AN A.S. PRATT PUBLICATION
JUNE 2020
VOL. 6 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 6 NUMBER 5 JUNE 2020

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [6] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [131] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2020–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc.

For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. 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.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 230 Park Ave. 7th Floor, New York NY 10169.

Identifying the Legal and Business Risks of Disinformation and Deepfakes: What Every Business Needs to Know

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

The authors review the legal and business risks that could arise from disinformation and manipulated media, address potential causes of action that could be brought by victims of disinformation against the individual creators or propagators of malicious content, and highlight some best practices that businesses can undertake to prepare for these new exposures.

Disinformation and "deepfakes" pose growing threats to the private sector. Already, disinformation has been weaponized to harm brands, move markets, and undermine trust in companies and industries. One recent study estimated that firms lose $78 billion each year due to disinformation, including $9 billion that companies and individuals spend every year trying to repair reputations damaged by disinformation and $17 billion lost due to financial disinformation.[1] According to another recent survey, by the Brunswick Group, 88 percent of investors consider disinformation attacks on corporations a serious issue.[2]

These problems will get much worse as "deepfakes"—photos, videos, audio and text manipulated by artificial intelligence ("AI"), often showing someone saying or doing things they never did—become more believable and easier to produce.

Disinformation is not an issue associated merely with social media. As discussed more below, realistic forgeries can be used in many contexts to contribute to such harms as social engineering, credential theft, business and insurance fraud, and falsified court evidence, among others. Major social media companies have established policies to address certain manipulated media on their platforms,[3] but the challenges associated

* The authors, attorneys with Wilmer Cutler Pickering Hale and Dorr LLP, may be contacted at matthew.ferraro@wilmerhale.com, jason.chipman@wilmerhale.com, and stephen.preston@wilmerhale.com, respectively. The authors express gratitude to Jonathan Cedarbaum, Kirk Nahra, and Louis Tompros for providing comments on this article.

[1] Michelle Castillo, *Exclusive: Fake News Is Costing the World $78 Billion a Year*, Cheddar, Nov. 18, 2019, https://cheddar.com/media/exclusive-fake-news-is-costing-the-world-billion-a-year.

[2] Robert Moran, Preston Golson & Antonio Ortolani, *Enter the Imposter*, Brunswick Review, Sept. 18, 2019, https://www.brunswickgroup.com/disinformation-attacks-insight-research-integrity-i12018/.

[3] *See, e.g.*, *Building Rules in Public: Our Approach to Synthetic & Manipulated Media*, Twitter, Feb. 4, 2020, https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html; *Enforcing Against Manipulated Media*, Facebook, Jan. 6, 2020, https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/.

with such media go beyond what platforms can do alone, especially when such media is spread by email, telephone or offline, or intended for innocuous purposes.

Thus, every business should prepare for this changing information environment.

To that end, this analysis, first, reviews the legal and business risks that could arise from disinformation and manipulated media. Those risks include:

1. Reputational Damage;
2. Extortion and Harassment;
3. Social Engineering and Fraud;
4. Credential Theft;
5. Market Manipulation;
6. Insurance Fraud;
7. Labor and Employment Issues;
8. Entertainment Industry Issues;
9. Cybersecurity Insurance;
10. Falsified Court Evidence; and
11. Regulatory Scrutiny.

Second, this analysis addresses potential causes of action that could be brought by victims of disinformation against the individual creators or propagators of malicious content, whether under long-established state and federal laws or under new laws enacted within the past year that specifically address deepfakes.

Third, this article reviews some best practices businesses can undertake today to prepare for these new exposures.

The issues discussed here are growing with the wider use and availability of convincing manipulated media. Concerned companies should discuss preparatory and mitigatory actions with counsel in light of their specific circumstances.

SPOTTING LEGAL AND BUSINESS RISKS OF DISINFORMATION

When we talk about disinformation in this context, we mean the deliberate spreading of falsehoods about individuals and businesses to influence public perceptions of those people and entities. The dangers of disinformation are multiplied by the growing realism of media manipulated by computers, commonly known as deepfakes. Disinformation, both traditional types and deepfakes, gives rise to numerous legal and business issues, including but not limited to the following.

