



---

**PROGRAM MATERIALS**

**Program #3244**

**February 11, 2022**

# **Fake News, Real Costs: How Disinformation and Deepfakes Impact Business and What to Do About It**

**Copyright ©2022 by**

- **Matthew F. Ferraro, Esq. - Wilmer Cutler Pickering  
Hale and Dorr LLP**

**All Rights Reserved.  
Licensed to Celesq®, Inc.**

---

**Celesq® AttorneysEd Center**  
**[www.celesq.com](http://www.celesq.com)**

**5301 North Federal Highway, Suite 150, Boca Raton, FL 33487  
Phone 561-241-1919**

# Fake News, Real Costs How Disinformation and Deepfakes Impact Business and What to Do About It

**Thomson Reuters / Celesq**

February 11, 2022

**Matthew F. Ferraro**

[Matthew.Ferraro@wilmerhale.com](mailto:Matthew.Ferraro@wilmerhale.com)

Twitter: @MatthewFFerraro

# Overview

- Central Concepts:

- (1) Disinformation is also a growing threat to business
- (2) “Deepfakes” will make this problem much worse
- (3) Disparate issues you’ve been reading about—viral narratives (anti-vaxx, voter ‘fraud’, QAnon, &c.), synthetic media (Tom Cruise deepfakes, audio frauds, &c.)—form a cohesive issue (“**information disorder**”) requiring innovative counsel

- What’s the answer? ***Disinformation and Deepfakes Risk Management (DDRM)***

- Disinformation and deepfakes can harm corporate brands, manipulate the markets, and harm valuations
- Companies should embrace strategies of prevention and mitigation that range from awareness and intelligence gathering on the front end to counter-communications and litigation on the back end
- Lawyers will play the central role in dealing with these issues.

# Agenda

- 1. Definitions & Background**
- 2. Disinformation Dangers**
- 3. Risk Management Responses**
- 4. Disinformation, Deepfakes, and the Law**
- 5. Deepfakes at the Bar**
- 6. Positive-use Cases for Deepfakes**
- 7. Questions**

# Definitions & Background

What Are We Talking About?

# Defining Terms

- ***Disinformation*** is when false information is knowingly shared to cause harm (intent here is key)
- ***Misinformation*** is when false information is shared, but no harm is meant
- ***Malinformation*** is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere
  - Revenge porn, doxing, etc.
- ***Information Disorder*** is all the above together, “information pollution on a global scale,” says CoE

# Truth Decay

America's current era of Truth Decay is defined in part by an increasing disagreement about objective facts that exists on scale not observed in previous periods. For example, despite having more evidence than ever before about vaccines being safe and effective at preventing disease, vaccine skepticism in the United States is on the rise.

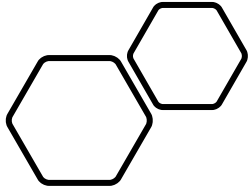
This is just one example of how public attitudes can diverge from facts and data in debates and discourse. So what's behind the decline?

RAND researchers have identified four main drivers:

1. cognitive biases
2. changes to the information ecosystem, including the rise of social media and changes in the economics of news
3. demands on the educational system that slow its ability to adapt to changes in the information ecosystem
4. political and social polarization

Without a common set of facts, it will be challenging to make progress on any of the major issues facing the country: COVID-19, healthcare, immigration, climate change, poverty and homelessness, and many others. Policymakers need shared facts and data to debate priorities and tradeoffs and to make effective policy decisions.

At the individual level, the diminishing role of facts can erode public trust in institutions, feed deepening political and other types of polarization, weaken or displace the meaningful civil discourse required for a healthy democracy, and contribute to alienation and disengagement. Furthermore, a rejection of facts can have immediate consequences for individuals. In the case of COVID-19, for example, rejecting facts about the disease and how it spreads can lead to health complications and even death.



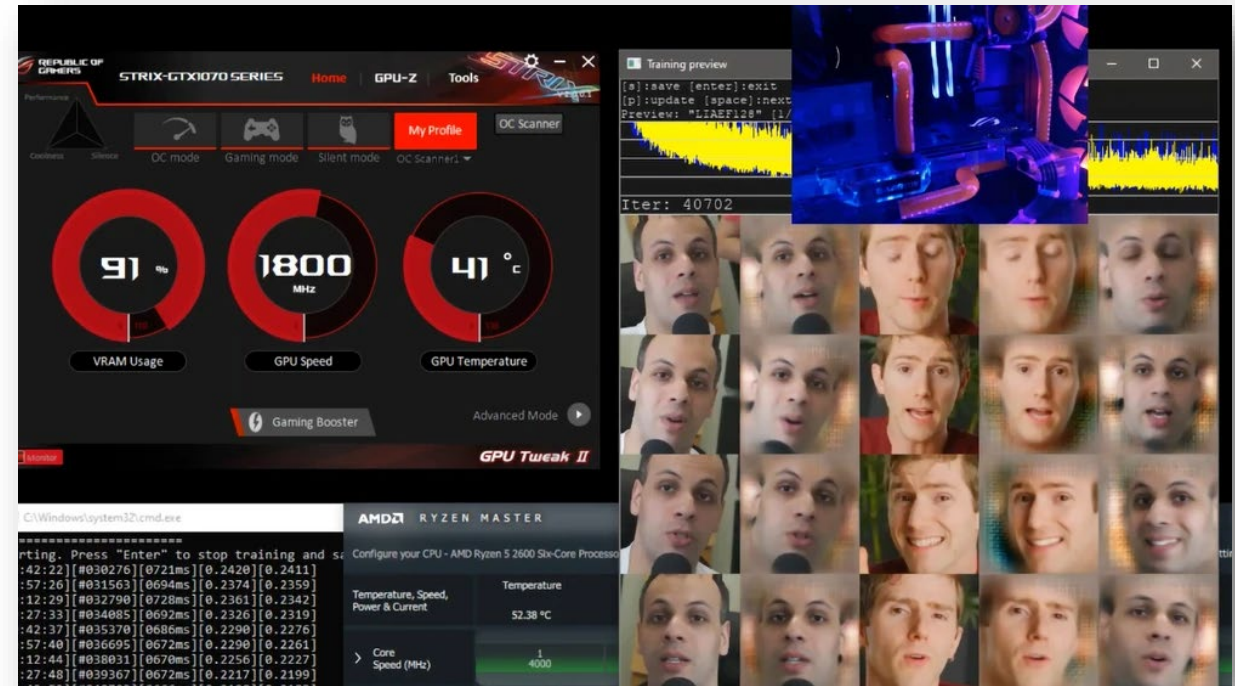
# What are Deepfakes?

- Deep Fakes (“deep learning” + “fake”)
- Synthetic media (text, images, audio, video) that is either manipulated or wholly generated by Artificial Intelligence (AI)
- Becoming essentially indecipherable to human eye
- As of 2020, there were more than 100 million deepfake videos online, which represented a year-over-year growth rate of 6,820%



# How Deepfakes Are Made

- Two computers compete in what's called a "Generative Adversarial Network" (GAN)
- One computer algorithm creates the fake media
- The other tries to detect it
- The competition continues until one computer cannot tell if the forgery is real or not



Source: [Vice](#)

# Liar's Dividend

- Profs. Citron & Chesney coined “liar’s dividend”:
- *Liars seize on deepfakes to cast doubt on real evidence of their wrongdoing.*
  - “Put simply: a skeptical public will be primed to doubt the authenticity of real audio and video evidence. This skepticism can be invoked just as well against authentic as against adulterated content.” 107 Cal. L. Rev. 1753, 1785 (2019)
- The dividend accrues to the liar.

