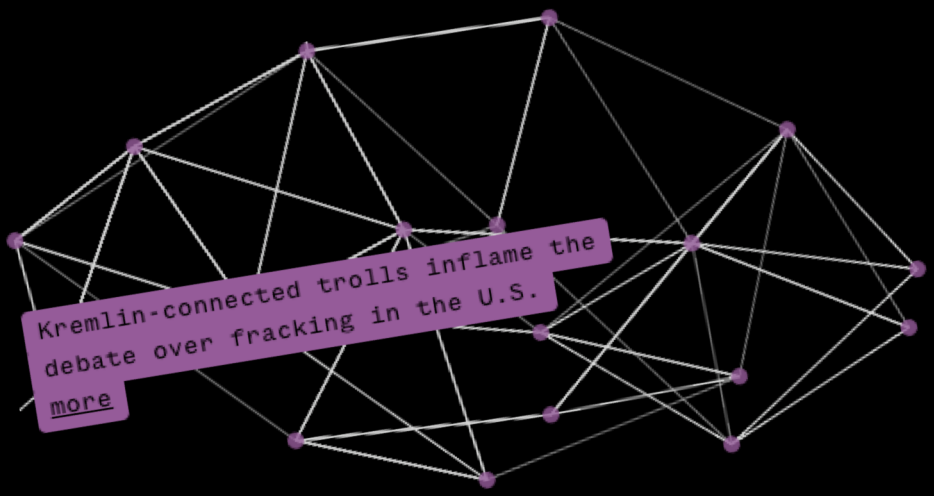
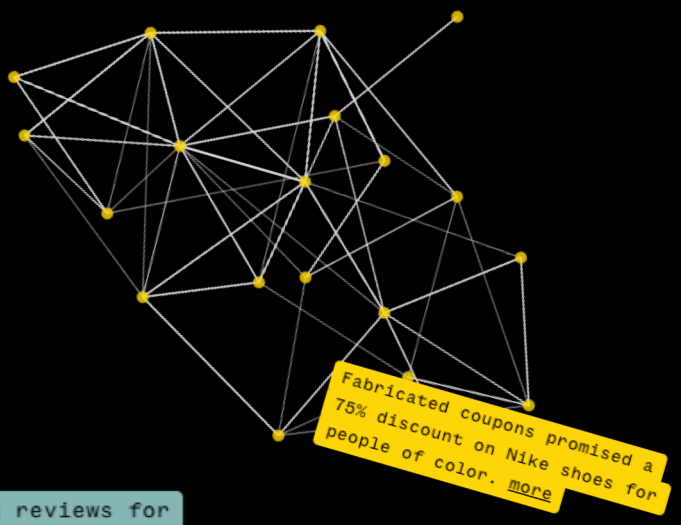
New Knowledge

Brands in the Crosshairs:

The Business Side of Disinformation

March 2019





Summary

In 2019 brands are faced with the problem of disinformation. There is powerful evidence that groups of hyperactive and often ideologically motivated social media users are engaged in coordinated and computational efforts to hijack brands, undermine credibility, and destroy reputations.

The Emerging Threat of Brand Disinformation

If you are part of a high-profile company or industry, your work has likely already been impacted by disinformation. And the problem isn't limited to one social media channel, manipulative campaign, or just a few brands. This is a global, pervasive and systemic issue with far-reaching impact from internet security, corporate business plans, government policies and the personal habits of everyday people.

Why this is everyone's problem

Even if you don't work for a major brand this issue will likely have an impact on you. Through the *Brand Disinformation Impact Study* we see,

- 73 percent of individuals surveyed said they are *highly likely* or *somewhat likely* to do business with a brand that has a positive reputation over a brand that has a negative reputation
- Over 16 percent said they would stop doing business with a brand at the center of a reputation damaging event
- 30 percent said they lose trust in the brand.

An attack on a major brand could durably alter public shopping habits. Lost sales equals lost revenue, which leads to falling stock prices. Even worse, if multiple blue chip companies incur attacks on the same day and their stocks plummet, the reverberations will be felt from Wall Street to our gross national product. How do we know this? It's already happening.

Vulnerable Brands

From big box stores to franchised chains, from pharma to agriculture, established brands with strong name recognition are most vulnerable to organized disinformation attacks. These companies invest considerable resources to work their widely trusted and valued products and taglines into popular culture on social media, in PTA meetings and party conversations, which adds to their exposure.

