Disinformation and Deepfakes Risk Management (DDRM)

Fake Viral Narratives and Synthetic Media Pose Risks to Business

Fast-spreading disinformation and the growing ease with which believable deepfake media can be created are threats that are poised to accelerate a range of business dangers, particularly those related to reputational risk, market manipulation and social engineering fraud. Businesses must have strategies in place to prepare for and respond to these challenges. At the same time, with synthetic media offering an array of innovative applications that can be used in legitimate ways, companies that want to benefit from the positive applications of deepfake technology must carefully assess the business and legal challenges of its use.

A GROWING BUSINESS RISK

The world is awash in disinformation, seemingly about everything. What scholars call "information disorder" has most obviously impacted politics, but the dangers reach much further—to individuals and to corporate America. In recent years, we have witnessed the emergence of growing threats to businesses of all kinds through the proliferation of viral false information and believable synthetic media (deepfakes) targeting the private sector. These new hazards require innovative business and legal responses, a collection of defenses that we refer to as ***disinformation and deepfakes risk management (DDRM)***.

Boards of directors, business executives and general counsel must understand these risks and position their companies to address them in a cost-effective manner. WilmerHale is at the forefront of this evolving field and works with companies across multiple industries to prepare for and respond to these challenges. DDRM requires a multifaceted and coordinated effort involving cybersecurity planning, forensic analysis and communications strategy to address potential reputational harm and communicate with all relevant constituencies, and judicious counsel who can prepare for the range of regulatory inquiries and litigation that may arise in the United States and other countries in response to the malicious use of disinformation and deepfakes.

UNDERSTANDING THE ISSUES

Disinformation in this context means the spreading of outright falsehoods, personal data or decontextualized information to mislead business partners, customers and the public.

Deceit is an ancient vice, but technology now allows believable falsehoods to spread faster and farther than ever before in human history. The growing ease with which believable deepfake media can be created threatens to accelerate a range of business dangers, particularly those related to reputational risk, market manipulation and social engineering fraud.

WILMERHALE®

Reputational Risk. Viral disinformation and deepfakes exacerbate the reputational challenges companies already face. Today, online conversations drive brand identities, and companies are increasingly taking positions on hot-button issues, making them prime targets for disinformation.

For example, in the summer of 2020, a QAnon-adjacent conspiracy theory circulated online that the furniture seller Wayfair was involved in child trafficking, due to the coincidental overlap of the names of some of Wayfair's products and those of missing children. Social media accounts posted addresses and maps of Wayfair's offices and profiles of its employees, and the names attempt was made to orchestrate a boycott and a campaign to short the company's stock.

Likewise, conspiracies metastasized online falsely asserting that 5G cell towers contributed to the spread of the coronavirus, instigating off-line violence against corporate assets, including dozens of arson attacks on towers and the harassment of telecommunications employees. The US Department of Homeland Security even issued an industry warning about the situation.

SUPPORTING POSITIVE USES OF DEEPFAKE TECHNOLOGY

There are many exciting positive applications of synthetic media. Increasingly, new and existing companies are using this technology in innovative ways to advance advertising, customer and employee engagement, and the arts. WilmerHale can help businesses at any stage of the corporate life cycle—from startups to industry leaders—address the business and legal challenges associated with this emerging field and its application to the metaverse, blockchain technology, nonfungible tokens, or NFTs, and other cutting-edge uses.

For example, because deepfakes often derive from copyrighted images, businesses that want to use them for commercial purposes will need to consider the provenance of source data, secure appropriate licenses and ensure protection for their own derivative media. Likewise, as synthetic media products and services come to market, businesses should consider the bounds they should place on their products to address the ethical and legal risks of employing realistic false media. Already, eight states prohibit deepfakes in some form and many others are considering such legislation. Manipulated media is quickly becoming a government-regulated field, requiring specialized counsel and, where necessary, public policy advocacy. WilmerHale works at the nexus of business, regulation and public policy and can help companies design manipulated media policies that are informed by the very latest developments.

And as one of its many reproofs of Western coronavirus pharmaceuticals, Chinese state media criticized the safety of Pfizer's COVID-19 vaccine and in January 2021 called 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 accompanied by believable synthetic video of a business leader seeming to use a racial epithet in an "undercover" video released on the eve of a major product launch, 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 false information about companies to drive stock prices. Manipulators now benefit from the increasing power of social media and meme stocks to drive market movements. For example, in December 2020, the Securities and Exchange Commission charged a Georgia man and several others for boosting false rumors of impending mergers and acquisitions through online posts that temporarily goosed the companies' stocks, to the defendants' profit.