Reputational Damage, to Both Businesses and Individuals

Gossip, half-truths and outright lies have harmed the reputations of individuals and organizations since time immemorial. What is different now is the speed with which false information can spread online, its scale, and the seeming veracity of forged images and audio.

In August 2017, for example, someone on the anonymous website 4Chan said he wanted to inflict pain on a "liberal place." He decided to launch a faux social media campaign that made it appear that Starbucks was giving free drinks to undocumented immigrants during a so-called Dreamer Day. The goal was to create bad publicity for the chain by making it look like Starbucks supported undocumented immigration. To spread the disinformation, a forger created realistic-looking graphics using the Starbucks font and logo and even coined a hashtag to promote the campaign (#borderfreecoffee). The tweets started to trend. The company swung into gear and directly responded to individuals who were retweeting bogus information.[4]

Similarly, in August 2019, a Twitter user claimed her account had been hacked to spread the rumor that the restaurant chain Olive Garden was helping fund President Trump's reelection campaign. While the rumor was easily disproven by campaign finance data—neither the restaurant nor its parent company donates to presidential candidates—the hashtag #BoycottOliveGarden quickly went viral with more than 52,500 tweets and retweets.[5]

Disinformation campaigns can target companies of all sizes. For example, in August 2017, Kids Plus Pediatrics, a pediatric medical practice in Pittsburgh, posted a video about the importance of the HPV vaccine. The medical practice was soon inundated by thousands of false negative user reviews. The assault was coordinated by anti-vaccination activists in 36 states and eight countries. The practice responded by developing a social media strategy, building what it called a "virtual cavalry" to speak out in favor of vaccines when future attacks occur, and by raising awareness to other doctors of disinformation risks.[6]

Foreign governments and organizations may also engage in brand assassination and target private companies for their own strategic or economic reasons. In 2015, for instance, online identities masquerading as New Yorkers but secretly controlled by

[4] Will Yakowicz, *Fake Starbucks Ad Tries to Lure the Undocumented With Discounted Coffee*, Inc., Aug. 8, 2017, https://www.inc.com/will-yakowicz/fake-starbucks-dreamer-day-4chan-meme.html.

[5] Steven Melendez, *Is Olive Garden Funding Trump? How a False Rumor Ignited a Twitter Boycott*, Fast Company, Oct. 27, 2019, https://www.fastcompany.com/90396218/olive-garden-funding-trump-false-rumor-ignites-boycott.

[6] Lena H. Sun, *Anti-Vaxxers Trolled a Doctor's Office. Here's What Scientists Learned From the Attack*, The Washington Post, March 21, 2019, https://www.washingtonpost.com/health/2019/03/21/anti-vaxxers-trolled-doctors-office-heres-what-scientists-learned-attack/.

Russian operatives claimed they had become ill after eating turkey sourced from a small company called Koch's Turkey Farms. The company began an internal food-safety review before learning that all the claims of illness were phony. The campaign was a hoax meant to stir up internal societal divisions against the "Koch Brothers," even though the name of the farm had no connection to that family.[7]

Imagine how much more devastating such disinformation will be if it involves realistic deepfake media. Consider the impact on consumer confidence of a widely shared, believable (yet manufactured) video showing a recently unveiled autonomous vehicle getting into a fiery accident. Or consider the impact on a public company of a manipulated audio clip that makes it sound like the company's high-profile chief executive officer made disparaging comments about an ethnic group. Remedying the reputational injuries inflicted by such efforts—beginning with proving that the media were forged—may require substantial investments of time and resources.

Extortion and Harassment

Deepfakes pose a particular threat of extortion and intimate harassment. According to a recent study by Deeptrace Labs, over 95 percent of all deepfake videos now on the internet are of nonconsensual pornography—that is, a nonconsenting person's face is placed on the body of a pornographic performer.[8]

Bad actors could use such deepfakes either to extort concessions from business leaders or to embarrass them by releasing the media, regardless of any demands. For example, one could threaten the release of an explicit nonconsensual deepfake that appears to depict either a business leader or a business leader's loved one.