LOCKER ROOM TALK

**TRUMP NOW SAYS THE ACCESS HOLLYWOOD TAPE MAY BE  
FAKE**

Source: [Vanity Fair](#)

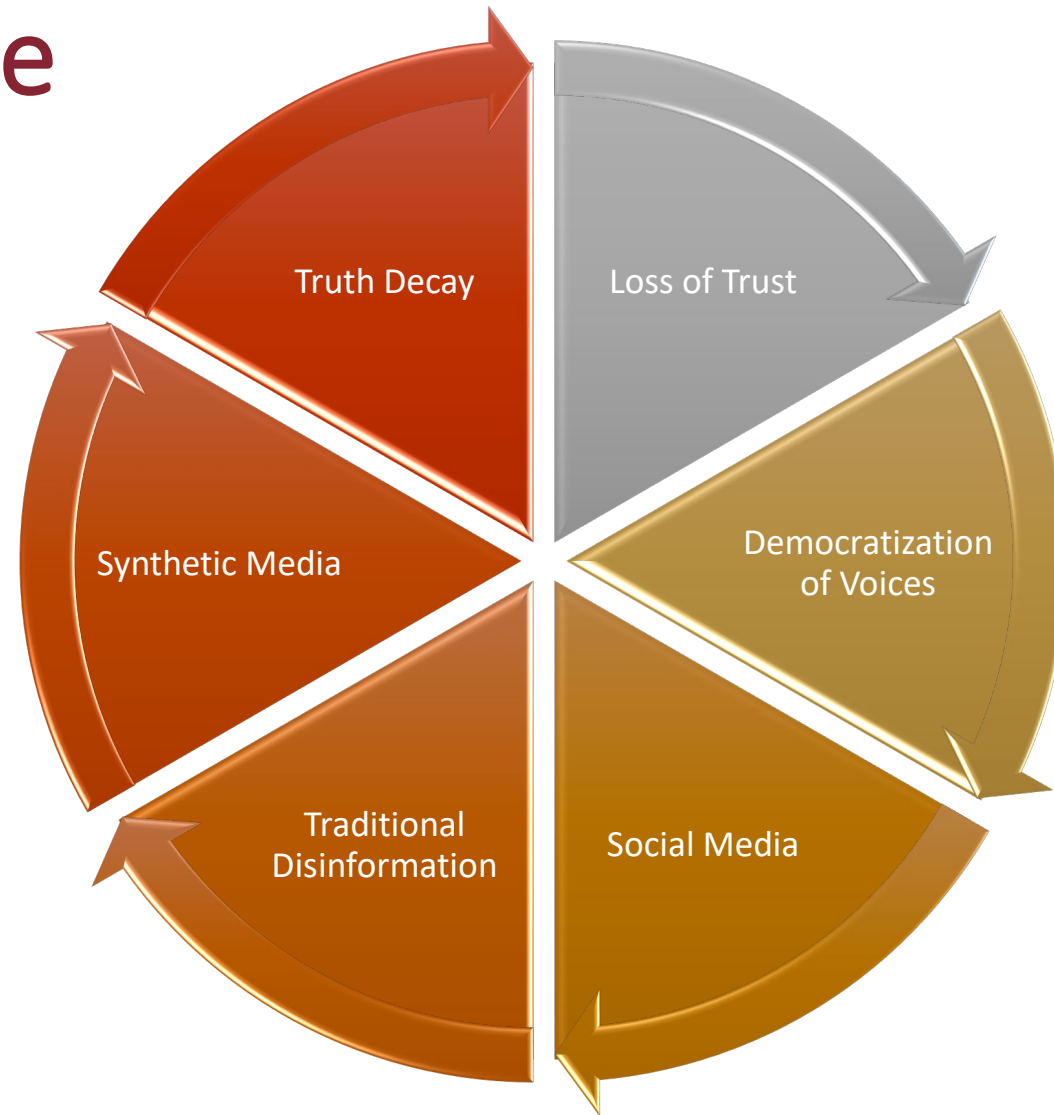
# Zealot's Dividend



Source: [Second Nexus](#)

- Coined by yours truly:
- ***Zealot's dividend*** describes the phenomenon when zealots or partisans dismiss inconvenient media evidence as manipulated or a deepfake that does not fit within their chosen narratives.

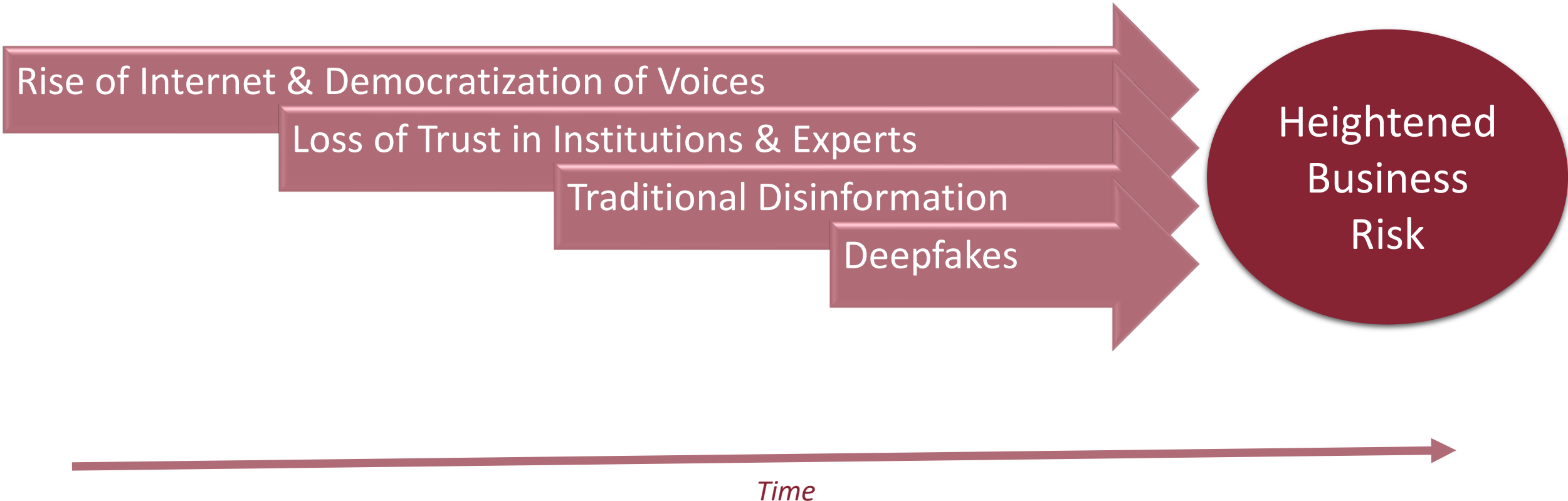
# Vicious Cycle



# Disinformation Dangers

Fake Narratives and Deepfakes Pose Rising Risks to Business

# Dynamic Environment for Business



# Businesses in Danger

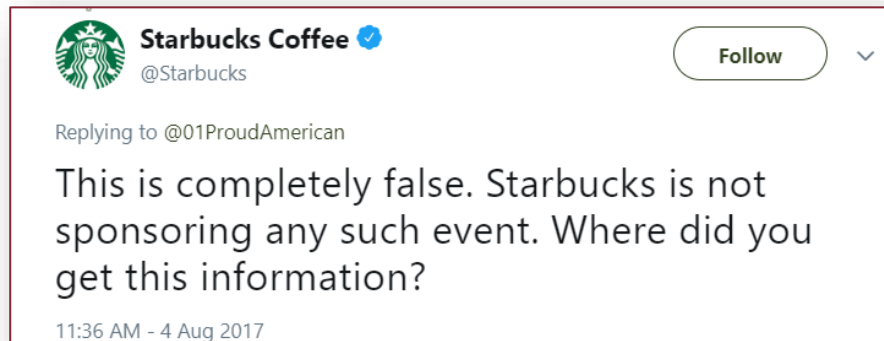
- Brunswick Group: **88%** of investors consider disinformation attacks on corporations a serious issue.
- Nov. 2019 study by cybersecurity firm CHEQ & University of Baltimore economist Robert Cavazos: **\$78 billion** each year is lost by firms due to disinformation.
  - Includes \$9 billion that companies and individuals spend every year trying to repair damaged reputations due to disinformation.
  - \$17 billion a year on financial disinformation.
  - Platforms spend \$3 billion a year trying to combat misinformation and on safety.

