amendment added language to include a sunset provision, limit the scope of the report to ways that deepfakes are used to commit fraud, cause harm, and violate federal civil rights, and clarify applicability of Freedom of Information Act and Paperwork Reduction Act requirements. Both the amendment and the legislation as modified were passed by voice vote en bloc with Senators Johnson, Portman, Paul, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Sinema, and Rosen present.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section establishes the short title of the bill as the "Deepfake Report Act of 2019."

Section 2. Definitions

This section defines "digital content forgery" as 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. This section defines "Secretary" as the Secretary of Homeland Security.

Section 3. Reports on digital content forgery technology

Subsection (a) requires the Secretary, acting through the Under Secretary for Science and Technology to produce a report on the state of digital content forgery technology. The report is to be provided one year after the enactment of the Act, and annually thereafter for five years.

Subsection (b) specifies the required contents of the report. The report is to include: an assessment of the technologies used to create or propagate digital content forgeries; a description of the types

of digital content forgeries, including those used to commit fraud, to cause harm, or to violate civil rights; and an assessment of how foreign governments, and their proxies and networks, use or could use digital content forgeries to undermine national security; an assessment of deep learning technologies used to generate deepfakes to commit fraud, cause harm, or violate civil rights; an analysis of the effectiveness of methods used to identify deep fakes; and, recommendations for employing methods to identify deepfakes as well as effective public warning methods for specific content. The report should also include, among other things as deemed appropriate by the Secretary, a description of the technological countermeasures that are, or could be, used to address concerns with digital content forgeries.

Subsection (c) allows the Secretary to consult with any other Federal agency or other interested parties and conduct public hearings to gather information and advice relevant to complete the reports required by this bill.

Subsection (d) stipulates that the reports should be unclassified, but may contain a classified annex.

Subsection (e) states that information used to produce the reports required by this bill that are exempt from the requirements under section 552 of title 5, United States Code (commonly known as the "Freedom of Information Act") are to remain exempt.

Subsection (f) states that the reports required by this bill are exempt from Subchapter I of chapter 35 of title 44, United States Code (commonly known as the "Paperwork Reduction Act").

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, August 16, 2019.

Hon. RON JOHNSON,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2065, the Deepfake Report Act of 2019.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 2065, Deepfake Report Act of 2019

As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 24, 2019

By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	*	*

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 2030?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

S. 2065 would require the Department of Homeland Security (DHS) to submit five annual reports to the Congress on digital content forgeries, also known as "deepfakes." Such forgeries manipulate digital content, such as videos, with the intent to mislead the viewer. The bill would require DHS to assess the use of digital content forgeries by foreign entities and evaluate available methods of detecting and mitigating such threats.

On the basis of information from DHS and considering information about similar reporting requirements, CBO estimates that enacting S. 2065 would cost less than $500,000 over the 2019–2024 period. Such spending would be subject to availability of appropriated funds.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Assistant Director for Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

Because S. 1151 would not repeal or amend any provision of current law, it would make no changes in existing law within the meaning of clauses (a) and (b) of paragraph XXVI of the Standing Rules of the Senate.

○