Why are these Types of Brands Threatened

Not surprisingly, brands and industries with high visibility are the most attractive targets for perpetrators of disinformation. An effort that successfully erodes an established brand launches a parasitic relationship, boosting the manipulative campaign's media exposure merely by getting "ink" alongside the known brand. For brands, it is a lose-lose proposition.

30%

Of consumers say they lose trust in a brand as a result of a brand controversy

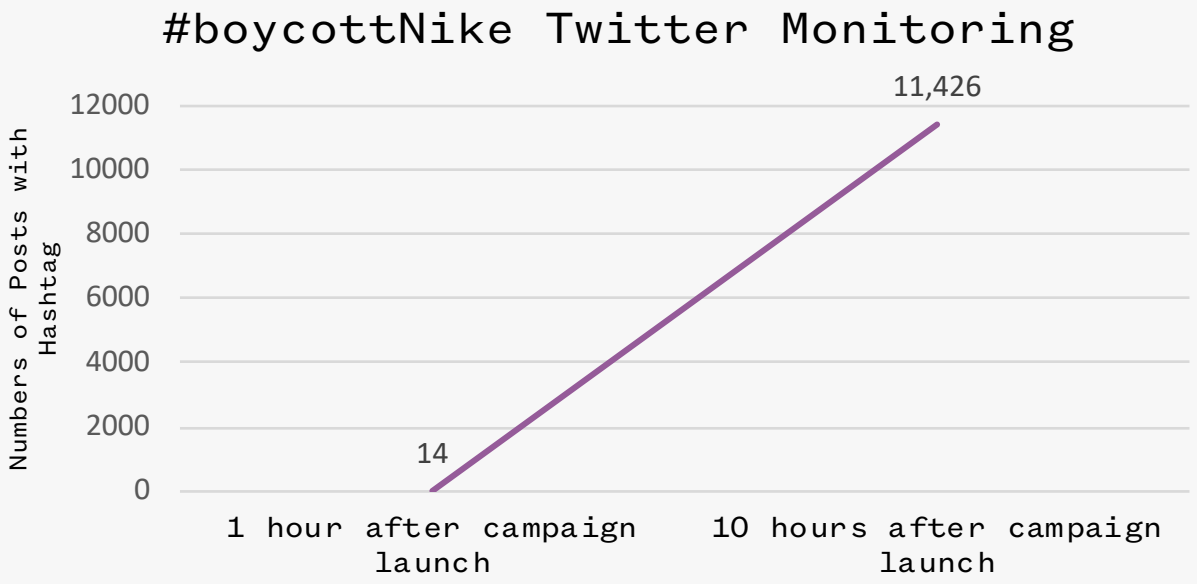
Case Study: Call for Nike Boycott

This fall, Nike chose Colin Kaepernick to appear in the ad campaign honoring the 30th anniversary of the iconic "Just Do It" campaign. The NFL quarterback had become a figure of controversy by repeatedly kneeling during the performance of the national anthem before games. His stated intent in kneeling was to raise awareness about police brutality, social injustice and systemic racism.

The company's controversial choice to feature Kaepernick sparked a strong and immediate response from supporters and detractors on social media. At 2:20 p.m. on September 3, 2018, Kaepernick tweeted a photo of himself featured in the Nike's new marketing campaign. A boycott hashtag #boycottNike spread rapidly after the athlete's initial tweet. At 3:00 p.m., our data indicated just 14 tweets that day contained the same hashtag. By midnight that number had ballooned to 11,426.

That same day, some Twitter users began posting videos of themselves burning Nike merchandise. Several of these posts received tens of thousands of retweets, not only providing a counter-narrative to the original ad, but providing a means for the public to actively participate in the protest. The issue also affected the NFL for whom Nike provides uniforms. Over the next two weeks, more than 58,000 tweets included #NFLboycott.

Only two days into the controversy, Nike officially released the ads featuring Kaepernick. Over a two week period ending on September 17, users tweeted the #NFLboycott hashtag over 120,000 times. On Twitter, between September 3 and September 17, New Knowledge collected over 671,000 tweets which included at least one of several relevant keywords or hashtags associated with Kaepernick or Nike.



