Volume 3, No. 4 | July–August 2020

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Editor's Note: "Deepfakes"
Steven A. Meyerowitz

The Federal "Deepfakes" Law
Matthew F. Ferraro, Jason C. Chipman, and Stephen W. Preston

The Name Game: Practical Branding Tips for Robotics Companies
B. Brett Heavner and Yinfei Wu

U.S. Department of Commerce Imposes Immediate Export Controls on Artificial Intelligence Software Used to Automatically Detect and Identify Objects Remotely
John P. Carlin, Nicholas J. Spiliotes, Charles L. Capito, Joseph A. Benkert, Panagiotis C. Bayz, Amy S. Josselyn, and Jonathan M. Babcock

Connected and Autonomous Vehicles: A Cross-Jurisdictional Comparison of Regulatory Developments
Steven Baker, Christian M. Theissen, and Bijal Vakil

EU Issues White Paper Outlining Framework for Regulating Artificial Intelligence
K.C. Halm and Jonathan Mark

Everything Is Not *Terminator*: Exporting Our AI, Biggering Our Values
John Frank Weaver

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 3, No. 4 | July–August 2020

227 **Editor's Note: "Deepfakes"**
Steven A. Meyerowitz

229 **The Federal "Deepfakes" Law**
Matthew F. Ferraro, Jason C. Chipman, and Stephen W. Preston

235 **The Name Game: Practical Branding Tips for Robotics Companies**
B. Brett Heavner and Yinfei Wu

243 **U.S. Department of Commerce Imposes Immediate Export Controls on Artificial Intelligence Software Used to Automatically Detect and Identify Objects Remotely**
John P. Carlin, Nicholas J. Spiliotes, Charles L. Capito, Joseph A. Benkert, Panagiotis C. Bayz, Amy S. Josselyn, and Jonathan M. Babcock

249 **Connected and Autonomous Vehicles: A Cross-Jurisdictional Comparison of Regulatory Developments**
Steven Baker, Christian M. Theissen, and Bijal Vakil

275 **EU Issues White Paper Outlining Framework for Regulating Artificial Intelligence**
K.C. Halm and Jonathan Mark

281 **Everything Is Not *Terminator*: Exporting Our AI, Biggering Our Values**
John Frank Weaver

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

The Federal "Deepfakes" Law

Matthew F. Ferraro, Jason C. Chipman, and Stephen W. Preston*

The authors discuss the key provisions of a federal law relating to "deepfakes."

There now is a federal law relating to "deepfakes"—false yet highly realistic artificial intelligence-created media, such as a video showing people saying things they never said and doing things they never did. The deepfake legislation is part of the National Defense Authorization Act for Fiscal Year 2020 ("NDAA"), the $738 billion defense policy bill the president signed into law after it was passed by the Senate 86-8 and the House 377-48.[1]

In two provisions related to this emerging technology, the NDAA:

1. Requires a comprehensive report on the foreign weaponization of deepfakes;
2. Requires the government to notify Congress of foreign deepfake-disinformation activities targeting U.S. elections; and
3. Establishes a "Deepfakes Prize" competition to encourage the research or commercialization of deepfake-detection technologies.

Reporting and Notification

The first deepfake-related provision, Section 5709, imposes a reporting requirement and notification provision, both on the Director of National Intelligence ("DNI").

The law directs that within six months of its enactment, the DNI must submit to the Congressional Intelligence Committees an unclassified report on the potential national security impacts of deepfakes (what it calls "machine-manipulated media" and "machine-generated text") and the actual or potential use of them by foreign governments "to spread disinformation or engage in other malign activities." The DNI is to submit to Congress any significant updates to this report annually.

Robotics, Artificial Intelligence & Law / July–August 2020, Vol. 3, No. 4, pp. 229–233.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

The report, which the DNI is to write in consultation with the heads of the elements of the U.S. Intelligence Community ("IC") that he or she determines appropriate, is to include:

- An assessment of the technical capabilities of foreign governments regarding deepfakes. The law specifically directs the assessments of the technical capabilities of China and Russia. It also directs the DNI to prepare an annex, which may be classified, describing Chinese and Russian governmental elements and private sector, academic, or nongovernmental entities that support or facilitate deepfake research and development or dissemination.
- An updated assessment of how foreign governments, foreign government-affiliated entities, or foreign individuals could use or are using deepfakes to harm U.S. national security interests with respect to "the overseas or domestic dissemination of misinformation," "the attempted discrediting of political opponents or disfavored populations," and "intelligence or influence operations" targeting the United States, allies, or jurisdictions that are believed to be subject to Chinese or Russian interference. Ukraine, for instance, would likely fall into this latter category.
- An assessment of the technologies that can counter deepfakes that have been or could be developed by the U.S. government "*or by the private sector with Government support*, to deter, detect, and attribute the use of" deepfakes by foreign adversaries.[2] This assessment must include "any emerging concerns related to privacy."
- A description by the DNI of the IC offices that have or should have the lead responsibility for monitoring the development and use of deepfakes. The DNI must describe in detail the IC's current capabilities and research geared to detect deepfakes, including the speed and accuracy of those assessments.
- A description of any research and development activities being considered or carried out across the IC.
- A list of updated recommendations regarding whether the IC needs additional legal authorities, resources, or personnel to address the deepfake threat.

Second, Section 5709 also requires the DNI to notify the Congressional Intelligence Committees "each time" the DNI determines

there is credible intelligence that a foreign entity has or is deploying deepfakes "aimed at the elections or domestic political processes of the United States." The DNI must also notify Congress if the disinformation campaign can be attributed to a foreign government, entity, or individual.

Competition

Section 5724 of the NDAA establishes a deepfakes competition run by the DNI "to award prizes competitively to stimulate the research, development, *or commercialization* of technologies to automatically detect machine-manipulated media."[3]

The NDAA authorizes the DNI to award up to $5 million total to one or more winners.

Other Bills

While the NDAA was the first bill to become law that contains sections related to deepfakes, two further bills have each passed one Congressional chamber and remain pending in the other.[4]

The Identifying Outputs of Generative Adversarial Networks ("IOGAN") Act[5] was adopted by the House by voice vote on December 9, 2019, and remains pending in the Senate. The IOGAN Act would direct the Director of the National Science Foundation ("NSF") to support "merit-reviewed and competitively awarded research on manipulated or synthesized content and information authenticity." Such research may include fundamental research on technical tools for verifying the authenticity of information and identifying manipulated media, social, and behavioral research on the ethics of the technology, and research on public understanding and awareness of deepfakes and best practices for public education.

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 the 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 of 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.

The Deepfake Report Act of 2019[6] passed the Senate on October 24, 2019, by unanimous consent and remains pending in the House. The bill would direct the Department of Homeland Security to issue a report within one year of enactment and every year for five years thereafter on deepfake technology—what it refers to as "digital content forgery technology." Among other things, the report would describe the kind of deepfakes that are used to commit fraud, cause harm, and violate federal civil rights; assess the harm of deepfakes to individuals; and assess methods to detect and counter such forgeries.

Other Deepfakes Laws

The NDAA caps a busy year for legislating in this emerging field. In 2019, two states enacted laws criminalizing certain deepfakes. Virginia became the first state in the nation to impose criminal penalties on the distribution of nonconsensual deepfake pornography. The law, which went into effect on July 1, 2019, made the distribution of nonconsensual "falsely created" explicit images and videos a Class 1 misdemeanor, punishable by up to a year in jail and a fine of $2,500.

On September 1, 2019, Texas became the first state in the nation to prohibit the creation and distribution of deepfake videos intended to harm candidates for public office or influence elections. The Texas law 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." It makes it a Class A misdemeanor, punishable by up to a year in the county jail and a fine of $4,000, 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."

California enacted two laws in October 2019 that, collectively, allow victims of nonconsensual deepfake pornography to sue for damages and give candidates for public office the ability to sue individuals or organizations that distribute "with actual malice" election-related deepfakes without warning labels near Election Day.

As the experience of the past year shows, the legislation in this area is changing rapidly as policymakers wrestle with new and emerging deepfake-related threats to national security, individuals, and businesses.

Notes

* Matthew F. Ferraro (matthew.ferraro@wilmerhale.com) is a counsel in the Washington, D.C., office of Wilmer Cutler Pickering Hale and Dorr LLP. Jason C. Chipman (jason.chipman@wilmerhale.com) and Stephen W. Preston (stephen.preston@wilmerhale.com) are partners in the firm's Washington, D.C., office.

1. S. 1790, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/1790/actions?KWICView=false. The deepfake-related provisions were originally part of a standalone bill, "The Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018, 2019, and 2020," which was incorporated into the NDAA.
2. Emphasis added.
3. Emphasis added.
4. Several other bills on this topic remain under consideration in various committees.
5. H.R. 4355, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/house-bill/4355/actions?KWICView=false.
6. S. 2065, 116th Cong. (2019), *available at* https://www.congress.gov/bill/116th-congress/senate-bill/2065/actions?KWICView=false.