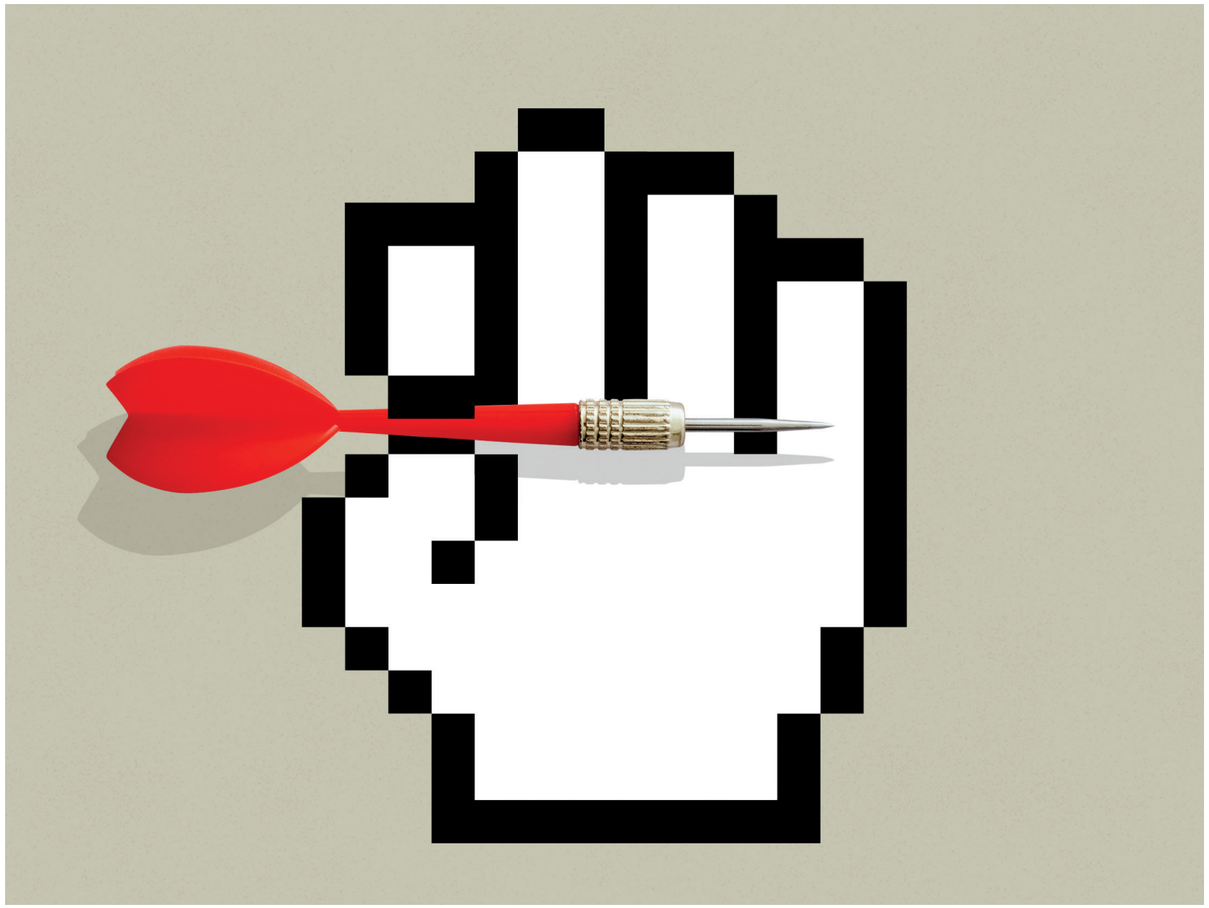


TARGET of Disinformation

WilmerHale attorneys **JASON CHIPMAN** and **MATTHEW F. FERRARO** talk fake news attacks and the law with Brunswick's **PRESTON GOLSON.**

Much has been made about the rise of fake news – false reports that look like genuine news articles – and the threat it poses to elections and democracy in general. Less well understood is the role disinformation can play in damaging the reputations of private corporations and institutions. Ill-timed disinformation attacks – perhaps around an IPO, key investor meeting, merger or product launch – could result in a significant loss of value.

For example, in April 2016, a clickbait site posing as TV news published false reports that Coca-Cola's bottled water brand Dasani was being recalled because of the presence of a parasite in the water that purportedly caused "several hundred" hospitalizations. As an illustration, standing in for an actual parasite, the hoax story carried a spooky image of a flat and transparent eel larva.