In 2018 a fake sex video seemingly of Indian investigative journalist Rana Ayyub circulated online, evidently in reprisal for her critical reporting of Prime Minister Narendra Modi and his political party. The harassment and humiliation that followed sent Ayyub to the hospital with heart palpitations and led her to withdraw from online life, according to reports.[9]

Social Engineering and Fraud

Deepfakes have been reportedly used to impersonate identities of corporate officers and facilitate fraud. For example, in March 2019, according to press reports, the CEO of a UK-based energy firm thought he was speaking on the phone with his boss, the

[7] Rob Barry, *Russian Trolls Tweeted Disinformation Long Before U.S. Election*, The Wall Street Journal, Feb. 20, 2018, https://www.wsj.com/graphics/russian-trolls-tweeted-disinformation-long-before-u-s-election/.

[8] *The State of Deepfakes 2019*, Deeptrace Labs, Oct. 7, 2019, https://deeptracelabs.com/mapping-the-deepfake-landscape/.

[9] *I Was Vomiting: Journalist Rana Ayyub Reveals Horrifying Account of Deepfake Porn Plot*, India Today, Nov. 21, 2018, https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21.

CEO of the firm's German parent company. The German CEO asked the British official to wire $243,000 to a Hungarian supplier. The British CEO complied. Only afterward did he realize that he had been duped; he was speaking to someone using AI-based software to impersonate the German CEO's voice, according to the energy firm's insurance carrier, Euler Hermes Group SA.[10]

Similarly, in July 2019, cybersecurity firm Symantec reported that three companies had fallen victim to deepfake audio attacks. Each time, a company's "CEO" called a senior financial officer to request an urgent money transfer. The scammer mimicked each CEO's voice with an AI program that had been trained on hours of their speech taken from earnings calls, YouTube videos, TED talks and so forth. Symantec said millions of dollars were stolen from each company, but it did not reveal the names of the businesses.[11] And in February 2020, a Pennsylvania attorney reported that he was fooled by what he believes was an AI-enabled voice clone of his "son," who tearfully claimed to need $9,000 in bail money. The father nearly wired the funds to someone impersonating the son's lawyer; he stopped only when the actual son called his father to warn him it was a hoax.[12]

In another, less-sophisticated case that demonstrates the trust with which videos are treated, Israeli fraudsters stole about $9 million from a businessman by impersonating the French foreign minister in a Skype videocall. The impostors designed a phony version of the minister's office and donned makeup to disguise themselves as the minister and his chief of staff.[13]

These frauds represent a new variant of what has been called "business email compromise" ("BEC"). In traditional BEC scams, someone gains access to or spoofs

---

[10] Catherine Stupp, *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*, The Wall Street Journal, Aug. 30, 2019, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402. The company's insurer stated the victim was tricked by a deepfake audio, although no third party verified that the audio was a deepfake and not just a convincing, conventional imitation.

[11] Kaveh Waddell & Jennifer A. Kingson, *The Coming Deepfakes Threat to Businesses*, Axios, July 19, 2019, https://www.axios.com/the-coming-deepfakes-threat-to-businesses-308432e8-f1d8-465e-b628-07498a7c1e2a.html; *see also* Bob Keaveney, *RSA 2020: Is Voice Fraud the Next Frontier for Scam Artists?*, Biz Tech Magazine, Feb. 26, 2020, https://biztechmagazine.com/article/2020/02/rsa-2020-voice-fraud-next-frontier-scam-artists.

[12] Ellie Rushing, *A Philly Lawyer Nearly Wired $9,000 to a Stranger Impersonating His Son's Voice, Showing Just How Smart Scammers Are Getting*, The Philadelphia Inquirer, March 9, 2020, https://www.inquirer.com/news/voice-scam-impersonation-fraud-bail-bond-artificial-intelligence-20200309.html.