# Top Business Risks

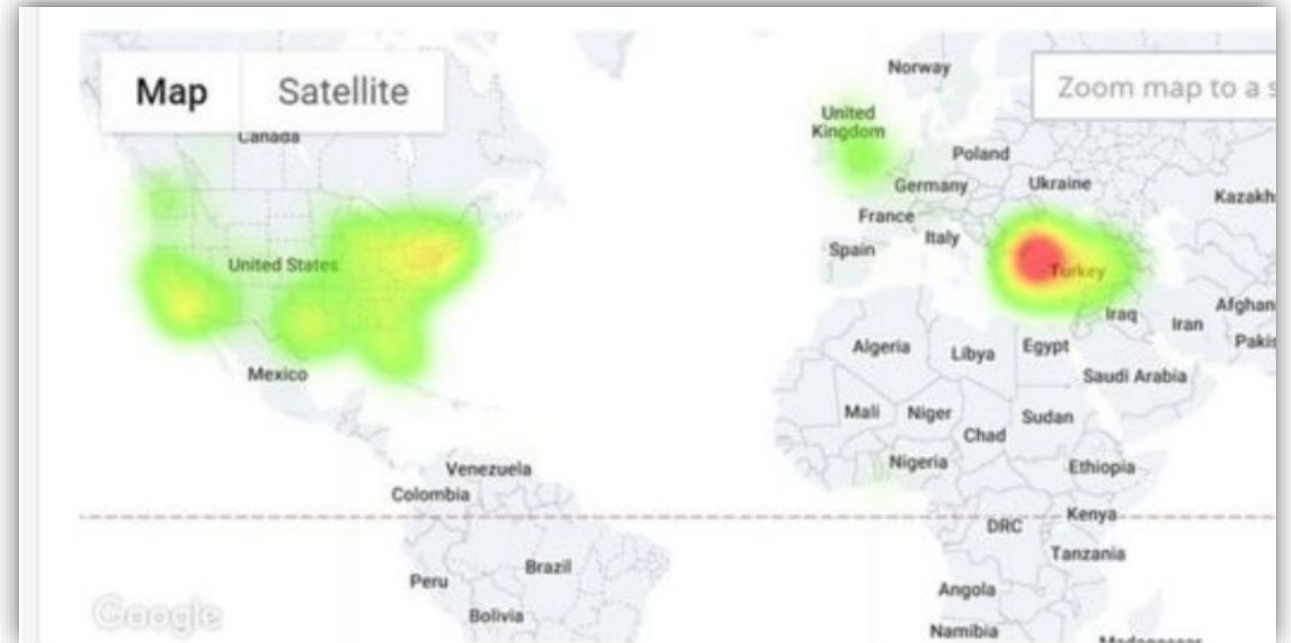
- ***Reputational Risk***
- ***Market Manipulation***
- ***Social Engineering Fraud***

# Reputational Risk – Starbucks

- In August 2017, someone on 4Chan said he wanted to inflict pain on a “[liberal place](#)”.
- Launched campaign against **Starbucks**.
- Posted bogus tweets advertising a “**Dreamer Day**” offering free drinks to undocumented immigrants.



# Reputational Risk – Wayfair



- QAnon-spread theory that Wayfair furniture seller is connected with child sex trafficking because of the coincidental overlap of the names of some of its pieces and of missing children.

# Reputational Risk – Vaccines

OPINION / EDITORIAL

## Why were US media silent on Pfizer vaccine deaths?: Global Times editorial

By Global Times

Published: Jan 15, 2021 08:00 PM



- China's Sinovac faced questions over the efficacy of its coronavirus vaccine.
- In response, PRC propaganda responded not by establishing its effectiveness, but by attacking reputation of US company Pfizer's vaccine and making misleading statements about risk factors ([CNN](#)).
- [In an editorial](#) on Jan. 15, the PRC's Global Times accused English-language media of "downplaying" deaths in Norway it appeared to claim were linked to vaccines, "as if they had already reached a consensus." The editorial said, "those major Western media will immediately hype any unfavorable information about Chinese vaccines and try to amplify their impact on public psychology."

# Reputational Risk –5G

- RT America has aired a series of deceptive reports on the dangers of 5G technology.
- RT has linked 5G signals to brain cancer, infertility, autism, heart tumors and Alzheimer's disease
- These claims ***“lack scientific support.”*** (N.Y. Times)
- Effort to sow doubt about America's future high-technology dominance.



# Reputational Risk – Huawei



Fake Twitter profiles supporting Huawei, a Chinese company that faced government restrictions in the West.

- In Dec. 2020, a Belgian trade lawyer wrote an article for Huawei attacking an anti-Huawei law
- Fake telecom “experts” retweeted the article
- Huawei then retweeted the fake accounts
- Millions of views

# Coming Soon? – Deepfake of bad boy CEO?

**Tesla stock closes down 6% after top executives resign and Elon Musk smokes weed on video**

PUBLISHED FRI, SEP 7 2018.9:38 AM EDT | UPDATED FRI, SEP 7 2018.7:32 PM EDT

What if next time it's fake and planned?



Elon Musk smokes marijuana with Joe Rogan's during a taping of Rogan's podcast show.

Source: YouTube

Source: [CNBC](#)

# Market Manipulation – Pump & Dump

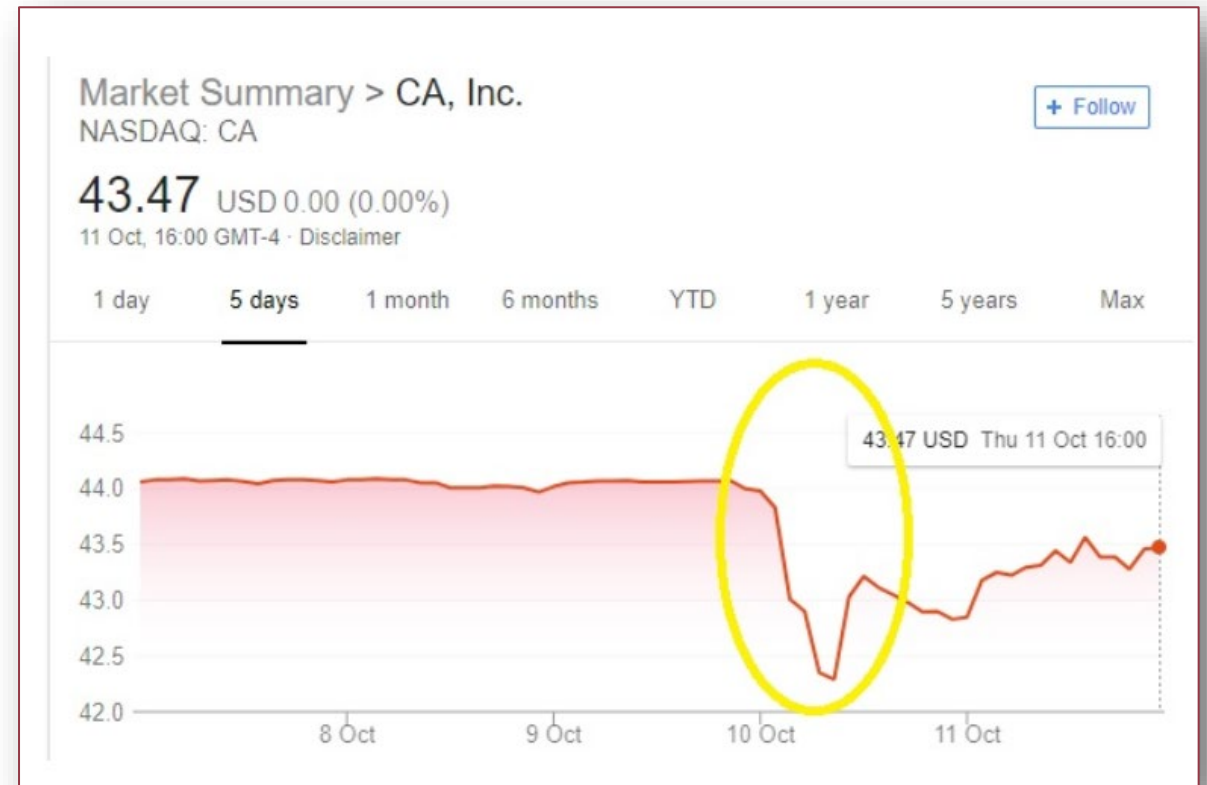
## SEC Charges Former Day Trader with Market Manipulation Scheme

Litigation Release No. 24989 / December 18, 2020

- In December 2020, the Securities and Exchange Commission (SEC) [charged](#) a Georgia man and several others for pushing mergers and acquisitions rumors through false online posts that temporarily goosed the companies' stocks
- Defendants profited from the jump in prices to the tune of ~\$36,000 in illicit profits
- These crimes are likely to be *more* damaging once malefactors leverage believable fake media to help sink or stoke equities.