Again, these crimes are likely to be even more damaging once malefactors leverage synthetic media to broadcast believable videos to push fake business news.

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.

The FBI has warned companies that such impersonations 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 will also leverage deepfake technology to conduct business identity compromise, in which deepfake tools will be used to impersonate employees to harm businesses.

PREPARATION AND RESPONSE

Businesses are not defenseless against disinformation and the risk of deepfakes. WilmerHale works with clients to prepare for and mitigate these new dangers across a range of disciplines—cybersecurity, crisis management, regulatory counseling and litigation, among others.

The business community should plan for disinformation and deepfakes risk like it plans for any number of cyberattacks or crisis events. Companies should proactively communicate accurate, positive messages about their business on social media, monitor how their brands are perceived online, and conduct self-assessments to understand the narratives that would be the most compelling against them. Businesses should work with counsel to amend crisis plans to manage disinformation dangers, assign roles and responsibilities to executives, train employees to detect deepfake scams, and practice corporate responses. They should also register their trademarks and copyrights because of the heightened protections available for registered intellectual property (IP). If IP is misused, registered owners can more easily have infringing posts taken down from social media sites and will have access to a greater range of remedies in litigation.

During an incident, a victim may wish to work with counsel to engage with social media platforms to request assistance in stopping the spread of false narratives. When suitable, a business should counter phony speech with accurate, positive messages about the company and consider publicly disclosing that it is being targeted by disinformation.

Finally, after a disinformation campaign, market manipulation or social engineering fraud, companies should work with counsel to notify their regulators, shareholders, customers, partners and workforce. If appropriate, victims may wish to advise law enforcement and/or bring legal action against disinformation purveyors to enforce their rights.

$78B

lost each year to private firms due to disinformation

- including **$9 billion** a year companies and individuals spend trying to repair reputations damaged by falsehoods
- including **$17 billion** lost due to financial disinformation[1]

88%

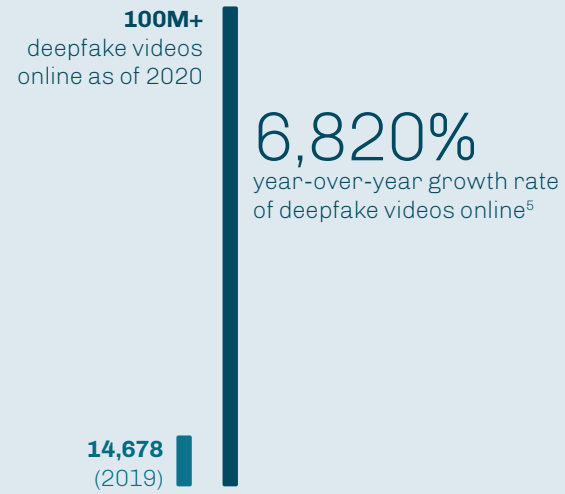
of investors consider disinformation attacks on corporations a serious issue[2]

53%

of US respondents agreed that "CEOs and business leaders should do whatever they can to stop the spread of misinformation, even if it comes from public officials"[3]

25%

of respondents thought business leaders were currently doing enough[4]



For more information, please contact:

Matthew F. Ferraro — matthew.ferraro@wilmerhale.com
Jason C. Chipman — jason.chipman@wilmerhale.com
Jason L. Kropp — jason.kropp@wilmerhale.com
Stephen W. Preston — stephen.preston@wilmerhale.com
Louis W. Tompros — louis.tompros@wilmerhale.com

[1] Michelle Castillo, *Exclusive: Fake News Is Costing the World $78 Billion a Year*, CHEDDAR (Nov. 18, 2019, 11:53 AM), https://cheddar.com/media/exclusive-fake-news-is-costing-the-world-billion-a-year.
[2] Robert Moran, Preston Golson, and Antonio Ortolani, *Enter the Imposter*, BRUNSWICK REV. (Sept. 18, 2019), https://www.brunswickgroup.com/disinformation-attacks-insight-research-integrity-i12018/.
[3] Preston Golson, *The Disinformation Wildfire*, BRUNSWICK REV. (May 5, 2021), https://www.brunswickgroup.com/disinformation-wildfire-i18810/.
[4] *Id.*
[5] SENTINEL, Deepfakes 2020: The Tipping Point 7 (2020), https://thesentinel.ai/media/Deepfakes%202020:%20The%20Tipping%20Point,%20Sentinel.pdf.

22_0230 4/22