[13] Kim Willsher & Oliver Holmes, *Conmen Made€8m by Impersonating French Minister - Israeli Police*, The Guardian, March 28, 2019, https://www.theguardian.com/world/2019/mar/28/conmen-made-8m-by-impersonating-french-minister-israeli-police; *see also* Aurelien Breeden, *Paris Court Convicts 6 in $50 Million Fake-Identity Scheme*, The New York Times, March 11, 2020, https://www.nytimes.com/2020/03/11/world/europe/france-identity-fraud-le-drian.html (six men were convicted in Paris of several such related impersonation schemes, which combined netted over $50 million).

the email account of a company employee or the account of an employee of a business associate and impersonates the real account owner to trick a company, its customers, its partners or its employees into sending money or sensitive data to the infiltrator. Traditionally, one guards against BEC schemes by telephoning the purported sender of the email. But realistic fake audio adds even more vulnerability to such compliance plans. Notably, in January 2020, the Federal Trade Commission hosted a workshop entitled "You Don't Say" on voice cloning technologies and their use in fraudulent schemes.[14]

Frauds caused by deepfakes or similar disinformation pose manifold risks for companies. Businesses not only stand to lose the value of defrauded funds, but they can also be subject to litigation by shareholders, investigations by regulators and—if auditors refuse to approve financial statements following such a fraud—loss of access to the capital markets.

Credential Theft

Similarly, through social engineering and convincing impersonation, hackers can gain information technology ("IT") credentials from unwitting corporate employees. With these credentials, they may be able to steal valuable company information, intellectual property, or the personally identifiable information of employees or customers, and hackers could even lace company computer systems with malware or ransomware. The second-order effects of these intrusions and thefts—from litigation to regulator investigations—would compound the loss already suffered as a result of the underlying attacks.

Market Manipulation

Fraudsters long ago discovered how to make money using regular disinformation—fake text and simple graphics—to move the financial markets. For example, in 2015 a Bloomberg.com look-alike website (with the URL "Bloomberg.market") ran a phony story that Twitter had received a $31 billion takeover bid. Twitter's share price jumped, and it is likely that whoever spread the story benefited from the surge.[15]

While no charges were filed in that case, the Securities and Exchange Commission ("SEC") has charged others for cyber "boiler room"-type schemes. For example, in 2014, the SEC charged two men with issuing false, rapid-fire news releases about a

[14] *You Don't Say: An FTC Workshop on Voice Cloning Technologies*, Federal Trade Commission, Jan. 28, 2020, https://www.ftc.gov/news-events/events-calendar/you-dont-say-ftc-workshop-voice-cloning-technologies.

[15] Steve Goldstein, *Twitter Takeover Hoax Is Latest Trick to Be Played on Wall Street*, Market Watch, July 14, 2015, https://www.marketwatch.com/story/twitter-hoax-latest-trick-to-be-played-on-wall-street-2015-07-14.

small biotech firm that drove the stock price up by a factor of eight in just a month.[16] And in 2010, a Canadian couple made $2.4 million after selling equity in microcap stocks that they pumped up using their website and social media accounts.[17]

Notably, a recent report by JPMorgan Chase observed that those market participants who use trading algorithms based on posts and headlines are particularly susceptible to disinformation manipulation.[18]

And the kind of disinformation that has worked for pump-and-dump schemes works for short sellers, too. For example, in October 2018, after Broadcom announced its intention to acquire CA Technologies for $19 billion, a phony memo circulated online, supposedly from the U.S. Department of Defense, saying the U.S. government would scrutinize the acquisition for national security risks. But the memo was phony—the U.S. government did not even have jurisdiction over the deal—and shares of both companies dropped when news of the memo broke.[19]

Likewise, in 2015, the SEC filed securities fraud charges against a Scottish trader whose false tweets caused sharp drops in stock prices of two companies, a semiconductor manufacturer and a medical research firm.[20]

The dangers of these scams will only grow as believable manipulated media can be made at scale. Imagine the impact of false narratives when they are driven by realistic fake video and audio—not just an article touting a phony acquisition but a credible video of what appears to be the companies' CEOs announcing the transaction. It will be more difficult to correct misperceptions and for the market to recover if the media are convincing, especially in an age when people believe what they want to believe.