# Market Manipulation – Short Sellers

- **Broadcom** announced its intention to acquire **CA Technologies** for \$19 billion.
- **Phony memo** circulated online supposedly from DoD saying US Government would review deal.
- Shares of both co's dropped.
- Called ***“a new phase of short-seller espionage.”***



# Social Engineering Fraud – Hong Kong Bank

EDITORS' PICK | Oct 14, 2021, 07:01am EDT | 78,580 views

## Fraudsters Cloned Company Director's Voice In \$35 Million Bank Heist, Police Find

- In January 2020, a bank manager in Hong Kong received a call from the director of a company whose voice he recognized
- The caller asked the banker to authorize financial transfers of \$35 million to finance an acquisition.
- Only later did the manager learn that he had been defrauded by “deep voice” technology, which impersonated the voice of the director in an advanced form of social engineering

# Social Engineering Fraud – UK Company

- In [March 2019](#), a UK CEO thought he was speaking to the company's German parent's CEO; UK CEO wired \$243,000 as requested.
- Realized later it was a deepfake voice forgery of German CEO.
- Newest variant of “business email compromise”.

## THE WALL STREET JOURNAL.

PRO CYBER NEWS

### **Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case**

Scams using artificial intelligence are a new challenge for companies

# Social Engineering Fraud – FBI Warning



## **Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations**

### **Summary**

Malicious actors almost certainly will leverage synthetic content for cyber and foreign influence operations in the next 12-18 months. Foreign actors are currently using synthetic content in their influence campaigns, and the FBI anticipates it will be increasingly used by foreign and criminal cyber actors for spearphishing and social engineering in an evolution of cyber operational tradecraft.

# Risk Management Responses

Disinformation and Deepfakes Risk Management (DDRM)

# What can businesses do?

## **Elite Eight (1 - 4)**

- 1. Proactively communicate your message**
- 2. Engage in social listening**
- 3. Do a self-assessment**
- 4. Register your trademarks & copyrights**

# What can businesses do?

## Elite Eight (5 - 8)

- 5. Prepare
- 6. Engage with social media platforms
- 7. Communicate your message
- 8. If necessary, go to court

# Disinformation, Deepfakes and the Law

An Evolving Area

# Potential Causes of Action

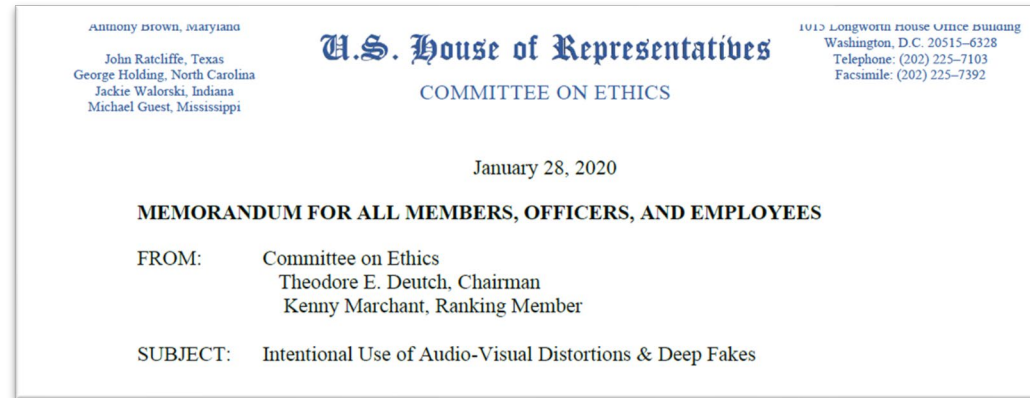
- Defamation
- Deceptive Trade Practices
- Intellectual Property Law
- False Light
- Right of Publicity
- Intentional / Negligent Infliction of Emotional Distress



# Solutions Beyond Law - Other Forms of Regulation

- Administrative Rulemaking
  - SEC, FCC, FTC, FEC
- Intellectual Property Regulating Bodies
  - WIPO, USPTO – considering who owns a deepfake?
- Rules of Evidence / State Bar Associations
  - E.g., Penalties for lawyers submitting deepfakes as evidence
- Unions and Guilds
  - E.g., SAG-AFTRA
- Ethics-Enforcing Professional Bodies

# E.g., House Committee on Ethics Guidance on Deepfakes



However, intentional distortions of audio and/or visual representations can be far more damaging. Members have a duty, and a First Amendment right, to contribute to the public discourse, including through parody and satire. However, manipulation of images and videos that are intended to mislead the public can harm that discourse and reflect discredibly on the House. Moreover, Members or their staff posting deep fakes<sup>3</sup> “could erode public trust, affect public discourse, or sway an election.”<sup>4</sup> Accordingly, Members, officers, and employees posting deep fakes or other audio-visual distortions intended to mislead the public may be in violation of the Code of Official Conduct.<sup>5</sup> Prior to disseminating any image, video, or audio file by electronic means, including social media, Members and staff are expected to take reasonable efforts to consider whether such representations are deep fakes or are intentionally distorted to mislead the public.

# State of Laws on Deepfakes

- Lawmaking on deepfakes is moving fast
- Within the past two years alone:
  - Seven (7) states have adopted laws barring some deepfakes
  - Federal government has adopted four (4) laws on deepfakes, focusing on reporting, Congressional notification, and research
- ~10 other bills pending in Congress
- ~20 Bills pending in ~12 states