Falsehoods in the marketplace have a long history. What's different now is the ease with which they can spread. True, opinion is protected by free speech rights, but corporations are not defenseless against intentional distortion, especially when used to enrich another party.

We asked WilmerHale Partner Jason Chipman and Senior Associate Matthew F. Ferraro, who are both visiting fellows at the National Security Institute at George Mason University, for their thoughts and insights into what legal options C-suites may consider when faced with a crisis brought about by disinformation attacks.

What kind of threats do businesses face from fake news?

Fake news is just a new way to refer to an old problem of false reports, misinformation, innuendo and smears, all of which can threaten corporations in profound ways. We generally group these threats into three categories. First are individuals motivated by animus, ideology or a simple desire to make trouble. They operate largely independently and do not seek remuneration or ransom but merely the satisfaction of damaging corporate brands they dislike. These actors leverage near-anonymous social media, like 4Chan, to find like-minded confederates and utilize specialized, "news article"-producing websites to target brands with relatively slick content.

In August 2017 for example, agitators launched a bogus campaign against Starbucks with tweets advertising "Dreamer Day," that claimed the coffee company's US stores would give out free Frappuccinos to undocumented immigrants. Advertisements, complete with the company's logo, signature font and pictures, raced around the web with the hashtag "#borderfreecoffee." It was all a hoax dreamt up by a rabble-rouser on 4Chan who wanted to inflict pain on what he called a "liberal place."

The second group covers actors who seek some defined benefit by engineering the release of misleading information. These individuals might aim to accrue advertising dollars by pushing traffic to websites or videos. Think salacious, attention-grabbing clickbait headlines that sound too good to be true – because they are. Similarly, false or misleading stories released at the right moment can drive down stock prices and provide opportunities for stock shorts and other financial windfalls.

In October 2018, for example, shares of both Broadcom and CA Technologies briefly plunged after a memo purporting to be from the US Department of Defense appeared, which said that the Committee on Foreign Investment in the United States (commonly known as CFIUS) would review Broadcom's $19 billion acquisition of CA Technologies. But according to press accounts, the memo was a forgery. Neither the DoD nor CFIUS were reviewing the deal. It is not clear who authored the phony document, but short sellers would have profited handsomely from the dip.

The third group includes state-backed actors. While we have seen no public evidence of them targeting private companies with fake news, it may be only a matter of time. One can easily imagine foreign cyber operations targeting the reputation of American companies with disinformation campaigns that seek to damage their brands and drive business to a foreign country's national champion.

Going forward, it will be critical for corporations to know how to navigate a world in which deceptive "news" stories propagated by all of these actors can race around the world at the speed of light, threatening reputations and revenue streams.

Have there been any digital disinformation cases where bad actors have been found or convicted?

This is a relatively new phenomenon with no obvious examples where purveyors of "fake news" were held liable for false reports. But trafficking in innuendo and libel is an ancient vice and current laws provide significant protection and well-established causes of action that can likely be employed. It is just a matter of applying proven strategies to new contexts. Consider the potential applicability of the following causes of action, among others.

Defamation and Trade Libel. There are many cases where courts have sustained claims for defamation against people who post smears on customer review websites. The same logic would apply to people who manufacture genuine-looking news articles that are just dressed-up libel. False statements denigrating the quality of a company's goods or services may also give rise to a claim for another tort known variably as trade libel, injurious falsehood or product disparagement. These torts are broader than pure defamation because they are not typically confined to false statements that damage a company's reputation.

Economic and Equitable Torts. State laws protect against malicious and dishonest interference in another party's future business relationships, which is essentially what fake news targeted at corporations

ILLUSTRATION: EDMON DE HARO

does. For example, the "Dreamer Day" hoax was intended to harm Starbucks' business with third-party patrons of their stores. Similarly claims for deceptive trade practices and unjust enrichment could also likely be made against unscrupulous short sellers who rely on fake news to drive down stock prices.

Intellectual Property Law. Federal trademark infringement laws could provide a cause of action against anyone who posts a fake news item which incorporates a company logo to make an "article" or post look genuine, because the poster would be using a trademark in a manner that would be likely to cause confusion among consumers.

The purveyors of disinformation are often overseas. Does international law offer any recourse for businesses?

This is a global problem, and that poses a hurdle to successful suits in US courts, but it can be surmounted, depending on the facts of the case. Furthermore, many countries have protections similar to those found in US law.