---

[16] Maria Armental, *SEC Charges Two With Penny Stock Fraud*, The Wall Street Journal, July 18, 2014, https://www.wsj.com/articles/sec-charges-two-with-penny-stock-fraud-1405716923; Matthew F. Ferraro & Jason C. Chipman, *Fake News Threatens Our Businesses, Not Just Our Politics*, The Washington Post, Feb. 8, 2019, https://www.washingtonpost.com/outlook/fake-news-threatens-our-businesses-not-just-our-politics/2019/02/08/f669b62c-2b1f-11e9-984d-9b8fba003e81_story.html.

[17] *SEC v. McKeown*, No. 10-80748-CIV-COHN (S.D. Fla. June 23, 2010), https://www.sec.gov/litigation/litreleases/2010/lr21580.htm.

[18] *Fake News and Bad News Are Depressing the Market, JPMorgan Strategists Say*, Fortune, Dec. 8, 2018, https://fortune.com/2018/12/08/fake-news-jpmorgan-kolanovic/. The SEC has issued an Investor Alert titled "Social Media and Investing – Stock Rumors" prepared by the Office of Investor Education and Advocacy. The alert aims to warn investors about fraudsters who may attempt to manipulate share prices by using social media to spread false or misleading information about stocks, and provides tips for checking for red flags of investment fraud. *Updated Investor Alert: Social Media and Investing — Stock Rumors*, Securities and Exchange Commission, Nov. 5, 2015, https://www.sec.gov/oiea/investor-alerts-bulletins/ia_rumors.html.

[19] Ed Targett, *Fake Memo Hits Broadcom, CA Technologies Shares*, Computer Business Review, Oct. 12, 2018, https://www.cbronline.com/news/broadcom-cfius-ca.

[20] Press Release, *SEC Charges: False Tweets Sent Two Stocks Reeling in Market Manipulation*, Securities and Exchange Commission, Nov. 5, 2015, https://www.sec.gov/news/pressrelease/2015-254.html.

Insurance Fraud

The insurance industry, among other sectors, often relies on the veracity of digital media to adjudicate claims. Auto insurers use photographs of cars to validate insurance reports, for instance, and healthcare companies often rely on medical imagery to verify claims. As digital media become more easily manipulatable, these industries will face greater challenges.

For example, Israeli researchers recently warned that deepfake radiology scans, which are altered to show false results, including fake cancerous nodes, are poised to spread in the next two to four years as deepfake technology becomes more easily accessible.[21] A fraudster could add phony tumors to medical scans and elicit needless insurance payments. Insurance companies will need to modify their trainings, practices and compliance programs to avoid being fooled.

Labor and Employment Issues

Believable falsified videos or audio could pose unique labor and employment risks. Already, employees are relying increasingly on clandestine video and audio recordings to support their claims of harassment or mistreatment.[22] Depending on the local rules, these recordings are usually admissible as the most reliable evidence,[23] even in spite of broad employer bans on workplace recordings.[24]

Given the prevalence of legitimate recordings of such behaviors, the public could be expected to lend credence to manufactured video and audio recordings purporting to substantiate claims of employer wrongdoing. Perhaps, after an employee is terminated, a video appears online depicting his or her supervisor engaging in inappropriate contact either with the former employee or with someone else. The former employee could use

[21] Jane Anderson, *Addressing 'Deep Fake' Scans Is Critical Amid Tech Advances*, Health Care Compliance Association, Nov. 11, 2019, https://www.jdsupra.com/legalnews/addressing-deep-fake-scans-is-critical-16100/ (quoting Yisroel Mirsky).

[22] Meredith Munro, *Common Evidentiary Trial Issues in Employment Law Cases: From Getting the #MeToo Evidence In, to Keeping the Collateral Source Evidence Out*, King & Greisen, LLP Blog, Aug. 13, 2018, https://www.kinggreisen.com/blog/common-evidentiary-trial-issues-in-employment-law-cases-from-getting-the-metoo-evidence-in-to-keeping-thecollateral-source-evidence-out.

[23] *Byrd v. Reno*, No. 96-2375CKKJMF (D. D.C. Mar. 18, 1998) ("[T]here is not and cannot be anything that is the substantial equivalent of the tape recording of a conversation . . .. There is literally no substitute for the tape recordings."); *Rauh v. Coyne*, 744 F. Supp. 1181, 1183-1184 (D. D.C. 1990) (admitting discrimination plaintiff's tape recording as an admission of a party-defendant); *see also* Fed. R. Evid. 901(a).