Case Study: Call for Nike Boycott Continued

The majority of posts appeared to be positive or neutral, but the volume of activity referencing a boycott was significant.

While the controversy described above originally unfolded organically on social media, representing an authentic PR issue, ideologically driven trolls began planning a hoax on the web forums 4chan and 8chan, aiming their sights at Nike. It began on September 5th when a user posted a fake coupon offering 75% off for the company's products for "people of color." The post was titled "Coupon Hell 2.0", referring to a coupon hoax that occurred in the food industry, which the group discussed several times while crafting the disinformation campaign against Nike.

The creators of the hoax revised the coupon several times, aiming to incite violence among customers at retail stores. At one point, a QR code was added which read, when scanned, "This is a ROBBERY, Move slowly and put all the LARGE bills in the shoe box OR everyone DIES." Like the other coupon campaign, these threads contained calls to action and plans to disseminate the hoax by sending it to high profile Twitter users or national media. But those plans did not gain traction.

By September 7, these plans had lost momentum, with users commenting their disappointment in the lack of follow-through. While this particular campaign failed to significantly materialize, it shows how easy it is to plan disinformation campaigns with the *potential* to cause serious crises for brands. It also illustrates the way in which an authentic PR issue, that needs authentic handling, can be opportunistically leveraged by ideologically driven trolls into a coordinated disinformation campaign that generates a massive mirage of consensus.

Vaccinations, Media, and Mania: Using Misinformation to Amplify a Deadly Argument

Similarly, ideologically driven trolls became active in the anti-vaccination movement. A vehicle of misinformation specifically, this movement has long used messaging riddled with scientific inaccuracies to promote controversial views. Activists often push pseudo-medical and rigorously debunked claims that vaccines cause irreversible conditions and are therefore more dangerous than the diseases they purport to protect us from. Whether they mean well or not, these activists may not know what they send to their social media groups may not be true, and their actions have irreversible repercussions of their own.

The internet enables the ability to publish and possible distribute any idea with trivial ease. Anti-vax narratives perform particularly well on social media, where algorithms reward emotionally provocative personal anecdotes and sensational content — not dry scientific facts. Anti-vaccine narratives are reliably viral, a regrettable and deadly irony. Using social media to amplify messages to reach new audiences, the movement capitalizes on our distributed information ecosystem by writing blogs and cross-promoting content across platforms.

Social media platforms and their gameable algorithms provide a space for the anti-vaccine movement to thrive.

Search functions and recommendation engines readily produce anti-vaccine content that is widely circulated.

The movement is predominantly comprised of people who do not have a professional medical background who are, nevertheless, shockingly comfortable asserting medical opinions on everything from SIDS to autism to cardiac arrhythmia. The dialog includes posts that exploit emotions of vulnerable people, such as the grief of parents who have lost a child. And as provocative nature of this conspiratorial misinformation is spread, we reduce the role of expertise and rigorous science in public discourse.

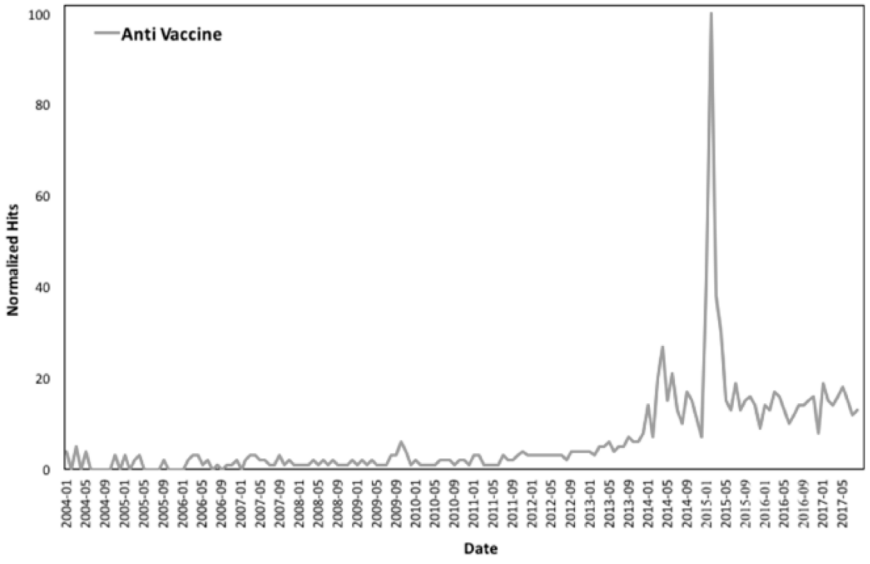


Figure 6. Worldwide Online Interest in the term 'Anti Vaccine' from January 2004 to August 2017.