# Themes

Nonconsensual  
Pornography

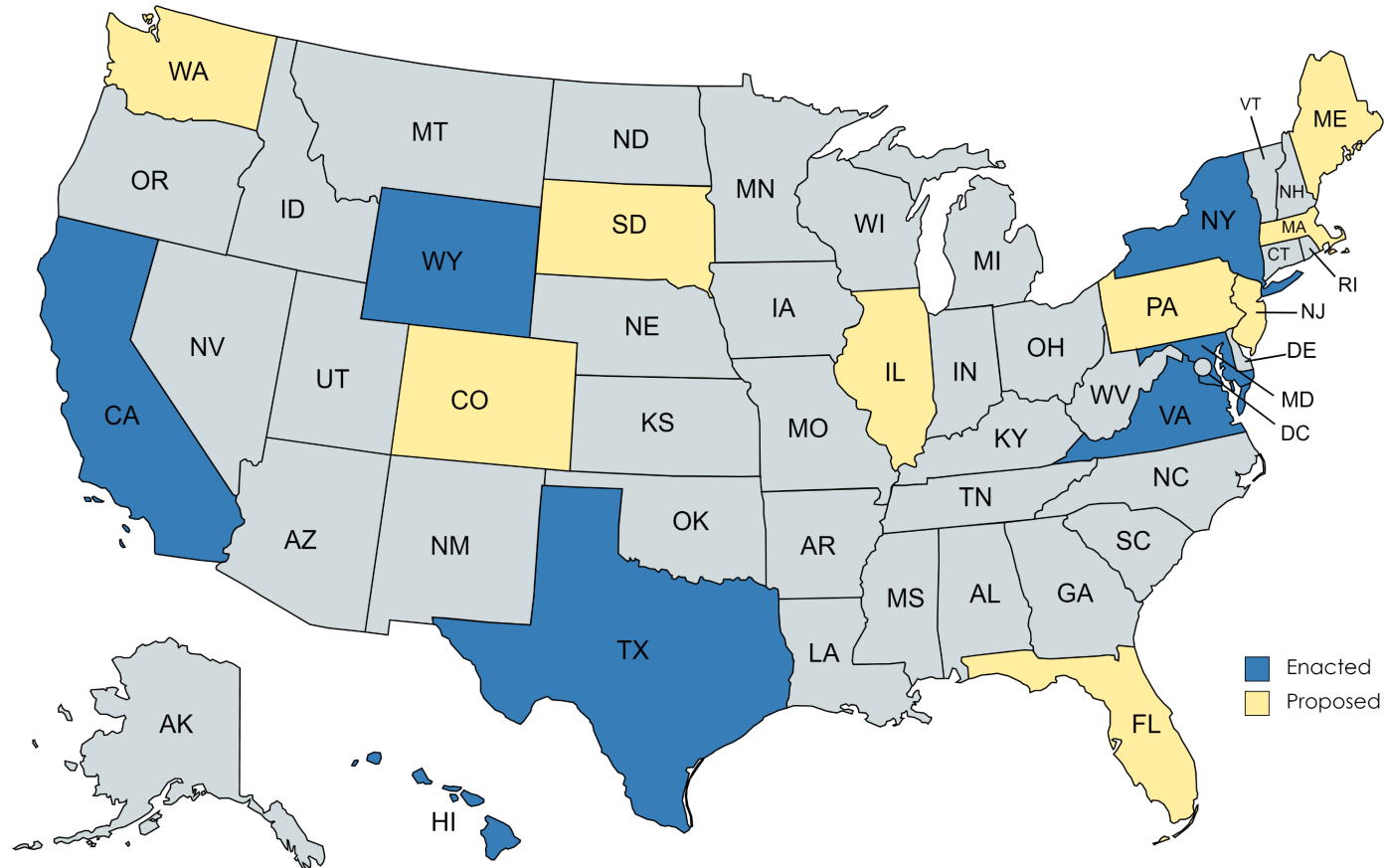
Elections

Property

Research,  
Reports,  
Notifications

- Federal Bills Focus on Research and Reports
- State Bills Focus on:
  - Nonconsensual Pornography
  - Election-Related Deepfakes
  - Post-Mortem Property Rights (NY)
- Typically, Bills Require Specific Intent and/or “Actual Malice”
- Civil Remedies/Private Rights of Action Far More Common than Criminal Penalties

# Lawmaking moving quickly



# Deepfakes at the Bar

## Evidentiary Issues

# Dubai Family Court

- In February 2020, an attorney in the United Arab Emirates claimed that a deepfake audio recording was used in a child custody case in the United Kingdom in an effort to discredit the child's Dubai-based father.
- According to [reports](#), the mother in the dispute used software and online tutorials to manipulate an audio recording of the father to include words he did not say to make it sound as though he was threatening the mother.
- Forensic experts were able to show the media had been manipulated.



# Evidentiary Rules

- Evidentiary rules impose authentication standards and requirements that will need to be leveraged to keep deepfakes from masquerading as unadulterated media
- The rules allow for the authentication of records “generated by an electronic process or system that produces an accurate result,” if “shown by a certification of a qualified person” in a manner set forth by the rules. FRE 902(13), (14)
- The rules also require advance notice to the other side and the opportunity to challenge the records. FRE 902(11) and 902(12)
- If the certification requirements are met, a party need not call a testifying witness at trial to establish authenticity
- Attorneys have obligations to verify the authenticity of media on their own before submitting it to court

# Ethical Duties

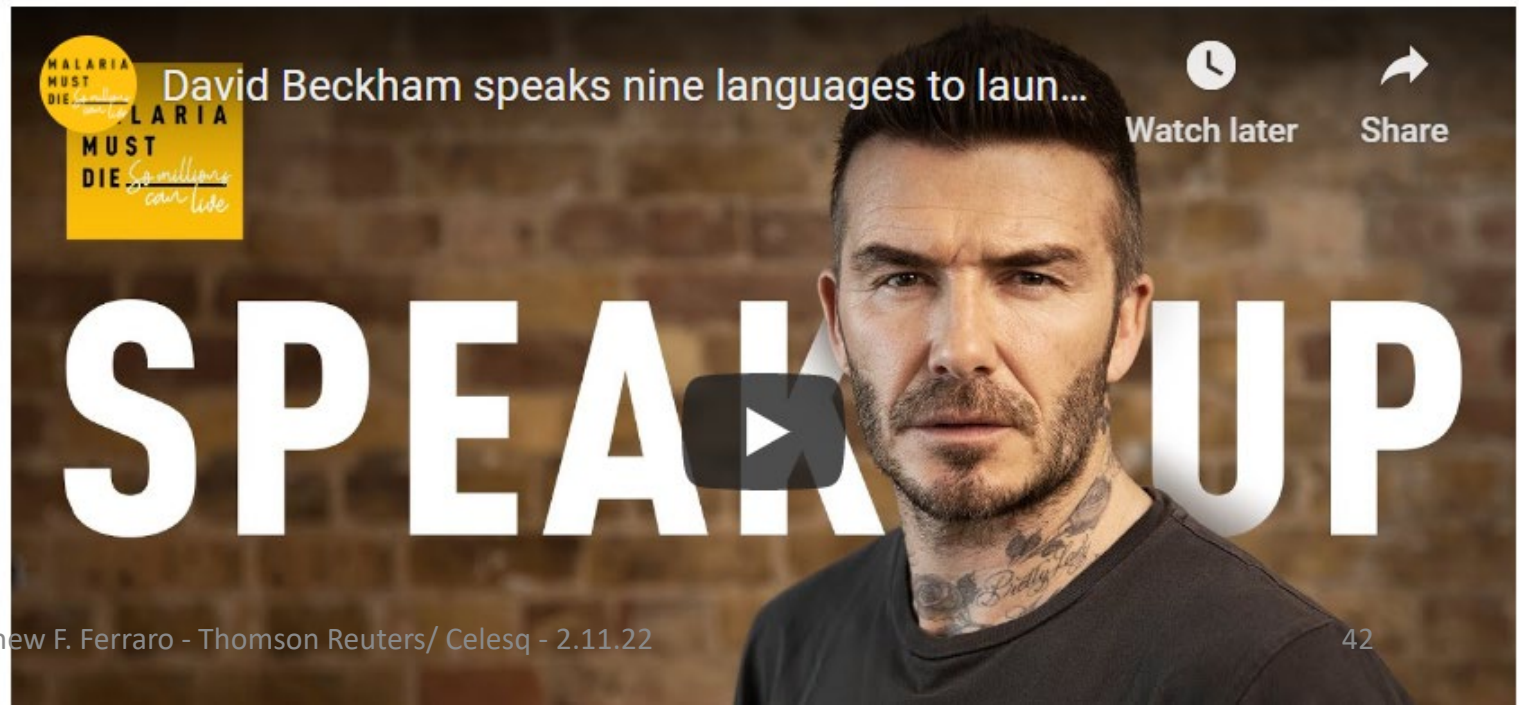
- Practitioners should be alert for opportunities to challenge admissibility on the basis that the evidence may have been faked.
- An attorney may not knowingly offer “evidence that the lawyer knows to be false,” like a deepfake. Model Rules of Professional Conduct r. 3.3(a)(3).
- Attorneys should not baselessly stoke that skepticism for advantage, claiming without good reason that evidence is manipulated or that jurors cannot believe their eyes or their ears
- In the face of these new challenges, lawyers have unique ethical obligations to serve society by acting in ways that buttress the public’s confidence in the rule of law and the administration of justice. Model Rules of Professional Conduct preamble ¶¶ 6, 13