[24] *Whole Foods Mkt. Grp., Inc. v. Nat'l Labor Relations Bd.*, 691 F. App'x 49, 50 & n.1 (2d Cir. 2017) (affirming order holding that Whole Foods' prohibition on all recording without management approval interfered with employees' exercise of labor rights, although noting, "This is not to say that every no-recording policy will infringe on employees' Section 7 rights. It should be possible to craft a policy that places some limits on recording audio and video in the work place that does not violate the Act.").

that video to substantiate a harassment claim or support class action litigation. Companies will need to prepare for this potential additional layer of legal and business risk.

Furthermore, many businesses embrace zero-tolerance rules when it comes to video evidence of inappropriate behavior. The greater use of convincing deepfakes may occasion a rethinking of such policies.

Entertainment Industry Issues

In an episode of the tech-dystopian television series *Black Mirror*, a mendacious talent manager drugs an unreliable pop singer named Ashley, rendering her unconscious. He then secretly replaces her with a hologram that goes on to carry out Ashley's performances in her place, without the audiences knowing any better.[25]

This fictional storyline illustrates the potentially game-changing role manipulated media may play in the future of entertainment. Soon, if an actor dies mid-shoot or otherwise cannot complete filming, producers may seek to finish the film without the missing actor by using deepfakes of him or her.[26] On the other hand, actors may seek to protect their digital likenesses from studio use without their consent.

Legislators have proposed at least one bill to prevent this practice. In New York, state legislators are considering a bill that would bar the use of a "digital replica for purposes of trade in an expressive work" without the permission of the depicted person. Accordingly, under this bill, *Black Mirror*'s "Ashley" would be illegal, absent the real star's consent.[27]

Studios may seek to contract around such laws. As *The Hollywood Reporter* noted in September 2019, "in the coming months and years, we can expect TV producers, filmmakers and performers to increasingly include provisions in their contracts that protect against encroaching legislation prohibiting the use of AI technology."[28]

Furthermore, because deepfakes are often created by stitching together material that may be copyrighted (such as an actor's likeness), it is an open question who owns the copyright to a deepfake that may be a composite of different voices and faces created by a third party. The World Intellectual Property Organization ("WIPO") and the U.S. Patent and Trademark Office ("USPTO") both recently asked for public comments on exactly this issue and whether there should be systems of equitable remuneration for

[25] Eriq Gardner, *Deepfakes Pose Increasing Legal and Ethical Issues for Hollywood*, The Hollywood Reporter, July 12, 2019, https://www.hollywoodreporter.com/thr-esq/deepfakes-pose-increasing-legal-ethical-issues-hollywood-1222978.

[26] David Singer & Camila Connolly, *How Hollywood Can (and Can't) Fight Back Against Deepfake Videos*, The Hollywood Reporter, Sept. 7, 2019, https://www.hollywoodreporter.com/thr-esq/how-hollywood-can-can-t-fight-back-deepfake-videos-guest-column-1237685.

[27] N.Y. A5605/S5959, https://www.nysenate.gov/legislation/bills/2019/a5605/amendment/b.

[28] David Singer & Camila Connolly, *How Hollywood Can (and Can't) Fight Back Against Deepfake Videos*, The Hollywood Reporter, Sept. 7, 2019, https://www.hollywoodreporter.com/thr-esq/how-hollywood-can-can-t-fight-back-deepfake-videos-guest-column-1237685.

individuals whose likenesses are used in manipulated media.[29] Rights holders of all kinds will want to consider this evolving area of law and the specific facts of particular manipulated media to ensure the protection of their intellectual property.

Cybersecurity Insurance

According to a recent survey of 500 senior executives, 76 percent of companies in the United States reported having cybersecurity insurance—although only 32 percent of U.S. firms said their cybersecurity insurance covers all risks.[30] While the details of these policies vary, cybersecurity insurance typically covers financial losses that result from data breaches and other cyber events. Insurance may cover the loss or damage to electronic data; the loss of income; the costs of extortion, notification, and reputational repair; and regulatory or litigation costs associated with the hack.[31]

These policies have not historically covered damage wrought by disinformation that targets private brands, corporate officers or businesses. As these threats grow, businesses will want to consider how to modify or supplement their current insurance policies to address all of their business risks and liabilities.

