Volume 3, No. 5 | September–October 2020

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 3, No. 5 | September–October 2020

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)

"Deepfakes" Pose Significant Market Risks for Public Companies: How Will You Respond?

Thaddeus D. Wilson, William T. Gordon, Aaron W. Lipson, and Brian M. Thavarajah*

The authors explain that, for public companies and their officers and directors, the nefarious use of "deepfakes" presents potentially great legal and financial challenges because of possible illegal attempts at market manipulation.

"Deepfakes" and related artificial intelligence technology pose substantial corporate compliance risks for financial institutions and companies alike. Proactive updates to compliance programs and technology together with vigilance can help protect against theft attempts and related schemes by cybercriminals.

"Deepfakes"

For public companies and their officers and directors, however, the nefarious use of "deepfakes" presents potentially greater legal and financial challenges because of possible illegal attempts at market manipulation. Many public company directors and officers speak frequently in investor calls, media interviews, industry conferences, and community events—usually leaving behind a trail of recorded video and audio. Consequently, these individuals are actively creating source materials allowing them to become the subject of a "deepfake." Bad actors may well use now freely available technologies to mine libraries of publicly available audiovisual records to create "deepfakes" that mimic statements by public company directors and officers.

The adverse effects of the use of a "deepfake" in this context could be considerable for a company and its shareholders. Not only could it trigger an investigation by the Securities and Exchange

Robotics, Artificial Intelligence & Law / September–October 2020, Vol. 3, No. 5, pp. 337–340.

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

Commission ("SEC"), the Federal Bureau of Investigation ("FBI") or other law enforcement agencies, but it could also result in shareholder lawsuits and fiduciary duty litigation. The following simple scenario highlights some of the challenges such a "deepfake" might raise.

Challenges for Public Companies

It is not hard to imagine a video clip showing two chief executive officers shaking hands and congratulating themselves and their companies on the future they will share together, as they publicly disclose for the first time an agreed-to tender offer. As the video clip makes its way across social media platforms, financial news aggregators, and even websites apparently connected with the issuers, the share price of the offeree skyrockets up 40 percent to just below the announced tender price. Normally these events are cause for celebration for the two issuers.

But in this case, no tender offer actually exists. A criminal enterprise has crafted a "deepfake" video by utilizing a treasure trove of public statements and recordings available on investor relations websites, corporate social media, and throughout the internet. Shortly before going live, the criminal enterprise invested in deep, out-of-the-money call options for the tender target, and perfectly timed its exit with the strike price having been reached. By the time the two public companies have responded, exchange circuit breakers have been tripped and confusion and a lack of confidence in each issuer's information results in the share prices falling below recent trading levels. Consequently, these public companies face an onslaught of adverse media requests and investigative activity from the SEC, Financial Industry Regulatory Authority ("FINRA"), and likely criminal law enforcement as well. Existing shareholders are likely to suffer harm, and potential shareholder derivative lawsuits may even follow.

Although somewhat fantastical, the age of "deepfake" market manipulation is likely right around the corner. Market manipulations require the public dissemination of information—often false, positive information—to succeed. And there is analogous SEC precedent resulting from market manipulation schemes that is instructive.

Recent SEC actions[1] have centered around the exploitation of the SEC's EDGAR website to file fake tender offer notices for the

purpose of artificially inflating the share price of publicly traded companies and, consequently, benefitting previously held trading positions by the perpetrators. Organized market manipulation rings are oftentimes willing to "invest" large sums to send spam email blasts, commission fake analyst reports, paper a message board with touts, mail glossy hardcopy materials, or bankroll a boiler room.

The move to "deepfake" technology by more sophisticated manipulation rings—with the potential for a greater positive market "bang" with a much smaller promotional cost—is likely a question of when and not if. The ability to combat these fakes by corporate victims and regulators will be challenging. For one, "deepfakes" of public company executives could gain much broader dissemination among investors and in the press than a regulatory filing, especially when dealing with exciting, or even embarrassing (in an effort to drive down the price to support short activity), statements or conduct. Additionally, depending on the sophistication of a "deepfake," companies may need time, and possibly the assistance of outside experts, to confirm that the released content does not reflect authentic remarks or conduct of an executive. Those steps could lead to a greater lag before the company can make subsequent corrective disclosures, thereby potentially expanding the period of stock price manipulation. Additionally, for those companies whose Twitter, Facebook, or corporate website are susceptible to being hacked, market manipulators are likely to look to those channels as a preferred means of distribution.

Conclusion

As illustrated by the example, "deepfakes" have the potential to create substantial issues for public companies and their directors and officers, including investigations and litigation. Accordingly, public companies would be well served to work with their legal and public relations advisors to revise their crisis management plans to address potential scenarios involving "deepfakes."

Notes

* Thaddeus D. Wilson (thadwilson@kslaw.com) and Aaron W. Lipson (alipson@kslaw.com) are partners in the Atlanta office of King & Spalding LLP. William T. Gordon (bgordon@kslaw.com) is a partner in the firm's office

in Houston. Brian M. Thavarajah (bthavarajah@kslaw.com) is counsel in the firm's Washington, D.C., office.

1. SEC Lit. Rel. No. 24204, July 17, 2018 (action alleging use of a fake tender offer filing to manipulate the price of Fitbit shares); *SEC v. PTG Capital Partners LTD, et al.*, 15-CV-04290, (S.D.N.Y.) (June 4, 2015) (action alleging use of a fake tender offer filing to manipulate the price of Avon shares).