# Positive-use Cases for Deepfakes

Business and Legal Opportunities

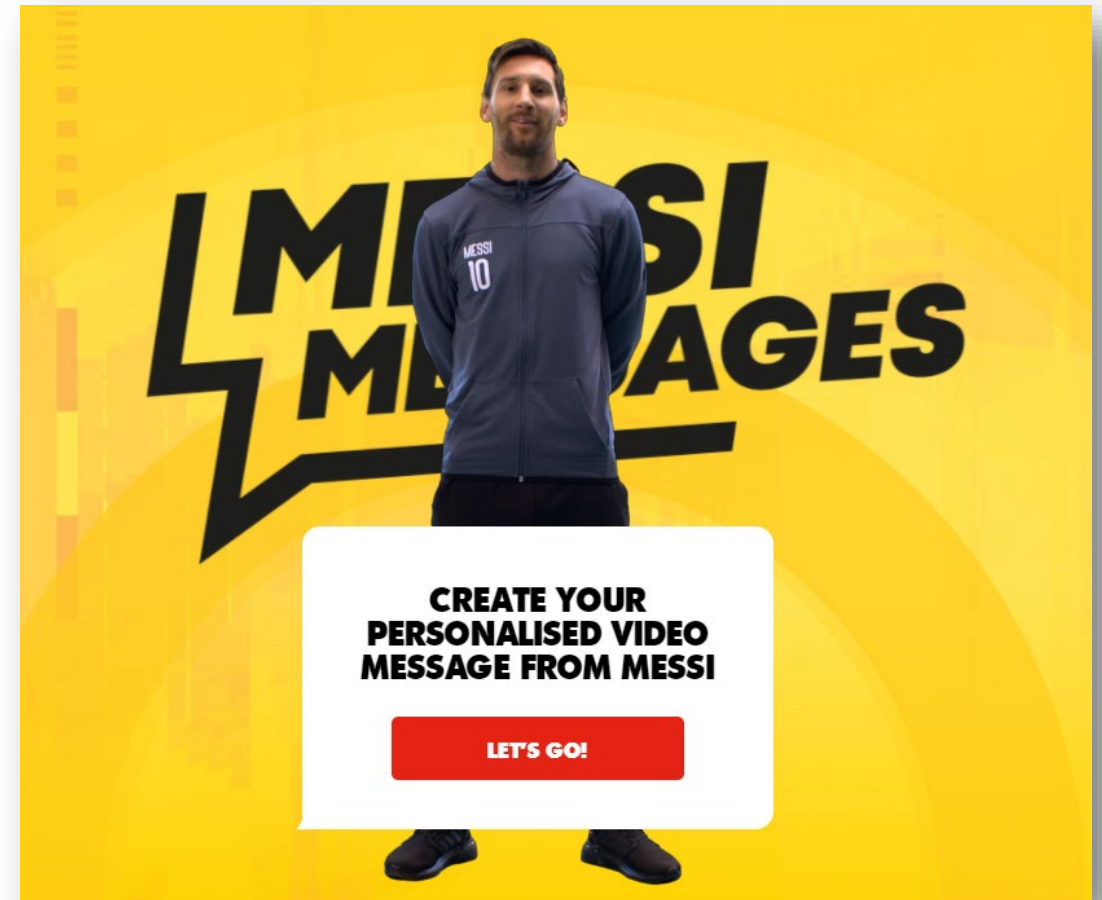
# Deepfakes Positive Use Cases

- Accessibility
- Outreach
- Entertainment
- Advertising
- Expression/Empathy



# Legions of Legal Issues

- Increasingly mainstream positive use cases of deepfakes
  - Movies
  - MyHeritage animates old photos
  - Messi Messages – personalized video message from soccer star Lionel Messi
- New frontier of synthetic media
- Early adopters need ethical guides, regulatory & legal review
- Licensing and Ownership of Manipulated Media



## *Bonus:* Tips for Good Information Hygiene

- Be skeptical not cynical
- Don't retweet or share phony things
  - Or things whose provenance is suspect
- Interrogate your sources of information
  - Trust experts and established journalists not random Internet profiles
- Look for corroboration from others
- If it's too outlandish to be true, it probably is false
- **Pay for news** (subscribe to newspapers)
- Use 2-factor authentication & change your password regularly



# Questions?

**Matthew F. Ferraro**

Counsel, Wilmer Cutler Pickering Hale & Dorr

[Matthew.Ferraro@wilmerhale.com](mailto:Matthew.Ferraro@wilmerhale.com)

Twitter: [@MatthewFFerraro](https://twitter.com/MatthewFFerraro)

More information / writings available at: <http://www.MatthewFFerraro>

DECEMBER 2020

## DECODING DEEPFAKES

By MATTHEW F. FERRARO

### THIS NSI BACKGROUND

- |                                             |                                                                                   |                                                                                                                                              |                                                                                |
|---------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <p><b>1</b> <b>DEFINES</b> “deepfakes”.</p> | <p><b>2</b> <b>EXPLAINS</b> how they are made and highlights recent examples.</p> | <p><b>3</b> <b>DESCRIBES</b> the dangers of deepfakes to national security, politics, business, economic security, and personal privacy.</p> | <p><b>4</b> <b>OUTLINES</b> potential technological and legislative fixes.</p> |
|---------------------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|

### WHAT ARE DEEPFAKES

- **Deepfakes Defined.** A deepfake is synthetic media (text, images, audio, or video) that is either manipulated or wholly generated by artificial intelligence (AI).<sup>1</sup> Put simply, it is a very convincing media forgery created by computers.
  - The term, “deepfake,” is a blend of the words “deep learning” (a branch of AI) and “fake.” Deepfakes are also sometimes called “machine-manipulated media,” “synthetic media,” “digital content forgeries,” and so forth.
  - In a recent example, MIT researchers, to show how easy it is to make a deepfake, created in 2020 a video in which President Richard Nixon announced that the Apollo 11 moon landing had failed. In truth, the researchers used deepfake technology to edit a video from a different Nixon speech to make his voice and facial movements appear he was giving a fabricated address.<sup>2</sup>
- **Deepfake Technology.** Deepfake technology uses computer systems called “generative adversarial networks” (GANs), wherein one algorithm (the generator) creates content modeled on source data, such as existing video or audio of an individual, while a second algorithm (the discriminator) tries to spot the artificial content.<sup>3</sup>
  - The competition between the two networks produces a better-and-better fake until the discriminator can no longer identify the forgery.
- **Growth of Deepfakes.** The technology used to make deepfakes is getting better and more accessible, and, as a result, the number of deepfakes available online is steadily increasing. As of July 2020, there were about 50,000 deepfakes on the Internet. The number doubles every six months.<sup>4</sup>

### DANGERS OF DEEPFAKES

- **Political Disinformation.** We are accustomed to believing that when a public official appears on camera to deliver an urgent message, the message and messenger are authentic. But a deepfake could create confusion or undermine official government conduct in the context of a political campaign, a public health emergency, a prosecution, or similar circumstances.
  - Imagine the political impact of a realistic looking fake video that circulates on the eve of an election of a candidate using a racial epithet. Likewise, imagine a believable forged video of a state official announcing that polling places had been closed. Voters could be discouraged from casting ballots, throwing doubt on the entire process.