Falsified Court Evidence

Highly realistic manipulated media pose a new challenge to the authenticity of evidence admitted into court. New Federal Rules of Evidence 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 certain manner.[32] But if the qualified person is tricked by the false evidence or lying about an AI-generated video, false media could be introduced as evidence. And the jury may believe it, even if they are told to be skeptical. Soon one can imagine the rise of dueling experts in court debating whether trial evidence is a deepfake or not.[33] Judges will also need to be

[29] *WIPO Raises Questions About Artificial Intelligence and Copyright*, Torrent Freak, Dec. 16, 2019, https://torrentfreak.com/wipo-raises-questions-about-artificial-intelligence-and-copyright-191216/ (the WIPO comment period closed on Feb. 14, 2020); *USPTO Questions if Artificial Intelligence Can Create or Infringe Copyrighted Works*, Torrent Freak, Nov. 7, 2019, https://torrentfreak.com/uspto-questions-if-artificial-intelligence-can-create-or-infringe-copyrighted-works-191107/ (the USPTO comment period closed on Jan. 10, 2020).

[30] *FICO Survey: Most US Firms Have Cybersecurity Insurance — But Only 1 in 3 Say It Is Full Coverage*, FICO Press Release, Aug. 21, 2018, https://www.fico.com/en/newsroom/most-us-firms-have-cybersecurity-insurance-but-only-1-in-3-say-it-is-full-coverage.

[31] *See generally* Marianne Bonner, *What Does a Cyber Liability Policy Cover?*, The Balance Small Business, Dec. 9, 2019, https://www.thebalancesmb.com/what-s-covered-under-a-cyber-liability-policy-462459.

[32] Federal Rule of Evidence 902(13); *see also* Fed. R. Evid. 902(14).

[33] Theodore F. Claypoole, *AI and Evidence: Let's Start to Worry*, The National Law Review, Nov. 14, 2019, https://www.natlawreview.com/article/ai-and-evidence-let-s-start-to-worry; Riana Pfefferkorn, *Too Good to Be True?*, NW Lawyer, September 2019, at 22, 24 ("The deepfakes arms race is sure to spawn a cottage industry of expert witnesses who can assess disputed videos.").

trained to scrutinize potentially manipulated media carefully. For example, recently, 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. The incident points to the new risks of crediting such evidence uncritically.[34]

Regulatory Scrutiny

Recently, some companies have been developing or acquiring deepfake technology for innocuous uses[35]—including a new app that allows users to swap a celebrity's face onto the user's video selfie, so the user can impersonate the star.[36] These technologies may draw greater regulatory scrutiny as Congress and state legislatures pass laws governing certain types of deepfakes. For example, California now prohibits certain nonconsensual pornographic deepfake media and certain deepfakes related to elections; Texas has adopted a criminal law making it a misdemeanor to produce and distribute certain deepfakes around public elections; and Virginia has made it a misdemeanor to distribute "falsely created" deepfake pornography. Other state legislatures and the U.S. Congress are considering further legislation to regulate manipulated media either through civil or criminal laws. These regulations may impact the terms and conditions companies place on deepfake tools and otherwise increase the need for close legal and business scrutiny of such technologies.

POTENTIAL CAUSES OF ACTION

While free speech rights protect opinion, businesses and individuals may have legal recourse, particularly when third parties defame private individuals or benefit financially from spreading lies. State and federal laws bar many kinds of online hoaxes. Laws that could be applicable, especially to deepfakes that falsely depict individuals engaged in demeaning and embarrassing conduct, may include the following:

---

[34] Patrick Ryan, *'Deepfake' Audio Evidence Used in UK Court to Discredit Dubai Dad*, The National (UAE), Feb. 8, 2020, https://www.thenational.ae/uae/courts/deepfake-audio-evidence-used-in-uk-court-to-discredit-dubai-dad-1.975764.

