Trending Stories

Sidewalk Toronto Goes Sideways: Five Lessons for Digital Governance (https://protegopress.com/sidewalk-toronto-goes-sideways-five-lessons-for-digital-governance/)

Deep fake at glitched background. Vector, eps 10

DISINFORMATION (HTTPS://PROTEGOPRESS.COM/CATEGORY/DISINFORMATION/)

Taking the Wide-Angle View of the Business and Legal Risks of Disinformation and Deepfakes

By Matthew F. Ferraro (https://protegopress.com/author/matthew-ferraro/) 3 months ago

In the midst of the coronavirus pandemic—as markets struggle (https://www.nytimes.com/2020/03/31/business/coronavirus-stock-market-updates.html), schools and businesses shutter (https://www.baltimoresun.com/coronavirus/bs-md-hogan-home-order-takeaways-20200330-svso6o5navaznmafxuf3tztmsa-story.html), and the healthcare system strains under the weight of increased morbidity and mortality—the world confronts another viral threat: a torrent of disinformation about the virus itself. In what the World Health Organization has labeled an "infodemic (https://www.nytimes.com/2020/02/06/health/coronavirus-misinformation-social-media.html)," charlatans have pushed alarmist, false information about the disease via social media and text messages. The Trump Administration leveled claims that foreign states (https://www.nytimes.com/aponline/2020/03/16/us/politics/ap-us-virus-outbreak-disinformation.html?searchResultPosition=2) are behind phony claims that a nationwide quarantine is in the offing and took legal action (https://www.reuters.com/article/us-health-coronavirus-usa-fraud/u-s-says-website-offered-phony-coronavirus-vaccines-idUSKBN21915G) against some pushing "cures".

The Facebook Oversight Board: A significant step for Facebook and a small step for freedom of expression (https://protegopress.com/the-facebook-oversight-board-a-significant-step-for-facebook-and-a-small-step-for-freedom-of-expression/)

The Bright Line Platforms Should Draw Around Election Misinformation (https://protegopress.com/the-bright-line-platforms-should-draw-around-election-misinformation/)

Systemic Racism Is a Cybersecurity Threat (https://protegopress.com/systemic-racism-is-a-cybersecurity-threat/)

The Case for A New Resume (https://protegopress.com/the-case-for-a-new-resume/)

The disinformation spreading about the coronavirus is the latest example of an ancient vice (innuendo, rumor, false witness) given new life in our interconnected age. Too often, the conversation about disinformation has been restricted to a few well-known use cases—fake news about electoral candidates or manipulated media of Hollywood celebrities.

On March 12, 2020, two WilmerHale (https://www.wilmerhale.com/en) colleagues and I published a Client Alert to broaden the aperture of our discussion of issues surrounding misinformation: "***Identifying the Legal and Business Risks of Disinformation and Deepfakes: What Every Business Needs to Know*** (https://www.wilmerhale.com/en/insights/client-alerts/20200312-identifying-the-legal-and-business-risks-of-disinformation-and-deepfakes-what-every-business-needs-to-know)," which is forthcoming as well in Pratt's Privacy and Cybersecurity Law Report (https://store.lexisnexis.com/products/pratts-privacy-cybersecurity-law-report-skuusSku22150403).

Our goal is to explain the many legal and business exposures private entities face from disinformation and deepfakes, or artificial intelligence (AI)-manipulated media. We show the many different ways the contemporary information environment can threaten businesses, and what they can do about them.

We note that disinformation is not an issue associated merely with social media. 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. Solutions to these challenges go beyond what social media platforms can do alone, especially when such media is spread by email, telephone or offline, or intended for innocuous purposes—like an AI-enabled face-swapping app that can be innocent fun but also implicate another's right to publicity or be used to defraud.

We review eleven key risk areas:

1. **Reputational Damage.** Disinformation about companies can negatively impact brand identities and harm valuations.
2. **Extortion and Harassment.** Over 95 percent of all deepfake videos now on the internet are of nonconsensual pornography—a nonconsenting person's face on a nude body. Such images can be used to extort or embarrass individuals, including business leaders.
3. **Social Engineering Fraud.** Recent accounts of fraudsters using AI-manipulated audio to trick victims into sending them money illustrate a growing risk in this area. These swindles represent a variant of what has been called "business email compromise," where someone impersonates an employee's email account to trick a company official into sending money to the scammer. Through these cons, 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 potentially loss of access to the capital markets.
4. **Credential Theft.** Through convincing impersonation, bad actors can extract information technology credentials from unwitting corporate employees. With these credentials, they may be able to steal valuable company information. Hackers could also lace company computer systems with malware or ransomware.
5. **Market Manipulation.** Fraudsters long ago discovered how to make money using regular disinformation to move the financial markets. We describe several examples of disinformation being used in pump-and-dump and short-selling schemes. The dangers of these scams will only grow as believable manipulated media (perhaps a fake video of a CEO announcing a merger) can be made at scale.
6. **Insurance Fraud.** The insurance industry often relies on the veracity of digital media to adjudicate claims. Research about the potential use of AI-manipulated radiology scans for insurance fraud demonstrates just one of a number of liabilities in this area.
7. **Labor and Employment Issues.** Employees are relying increasingly on clandestine recordings to support their claims of harassment or mistreatment. 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. Companies will need to prepare for this potential additional layer of legal and business risk.
8. **Entertainment Industry Issues.** Content creators may wish to use AI-enabled manipulated media as part of their expressive works, while actors will seek to protect their digital likenesses from studio use without their consent. Navigating this tension, and evolving regulations, will take deliberation. So too will questions of who owns deepfakes, which are often created by stitching together material that is copyrighted.

9. **Cybersecurity Insurance.** While the vast majority of businesses have cybersecurity insurance, very few policies address the threat of disinformation. Businesses will want to consider how to modify or supplement their current policies to address these issues.
10. **Falsified Court Evidence.** Highly realistic falsified media pose challenges to the authenticity of evidence admitted into court. Court rules will need to adapt, and judges will need to be trained to scrutinize carefully potentially manipulated media.
11. **Regulatory Scrutiny.** Recently, some companies have developed deepfake technology for innocuous, commercial uses. These technologies may draw greater regulatory scrutiny as Congress and state legislatures pass laws to govern certain types of deepfakes.

In addition to spotting the legal and business risks, we also identify 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 tort laws, federal intellectual-property protections, or laws enacted within the past year that specifically address deepfakes. Finally, the paper reviews seven best practices businesses can undertake today to prepare for these hazards.

Protecting private entities and individuals from the risks of disinformation and deepfakes will take new thinking, preparation and diligence. Identifying the threat vectors, reasonable responses, and prudent preparatory measures are important places to start. Our full Client Alert is available **here** (https://www.wilmerhale.com/en/insights/client-alerts/20200312-identifying-the-legal-and-business-risks-of-disinformation-and-deepfakes-what-every-business-needs-to-know) and via **PDF** (https://wilmerhalecommunications.com/e/wgeeoxlxy5yscnq/54f2fee4-2df9-4408-92bf-ed6bdf8dccc4).

PREVIOUS
SOCIAL MEDIA FUELS WAVE OF CORONAVIRUS MISINFORMATION AS USERS FOCUS ON POPULARITY, NOT ACCURACY (HTTPS://PROTEGOPRESS.COM/SOCIAL-MEDIA-FUELS-WAVE-OF-CORONAVIRUS-MISINFORMATION-AS-USERS-FOCUS-ON-POPULARITY-NOT-ACCURACY/)

NEXT
SMOKE SCREENS: AN INITIAL ANALYSIS OF THE CORONAVIRUS LAWSUITS IN THE UNITED STATES AGAINST CHINA AND THE WORLD HEALTH ORGANIZATION (HTTPS://PROTEGOPRESS.COM/SMOKE-SCREENS-AN-INITIAL-ANALYSIS-OF-THE-CORONAVIRUS-LAWSUITS-IN-THE-UNITED-STATES-AGAINST-CHINA-AND-THE-WORLD-HEALTH-ORGANIZATION/)

YOU MAY ALSO LIKE

(https://protegopress.com/the-bright-line-platforms-should-draw-around-election-misinformation/)
DISINFORMATION (HTTPS://PROTEGOPRESS.COM/CATEGORY/DISINFORMATION/)
ELECTION SECURITY (HTTPS://PROTEGOPRESS.COM/CATEGORY/ELECTION-SECURITY/)

THE BRIGHT LINE PLATFORMS SHOULD DRAW AROUND ELECTION MISINFORMATION (HTTPS://PROTEGOPRESS.COM/THE-BRIGHT-LINE-PLATFORMS-SHOULD-DRAW-AROUND-ELECTION-MISINFORMATION/)
BY **DANIEL KREISS (HTTPS://PROTEGOPRESS.COM/AUTHOR/DANIEL-KREISS/)** AND **BRIDGET BARRETT (HTTPS://PROTEGOPRESS.COM/AUTHOR/BRIDGET-BARRETT/)** 7 DAYS AGO

(https://protegopress.com/covid-19-misinformation-and-disinformation-responses-sorting-the-good-from-the-bad/)
DISINFORMATION (HTTPS://PROTEGOPRESS.COM/CATEGORY/DISINFORMATION/)