- **National Security.** There are major national security implications of deepfakes. They could be used in a variety of ways to undermine governmental leadership, disrupt effective military communication, or even spark conflict.
  - Consider the potentially deadly repercussions of a fake video of the American president announcing a missile strike on North Korea that goes viral before it can be explained.
- **“Liar’s Dividend.”** Deepfakes can bestow a “Liar’s Dividend”—one can successfully deny the authenticity of genuine content by claiming the content is a deepfake.<sup>5</sup>
  - This happened in 2018 in Gabon when opponents of the president claimed that a video of him was fake and he was incapacitated or dead. The conspiracy spread and, within a week, the military launched a coup.<sup>6</sup>
- **Personal Privacy.** Deepfakes pose a particular threat of intimate harassment. According to a 2019 study, over 95% of all deepfake videos are of nonconsensual pornography<sup>7</sup>—a nonconsenting person’s face placed on the body of a pornographic performer. Most of those videos are today of famous female actors, but the technology menaces everyone’s privacy, including governmental leaders and their loved ones.<sup>8</sup>
- **Economic Security.** Disinformation and deepfakes endanger economic security and the private sector,<sup>9</sup> including through stock-price manipulation, credential theft, and fraud.<sup>10</sup> Well-timed deepfakes could also cause systemic harm to the economy by, for example, undermining confidence in the central bank, sparking a market sell-off, or crippling a U.S. business to favor a foreign national champion.
  - For example, in March 2019, an insurer reported that one of its clients lost roughly \$250,000 after a company official wired money to a telephone caller impersonating the parent company’s CEO with AI-based software.<sup>11</sup>
  - More than 70 countries already have state-sponsored disinformation units.<sup>12</sup> These outfits could relatively easily use manipulated media to target the economic lifeblood of adversaries or protect national champions. For example, imagine the Chinese state promoting a convincing synthetic video of the violent crash of an American autonomous vehicle to undermine confidence in a U.S. competitor for the benefit of a Chinese automotive company.<sup>13</sup>

## ■ DEALING WITH DEEPFAKES

- **Technological Fixes.** There are basically two technological ways to counter deepfakes. One is to detect the phony media after it is created. For example, Microsoft launched a new tool in September 2020 to spot deepfakes by giving a confidence score to analyzed pictures and videos about whether they were manufactured artificially.<sup>14</sup>
  - The second way is to verify photographs at the “point of capture” in such a manner that they cannot be altered or modified after the fact.<sup>15</sup> That technology is also proceeding apace: in October 2020, Qualcomm and a startup called Truepic announced that it would embed a photo and video verification tool leveraging image-provenance technology within smartphone chips that will be available in some Android devices in 2021.<sup>16</sup>
- **Legislative Action.** Legislators in Congress and the states have moved quickly to address the dangers of manipulated media by outlawing certain uses of deepfakes and studying their implications for national and economic security.
  - Five states (California, Maryland, New York, Texas, and Virginia) have adopted laws barring certain deepfakes that target candidates for public office or deepfake pornography. About ten other states are considering similar legislation.
  - Congress passed the first national law on deepfakes in 2019. It requires intelligence agencies to report on the foreign weaponization of deepfakes and to notify Congress of deepfake activities targeting elections.<sup>17</sup> Congress is considering about 10 other bills on deepfakes that mostly require reports and research.
- **Other Actions.** There are non-legislative mechanisms that can address deepfakes. For example, in January 2020 the U.S. House of Representatives Committee on Ethics cautioned Representatives and their staffs against posting deepfakes because they could be in violation of the House’s Code of Official Conduct.<sup>18</sup> Similarly, ethical guidelines, professional rules, and social norms may be developed to address deepfakes.<sup>19</sup>

## » KEY ITEMS TO WATCH

### EXPONENTIAL INCREASE

- Whether deepfakes will continue to proliferate exponentially and whether the technology to create them will continue to improve and become universally accessible.

### LEGISLATIVE EFFORTS

- Whether the President signs the National Defense Authorization Act for FY 2021, which would require the Departments of Defense and Homeland Security to study the threats posed by deepfakes to the military and national and economic security; whether Congress will amend federal election law to prohibit deepfakes in elections; and whether more states will bar deepfake pornography or election-related deepfakes and whether successful claims will be brought under those laws.

### TECHNOLOGICAL FIXES

- Whether efforts to improve and distribute technologies to detect deepfakes or to verify images at the point of capture will be widely adopted and able to catch and stay ahead of deepfake technology.

## ENDNOTES

Matthew F. Ferraro is an NSI Visiting Fellow at George Mason University's Antonin Scalia Law School. He is an attorney and former intelligence officer who writes widely on national security and legal issues. A term member of the Council on Foreign Relations, he is counsel at the international law firm Wilmer Cutler Pickering Hale and Dorr where he represents clients on matters related to defense and national security, cybersecurity, and crisis management. Previously, Mr. Ferraro held staff, policy, and operational positions with the Director of National Intelligence, Central Intelligence Agency, and other government agencies.

1 See generally NINA SCHICK, DEEPFAKES: THE COMING INFOCALYPSE 8 (2020).

2 Bonnie Burton, *MIT Releases Deepfake Video of 'Nixon' Announcing NASA Apollo 11 Disaster*, CNET (Jul. 20, 2020), <https://www.cnet.com/news/mit-releases-deepfake-video-of-nixon-announcing-nasa-apollo-11-disaster/>; Mike Well, *Apollo 11 'Disaster' Video Project Highlights Growing Danger of Deepfake Tech*, SPACE.COM (Jul. 19, 2020), <https://www.space.com/apollo-11-disaster-deepfake-video-tech.html>.

3 Sarah Basford, *What Deepfakes Actually Are*, GIZMODO (Jul. 31, 2020), <https://www.gizmodo.com.au/2020/07/what-are-deepfakes/>; Meredith Somers, *Deepfakes, Explained*, MIT (Jul. 21, 2020), <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained>.

4 Henry Ajder, *Deepfake Threat Intelligence: A Statistics Snapshot from June 2020*, SENSITY (Jul. 3, 2020), <https://sensity.ai/deepfake-threat-intelligence-a-statistics-snapshot-from-june-2020/> (Sensity was previously known as Deeptech Labs).

5 Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIFORNIA LAW REVIEW 1753, 1785-1786 (2019).

6 Rob Toews, *Deepfakes Are Going To Wreak Havoc On Society. We Are Not Prepared*, FORBES (May 25, 2020), <https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared/>.

7 Giorgio Patrini, *The State of Deepfakes 2019*, SENSITY (Oct. 7, 2019), <https://sensity.ai/mapping-the-deepfake-landscape/>.

8 Jane Litynsky & Scott Lucas, *Thousands of Women Have No Idea a Telegram Network is Sharing Fake Nude Images of Them*, BUZZFEED (Oct. 20, 2020) <https://www.buzzfeednews.com/article/janelitynsky/telegram-deepfake-nude-women-images-bot> (deepfake technology allowed users to create photo-realistic simulated nude images of 680,000 women without their knowledge or consent, according to tech researchers).

9 See Matthew F. Ferraro, Jason C. Chipman & Stephen W. Preston, *Identifying the Legal and Business Risks of Disinformation and Deepfakes: What Every Business Needs to Know*, 6 PRATT'S PRIVACY AND CYBERSECURITY LAW REPORT 142, 142 (2020); Claire Atkinson, *Fake News Can Cause 'Irreversible Damage' to Companies—And Sink Their Stock Price*, NBC NEWS (Apr. 25, 2019), <https://www.nbcnews.com/business/business-news/fake-news-can-cause-irreversible-damage-companies-sink-their-stock-n995436>.

10 Ferraro, et al., *supra* note 9, at 143.

11 *Id.* at 145-146 (citing reports).

12 Matthew F. Ferraro & Preston B. Golson, *The Next Gray Zone Conflict: State-Based Disinformation Attacks on the Private Sector*, LAWFARE (Mar. 24, 2020), <https://www.lawfareblog.com/next-gray-zone-conflict-state-based-disinformation-attacks-private-sector>.

13 *Id.* (describing how a Russian company recently designed a fake electric car accident to garner attention, and several media outlets treated the bogus video as if it were real); Cat Zakrzewski, *Businesses Should be Watching Out for Deepfakes Too, Experts Warn*, WASHINGTON POST (Dec. 13, 2019), <https://www.washingtonpost.com/news/powerpost/paloma/the-technology-2020/2019/12/13/the-technology-2020-businesses-should-be-watching-out-for-deepfakes-too-experts-warn/5df279f1602ff125ce5b2fe7/>.

