Volume 4, No. 4 | July–August 2021

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL

The Journal of Robotics, Artificial Intelligence & Law

Volume 4, No. 4 | July–August 2021

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. Copyright 2021 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

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 8 a.m.–8 p.m. 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)

FBI Warns Companies of "Almost Certain" Threats From Deepfakes

Matthew F. Ferraro, Jason C. Chipman, and Benjamin A. Powell*

The Federal Bureau of Investigation issued a Private Industry Notification advising companies on what are commonly referred to as "deepfakes." The authors of this article explain the notification and offer tips to guard against deepfake risk.

On March 10, 2021, the Federal Bureau of Investigation ("FBI" or "Bureau") issued a private industry notification ("PIN")[1] advising companies that "[m]alicious actors almost certainly will leverage synthetic content for cyber and foreign influence operations in the next 12-18 months."

Deepfakes

The FBI's stark warning—a first related to what are commonly referred to as "deepfakes"[2] (synthetic media that is either wholly created or altered by artificial intelligence or machine learning)—comes amid rising awareness of the prevalence and potential dangers of disinformation in general,[3] and highly realistic phony media in particular. For example, in February, believable deepfake videos of Tom Cruise appearing to play golf, walk through a store, and do a magic trick went viral online, suggesting that the era of nearly "flawless forgeries"[4] has arrived.

The Notification

The FBI wrote in its notification that foreign actors are already using synthetic content in influence campaigns. The Bureau anticipates that artificial intelligence–enabled phony media will be used increasingly by "foreign and criminal cyber actors for spearphishing and social engineering" crimes. (Spearphishing refers to when a

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

fraudster sends emails ostensibly from a known or trusted sender to induce a target to reveal confidential information or gain access to an otherwise closed network.)

Specifically, the Bureau notes that Russian, Chinese, and Chinese-language actors are already using synthetic profile images to make fake online accounts, known as sockpuppets,[5] appear authentic and to push foreign propaganda campaigns. The FBI also advises that actors of unknown origin have posed as "journalists" using manufactured profile images and have pushed fake articles that legitimate media outlets have picked up and amplified.

The FBI warns that malicious cyber actors will not just push propaganda on behalf of foreign actors but also leverage synthetic media and deepfakes to attack the private sector. In particular, the FBI warns that synthetic content may be used in a "newly defined cyber attack vector" called "business identity compromise" ("BIC"), where deepfake tools will be employed to create "synthetic corporate personas" or imitate existing employees and will likely cause "very significant financial and reputational impacts to victim businesses and organizations."

These threats represent an evolution in business email compromise ("BEC") schemes, which occur when a hacker compromises a corporate email account to facilitate fraudulent financial transactions.

Tips to Guard Against Deepfake Risk

To guard against the evolving dangers of deepfakes, the FBI provides several tips for individuals and organizations. These include the following:

- Establish good information hygiene: multifactor authentication, training to identify attempts at social engineering and spearphishing, and caution when providing sensitive personal or corporate information digitally, among others.
- Train employees to use the SIFT media resiliency framework, which encourages individuals to Stop, Investigate information's source, Find trusted coverage, and Trace the original content.
- Review profile photos of online accounts closely for visual clues of falsity, including visual distortions around pupils

and earlobes, indistinct and blurry backgrounds, and random distortions or visual artifacts.

- Establish and practice a communications continuity plan in the event social media accounts are compromised.

The FBI encourages the public to report information concerning suspicious or criminal cyber activity or malign foreign actors to their local FBI field office[6] or the FBI's 24/7 Cyber Watch.[7]

Because of the threats posed by BEC intrusions, many organizations over the past several years have taken steps to protect their treasury functions and their accounts payable from manipulation that can occur when hackers take control of a trusted company email account. The potential for deepfake technology to create a new category of BIC activities threatens to complicate company authentication protocols.

Companies may want to revisit their security practices in the face of these intensifying challenges to information security. Unfortunately, this is just one of the many new risks facing businesses from the growing believability and accessibility of deepfakes and the spread of disinformation and conspiracy theories more generally. These risks range from reputational harm to fraud, market manipulation, and credential theft, among others.

Notes

* Matthew F. Ferraro is counsel at Wilmer Cutler Pickering Hale and Dorr LLP advising clients on matters related to defense and national security, cybersecurity, and crisis management. Jason C. Chipman is a partner at the firm handling complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States and related export controls. Benjamin A. Powell is a partner at the firm and co-chair of its Cybersecurity and Privacy Practice handling cybersecurity, data breach, and related investigation matters. The authors may be reached at matthew.ferraro@wilmerhale.com, jason.chipman@wilmerhale.com, and benjamin.powell@wilmerhale.com, respectively.

[1] *Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations*, FBI Private Industry Notification (Mar. 10, 2021), https://www.documentcloud.org/documents/20509703-fbipin-3102021.

[2] Matthew F. Ferraro, *Decoding Deepfakes*, National Security Institute Backgrounder (Dec. 1, 2020), https://nationalsecurity.gmu.edu/ddf/.

[3] Shannon Vavra, *FBI Alert Warns of Russian, Chinese Use of Deepfake Content*, Cyber Scoop (Mar. 10, 2021), https://www.cyberscoop.com/fbi-foreign-actors-deepfakes-cyber-influence-operations/.

[4] Emma Bowman, *Slick Tom Cruise Deepfakes Signal That Near Flawless Forgeries May Be Here*, NPR (Mar. 11, 2021), https://www.npr.org/2021/03/11/975849508/slick-tom-cruise-deepfakes-signal-that-near-flawless-forgeries-may-be-here.

[5] *Sockpuppet*, Techopedia, https://www.techopedia.com/definition/29043/sockpuppet.

[6] *See* Field Offices, FBI, https://www.fbi.gov/contact-us/field-offices.

[7] FBI's 24/7 Cyber Watch can be contacted at: cywatch@fbi.gov.