Deepfakes and Other Disinformation Pose Growing Business Threats, Say WilmerHale Lawyers

JULY 2, 2019

Partners Jason C. Chipman and Brent J. Gurney and Senior Associate Matthew F. Ferraro presented a webinar on what Chipman called "a growing problem for companies around the world": sophisticated disinformation campaigns aimed at harming brands, manipulating the market and shifting political opinions.

In the June 20 webinar, "Hard Truth: Disinformation Threatens Business," the lawyers discussed how companies can prepare for such attacks and how they can manage the aftermath. The audience primarily included representatives from major banks and financial services companies, as well as healthcare and aerospace businesses, among others.

"It's an old problem—people have tried to trade on rumor, innuendo, false information and propaganda for a long time," said Chipman, who counsels clients on data security and cyber incident response. "But now the speed at which information can move and the scale at which it can spread can create problems for businesses."

Ferraro, a former US intelligence officer who has published widely on the issue (including with Chipman in *The Washington Post*), offered many examples of real-life disinformation campaigns. These ranged from antivaxxers who attacked a pediatric clinic on social media after the clinic shared information about the HPV vaccine, to profiteers who circulated a doctored Bloomberg article about a phony takeover of a social media company that drove up share prices, to Russian state–backed "news" reports aimed at undermining US investments in 5G technology by claiming, without evidence, that the technology poses serious health risks.

Ferraro also noted the "more significant threat" presented by altered photos and videos, particularly so-called "deepfakes," which use artificial intelligence to create forged videos of people saying things they never said and doing things they never did. He cited research estimates that, in a mere 18 to 24 months, it will be possible to create deepfakes that are "nearly indecipherable" to the human brain.

"Imagine what could happen to an IPO or a product launch if a deepfake of a CEO saying something embarrassing or incriminating was circulated right before," said Ferraro. "There's also the threat

that deepfakes will be submitted as evidence in litigation."

Chipman then discussed how businesses can prepare for and mitigate the effects of such incidents. "It's similar in many ways to how we think about cyber threats," he said. "IT departments all the time deal with threats to information systems—most of the times those are run-of-the-mill problems, but sometimes they are not. When that happens, it's very important that organizations have a response plan that accounts for the scope of the threat and that has a role for the component entities within the organization."

Litigation can be a valuable part of that plan, noted Gurney, who broke down potential claims that companies could bring if targeted. He also emphasized the importance of preparation: "Companies should get ahead of this in tabletop exercises or crisis planning and consider likely ways in which [they] might be attacked, the best venues for litigation, and the best jurisdictions in terms of caselaw and precedent," he said. "Given the speed at which things happen, it can be a significant detriment if you wait until you're already in the middle of crisis."

Watch the full webinar.