14 Leo Kelion, *Deepfake Detection Tool Unveiled by Microsoft*, BBC (Sept. 1, 2020), <https://www.bbc.com/news/technology-53984114>.

15 Mounir Ibrahim, *To Beat Deepfakes, We Need to Prove What is Real. Here's How*, WORLD ECONOMIC FORUM (Mar. 23, 2020), <https://www.weforum.org/agenda/2020/03/how-to-make-better-decisions-in-the-deepfake-era/>.

16 Olivia Solon, *Qualcomm Announces Photo Verification Tool*, NBC NEWS (Oct. 15, 2020), <https://www.nbcnews.com/tech/security/qualcomm-announces-photo-verification-tool-n1243550>.

17 Matthew F. Ferraro, Jason C. Chipman & Stephen W. Preston, *The Federal "Deepfakes" Law*, 3 THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW 229, 229 (2020).

18 Memorandum for All Members, Officers, and Employees from Committee on Ethics, Subj. Intentional Use of Audio-Visual Distortions & Deep Fakes (Jan. 28, 2020), [https://ethics.house.gov/sites/ethics.house.gov/files/wysiwyg\\_uploaded/Deep%20Fakes%20Pink%20Sheet%20Guidance-Final.pdf](https://ethics.house.gov/sites/ethics.house.gov/files/wysiwyg_uploaded/Deep%20Fakes%20Pink%20Sheet%20Guidance-Final.pdf).

19 See Matthew F. Ferraro, *Through A Straw Darkly*, N.Y.U. JOURNAL OF LEGISLATION & PUBLIC AND POLICY QUORUM (2020), <https://nyujpp.org/quorum/ferraro-reflections-on-nyu-deepfakes-conference/>.

## Disinformation Dangers: Fake Narratives and Deepfakes Pose Rising Risks to Business

**The growing ease with which believable deepfake media can be created will accelerate a range of business dangers, particularly those related to reputational risk, market manipulation, and social engineering fraud.**

*By Matthew F. Ferraro*

The world is awash in disinformation. Untruths and half-truths abound, seemingly about everything, from phantom voter fraud, to lies about the coronavirus, to tall-tales of pedophilic cabals bestriding the globe. And while this “[information disorder](#)” has often been thought of as primarily effecting politics, the malady runs [deeper](#).

We are witnessing the emergence of a growing threat to businesses of all kinds: the proliferation of viral false information and believable synthetic media (or, [deepfakes](#)) targeting the private sector. These new hazards require innovative business and legal responses, what I call ***disinformation and deepfakes risk management (DDRM)***.

Disinformation in this context means the spreading of outright falsehoods, personal data, or decontextualized information in a farrago of fact and myth to mislead others.

Bearing false witness is as old as human history, but technology has given new potency to this ancient vice, allowing deceptions to spread faster and farther than ever before. One [2019 study](#) estimated that firms lose \$78 billion each year due to disinformation. A separate [survey](#) found that 88% of investors considered disinformation attacks on corporations a serious issue.

The growing ease with which believable deepfake media can be created will accelerate a [range of business dangers](#), particularly those related to reputational risk, market manipulation, and social engineering fraud.

**Reputational Risk.** Viral disinformation and deepfakes exacerbate reputational challenges companies already face. Today, online conversations drive brand identities, which themselves are increasingly taking on [political](#)



/iStockphoto

[valences](#) that make them prime targets for disinformation purveyors.

For example, in the summer of 2020, a QAnon-adjacent conspiracy theory circulated online that the furniture seller [Wayfair](#) was involved in child trafficking because of the coincidental overlap of the names of some of Wayfair’s products and those of missing children. Social media trolls [posted](#) the address and maps of Wayfair’s offices and the LinkedIn profiles of its employees, and tried to orchestrate a campaign to short the company’s stock. It all sounds absurd, but these fabrications dominated online conversation about the company for weeks.

Likewise, during the pandemic, conspiracies metastasized online that 5G cell towers contributed to the spread of the coronavirus, instigating off-line [violence](#) against corporate assets, including dozens of arsons of cell towers and episodes of harassment against telecommunications employees. The situation grew sufficiently dire that the U.S. Department of Homeland Security issued an industry [warning](#) about the peril to privately-owned communications infrastructure.

And, in one of its many reproofs of Western coronavirus vaccines, Chinese state media [attacked](#) the safety of Pfizer's COVID-19 vaccine and called in January 2021 for an investigation into the deaths of two dozen elderly Norwegians after they received it.

Consider how much more convincing such conspiracies will become when they are joined by believable synthetic video of, say, a CEO appearing to use a racial epithet, a car company's flagship autonomous vehicle exploding in an apparently deadly crash, or a "news" report on the supposed health dangers of a new consumer technology.

**Market Manipulation.** Pump-and-dump and short-seller schemes have long relied on the circulation of false information about companies to drive stock prices. The increasing power of social media and [meme stocks](#) in market movements have amplified the power of such dissemblers.

For example, in December 2020, the Securities and Exchange Commission (SEC) [charged](#) a Georgia man and several others for pushing mergers and acquisitions rumors through false online posts that temporarily goosed the companies' stocks and allowed the defendants to profit from the jump in prices.

Again, these crimes are likely to be all the more damaging once malefactors leverage believable fake media to help sink or stoke equities.

**Social Engineering Fraud.** Deepfakes have already been used to impersonate trusted parties and defraud businesses. For example, in January 2020, a [bank manager](#) in Hong Kong received a call from the director of a company whose voice he recognized. The caller asked the banker to authorize financial transfers of \$35 million to finance an acquisition. The director also emailed the bank manager, and the banker began to execute the transfers. Only later did the manager learn that he had been defrauded by "[deep voice](#)" technology, which impersonated the voice of the director in an advanced form of social engineering. This heist followed [reports](#) from 2019 that a British CEO wired a quarter-million-dollars at the behest of a caller who used similar technology to impersonate the CEO of the British firm's German parent company.

The FBI has put companies on notice that such impersonation crimes will escalate. In March 2021, the FBI issued [a private industry notification](#) (PIN) advising companies

that threat actors "almost certainly" will use synthetic media "for cyber and foreign influence operations in the next 12-18 months." The PIN warned that malicious cyber actors will not just push propaganda on behalf of foreign states but also leverage deepfake technology to conduct [business identity compromise](#), where deepfake tools will be employed to impersonate employees to damage business finances and reputations.

What can businesses do? Companies will need to work with their counsel to craft responses **before, during, and after** a disinformation episode.

Beforehand, a business should plan for disinformation and deepfakes risk like it plans for any number of cyber-hacks or crisis events. It should proactively communicate an accurate positive message about its business on social media, monitor how its brand is perceived online, and conduct a self-assessment to understand the narratives that would be the most compelling against it. A business should amend crisis plans to manage disinformation dangers, assign roles and responsibilities to executives, train its employees to be on the lookout for deepfake scams, and drill for the span of disinformation harms. Also, a company should register its trademarks and copyrights, given the strong protection intellectual property enjoys under federal law. If a victim's IP is misused, copyright or trademark owners can ask that social media posts be taken down and take other legal action.

During an incident, a victim may wish to engage with social media platforms to request assistance staunching the spread of false narratives. When suitable, a business should counter phony speech with accurate positive messages about the company, and perhaps raise the alarm through the news media that it is the victim of disinformation by malevolent actors.

Finally, after a disinformation campaign, market manipulation, or social engineering fraud, companies should consider notifying their regulators, shareholders, customers, and partners. If necessary and appropriate, victims should consider bringing legal action against deceivers.

Corporate counsel will need to weigh carefully business goals and legal risks in the face of these new challenges.

**Matthew F. Ferraro**, a former U.S. intelligence officer, is counsel at WilmerHale and a visiting fellow at the National Security Institute of George Mason University. [matthew.ferraro@wilmerhale.com](mailto:matthew.ferraro@wilmerhale.com), @MatthewFFerraro