[35] Corinne Reichert, *Snap Reportedly Acquires a Deepfake Startup*, CNET, Jan. 3, 2020, https://www.cnet.com/news/snap-reportedly-acquires-a-deepfake-startup/; Josh Constine, *ByteDance & TikTok Have Secretly Built a Deepfakes Maker*, Tech Crunch, Jan. 3, 2020, https://techcrunch.com/2020/01/03/tiktok-deepfakes-face-swap/.

[36] Zane Mathews, *Fun or Fear: Deepfake App Puts Celebrity Faces in Your Selfies*, Kool 107.9 FM, March 6, 2020, https://kool1079.com/fun-or-fear-deepfake-app-puts-celebrity-faces-in-your-selfies/ (describing "Impressions.app").

- Defamation;
- Trade Libel;
- False Light;
- Violation of the Right of Publicity;
- Intentional Infliction of Emotional Distress; and
- Right of Publicity (if the deepfake material contains the image, voice or likeness of a public figure).

Disinformation and deepfakes that harm a victim's commercial activities may also be actionable under widely recognized economic and equitable torts, including the following:

- Tortious Interference with Prospective Economic Advantage;
- Unfair and Deceptive Trade Practices; and
- Unjust Enrichment.

Federal laws may be applicable if the disinformation misappropriates intellectual property. The Lanham Act prohibits the use in commerce, without the consent of the registrant, of any "registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods" in a way that is likely to cause confusion. The Lanham Act also prohibits infringing on unregistered, common-law trademarks.[37] And the Copyright Act, which protects original works of authorship, may provide remedies if the manipulated media is copyrighted.[38]

Finally, recently enacted laws in California provide private causes of action to victims of some nonconsensual deepfake pornography 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. These may also be applicable, depending on the circumstances. None of these laws disturb the immunity social media platforms have under federal law to liability for the information provided by others on their platforms, and several proposed and enacted laws related to deepfakes specifically recognize and extend that immunity.

BEST PRACTICES

What can companies do to protect their brands and valuations from disinformation and deepfakes? Companies need to tailor their efforts to the risks they face, and they

[37] 15 U.S.C. § 1114(1)(a).
[38] 17 U.S.C. §§ 101-810.

should discuss strategies with counsel. But the following are seven general practices they may want to adopt:[39]

1. *Engage in social listening.* Companies should understand how their brands are perceived on social media to get advance warning of any effort to spread disinformation.
2. *Do a self-assessment.* Private businesses need to look in the mirror and ask: What upcoming events carry the greatest risk? What aspects of the business are most vulnerable to attack? What messages (both good and bad) would have the most resonance?
3. *Register your trademarks.* Given the strong protection federal law provides for intellectual property, companies should preemptively register their trademarks and trade dress, before they are manipulated by bad actors.
4. *Prepare.* A business will be handicapped in carrying out an effective response strategy if it begins to consider the problem only *after* their employees fall victim to identify theft or fraud or after bogus tweets start trending. It needs to prepare for such events, similar to how a business plans for phishing attacks and cybersecurity breaches. It should assign responsibilities to members of an incident response team. Run drills. And consider using technology to make videos of C-suite executives harder to manipulate.
5. *Engage with social media platforms.* If a business sees disinformation about it spreading online, it should consider contacting the social media platforms being used to spread it. Sometimes such disinformation violates the platforms' terms of service and can be removed.
6. *Communicate your message.* Companies should speak directly to their customers, the media and the public. They should line up third-party validators, proactively engage regulators and, as needed, make SEC disclosures.
7. *If necessary, go to court.* Free speech rights protect opinions, but businesses are not defenseless when their brands are defamed or their markets are manipulated.

CONCLUSION

Disinformation and deepfakes pose serious and growing business and legal risks across a range of issues for companies of all sizes. While businesses are not defenseless in this new and different information environment, protecting entities and individuals will require forward thinking, preparation, and diligence.

---

[39] *See generally* Matthew F. Ferraro, *Disinformation Is Harming Businesses. Here Are 6 Ways to Fight It*, CNN, June 10, 2019, https://www.cnn.com/2019/06/10/perspectives/disinformation-business/index.html.