Case Study: Sudden Death After HPV Vaccine Spurs Online Response and Legal Action

The anti-vaccination community has specifically engaged in a dangerous and misleading narrative that attempts to connect Gardasil to unexpected deaths of teenagers who received the vaccine. The movement claims without scientific support that the drug causes everything from infertility to death.

When Christina Tarsell died after having the Gardasil vaccine, her mother sued Merck. In a legal case, Dr. Yehuda Shoenfeld presented testimony supporting the anti-vaccination position, saying that the HPV vaccine had triggered an autoimmune response that manifested in arrhythmia. But arrhythmia is typically caused by coronary artery disease, vasculitis, metabolic alterations, or damage to the heart in the form of myocarditis. Neither the autopsy nor additional analysis by the CDC found evidence to support that Tarsell had any of those conditions. Despite widely-accepted medical facts, social media groups are rife with posts that promote and defend the anti-vaccination position.

Statistically, young people who pass away prematurely and seemingly without explanation are often victims of an undiagnosed heart defect. The fact that a fatal arrhythmia occurred near the time a vaccine was administered is considered coincidental by most of the medical community.

Case Study: Pumping Disinformation

Foreign disinformation agents have also sought to cause friction and doubt within the U. S. energy dialogue. According to a spring 2018 report released by House Committee on Science, Space and Technology, Russia conducted a coordinated disinformation campaign to influence U. S. domestic energy policies. Analysis revealed social media posts advocating positions circulated specifically to agitate environmentalists and cause tension in the U.S.

The report found that between 2015 and 2017 there were about 9,000 Russian posts about U.S. energy policy and events on Facebook, Instagram and Twitter. During the same time period, an estimated 4,334 accounts linked to the Internet Research Agency (IRA), a company established by the Russian government that engages in online influence operations for the Russian government and businesses. While some of these posts and tweets specifically target pipelines, fossil fuels and climate change, the report illustrates Russia is seeking to disrupt the growing acceptance of fracking technology in the U.S.

The motivation for this specific coordinated attack is evidently economic. A strong U.S. energy economy negatively impacts Russia's oil and natural gas economy. Eastern, central, and southeastern European countries currently import 70 percent or more of their natural gas from Russia. But that is changing.

For example, according to the report, Poland recently signed a five-year deal with the U.S. to import liquefied natural gas to decrease dependency on Russian energy supplies. With economic stakes this high, it is not a surprise that state-actors are willing to weigh in and cause damage.

New Knowledge also observed direct evidence of anti-fracking propaganda from fake or misleading social media accounts. In particular, the IRA targeted anti-establishment pundits to undermine support for US domestic energy production. New Knowledge found that a cross-platform strategy maximized the campaign's reach and shareability, and that these strategies were orchestrated by Russian government-established media outlets and the Internet Research Agency. Proprietary analysis tools created by New Knowledge successfully tracked these disinformation campaigns.

Looking Forward

How Brands Fight Back

Familiar brands sometimes take stands on social issues important to them and their customers, using their reputation and market position as a soapbox to assert values. Though plentiful research indicates that consumers increasingly consider values when making purchasing decisions, doing so can incite rabid responses and even risk violence. How did we get here? A cottage industry of disinformation has co-evolved with internet culture, and our public discourse now transpires across an information eco-system built for virality and which rewards rage.

The brands and industries in these case studies were simply hijacked and used as vehicles for advancing agendas. And the cost of these actions that fabricate an illusion of massive consensus is the deterioration of brands. Perhaps even worse, the signal of *authentic* social concerns gets drowned by the noise of inauthentic manipulation and computational propaganda.

Focused tools and process built to defend information integrity and the utilization of reliable threat detection technologies can disrupt the effort, and prevent irreparable damage. Adoption of automated solutions designed to monitor internet activity for manipulative, inauthentic campaigns raises the cost of disinformation as a whole, making it more costly for perpetrators to take an established brand hostage and damage its hard-earned reputation.