When is suing or seeking law enforcement action useful to counteract disinformation?

This is an important question that each client must answer for itself. It's important to consider remedies short of litigation, as well. For example, engaging with web-hosting platforms may reveal potential remedies to limit the damage from false stories. Where litigation is being considered, key issues to evaluate include:

1. **Jurisdiction.** Does the hoaxer reside in the US or have sufficient contacts with the country to establish jurisdiction?
2. **Ability to pay.** Is the defendant judgment proof? Do they have any funds to pay a civil award if they are found liable?
3. **Time and expense.** Litigation can be expensive and slow. A client will need to consider whether the effort is worth it in time and money.

On the other hand, litigation not only can vindicate a corporation's rights but also deter other malefactors from similar behavior, bring to light valuable information about opponents, or expose wrongdoing to the press and the marketplace. Businesses will want to consider the facts of each situation and confer with outside counsel before making any moves.

Are there other ways corporations or institutions could respond to digital disinformation?

Fake news poses a serious threat to the integrity of corporate brands and their bottom lines. Like other new phenomena, such as cyber hacking and ransomware, corporations should not wait for the worst to happen before taking proactive steps. We recommend three broad strategies to defend against digital disinformation.

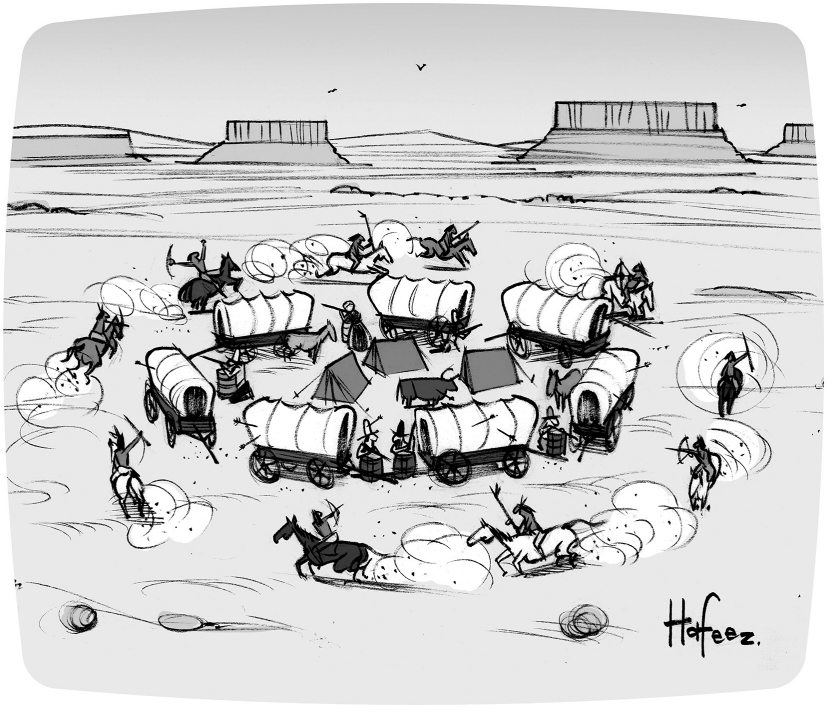
First, prepare. Increasingly, companies prepare for cybersecurity breaches through planning and table-top exercises. In the same vein, now is the time to game-out how a company will handle a fake-news attack. Assign roles to in-house talent who will lead in a crisis. Identify third-party validators who will vouch for the brand. Establish a brand presence on all major social media platforms, from Facebook and Twitter, to Instagram and Snapchat.

Second, proactively engage in the new media environment. Do not be caught flatfooted when an anonymous Twitter troll's misinformation reaches traditional media outlets. Stay attuned to what is being said about you and your brand. Communicate with your customers, business partners, employees and suppliers. Build trust so they know to whom to turn with questions about what's true and fake.

Third, speak for yourself. Be prepared to talk directly to customers and the public at large to debunk fakery. In this context, the solution to bad speech is more direct and credible speech. ◆

"DO NOT BE CAUGHT FLATFOOTED WHEN AN ANONYMOUS TWITTER TROLL'S MISINFORMATION REACHES TRADITIONAL MEDIA OUTLETS."

PRESTON GOLSON is a Brunswick Director based in Washington, DC. He is a former CIA spokesperson.



*"**We** know the cavalry aren't coming, but if we announce it on Twitter, they'll probably **think** the cavalry are coming."*

ILLUSTRATION: KAAMRAN HAFEEZ