CORPORATE COUNSEL
The Business Magazine for In-House Counsel
corpcounsel.com | December 13, 2021

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 deceits 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 valences that make them prime targets for disinformation purveyors.

/iStockphoto

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 orchestra 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 cyberhacks 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.*