THE "FAKE" EPIDEMIC

How Fake News, "Like-Farming" and Scam GoFundMe Campaigns Are Undermining Trust in the Internet – And What We as A Society Must Do About It

March 2017

digitalcitizens alliance

Table of Contents

Supreme Court Justice Potter Stewart once had a simple answer when it came to identifying obscene material: "I know it when I see it." Today, when it comes to the Internet and the emergence of so-called fake news, "tales of woe" scams that tug at our heartstrings and tricks to infect our computers, it's not as easy.

Manipulation – whether to influence elections, steal money or take control of your computer - is eroding trust in the Internet because sometimes it's often hard to know whether a story is fake or not.

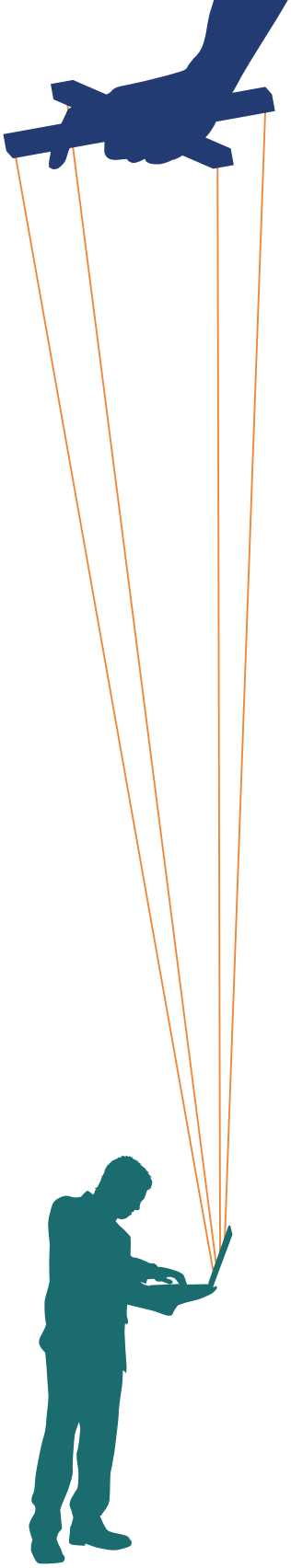
But one thing is clear: their impact is real. In the last few months fake news, described as false and sometimes sensationalist information presented as fact, has been at the center of controversy. However, fake news is just one of the many ways online scammers are distorting the Internet for their own gain.

From so-called "like-farming" – using sob stories to target potential victims – to fraudulent crowd-funding schemes, it's becoming harder than ever to know whether what is on the Internet is real or not.

And the distortion is having a corrosive effect on the Internet. The emergence of fake news, for example, has led the majority of Internet users to report that it's made them less likely to rely on the Web as a source of online information. Many Internet users admit that they've inadvertently spread fake information by reposting it or sending it to a friend – only to learn later that it was bogus.

The Digital Citizens Alliance views fake information as a sort of cancer on the integrity of the Internet. When criminals use a tale of woe (example on Facebook: "Share this image and Mark Zuckerberg will donate $5 to a children's hospital") to identify their next victims, it is likely to make citizens think twice before donating to legitimate worthwhile causes.

And the problems go well beyond Facebook. There are numerous examples of scammers creating GoFundMe campaigns to try to take advantage of a tragedy. One of the most egregious was GoFundMe campaigns set up posing to raise money for victims of the Orlando shooting in a gay nightclub.[1]



[1] http://www.bradenton.com/news/nation-world/national/article98342247.html

While the schemes are diverse, by and large their motive is nearly always the same: money. And unless this "Fake Epidemic" is addressed, it will eat away at the fabric of digital society and limit the positive role the Internet plays in our lives.

Fortunately, key technology leaders are recognizing the corrosive impact. Digital platforms such as Google, Facebook, and Twitter have taken steps to identify and eradicate fake information on their sites. And Digital Citizens acknowledges how difficult this issue can be. One, it requires these companies to make sometimes uncomfortable value judgments (for example, what is fake news?). Two, it can compel them to take more legal responsibility for what appears on their platforms than they've been willing to take thus far.

But attitudes seem to be changing as fake news and scams become so insidious that it's now a digital health crisis. Digital Citizens believes it will take a thoughtful and measured combination of company action, consumer education, and government leadership to beat back the forces that stand to gain from the proliferation of fake information. A free and open Internet cannot be sacrificed to achieve these goals, but if done wisely, we can collectively make the Internet a more credible and safer experience for all users.

Fake News, Real Impact

Fake news is not new: for as long as news has been circulated, some have attempted to manipulate it for their own ends. Some point to the role William Randolph Heart's "yellow journalism" played in starting the Spanish-American War in 1898.[2] What has changed is the scale and ability to circulate false and sensational information due to the emergence of social networks.

The legacy of the 2016 U.S. election will be how the combination of fake news and social networks confused many Americans and devalued news reporting. It was brazen, going well beyond opinion making to outright false stories created by operators – some of whom were overseas – who saw an opportunity to make money and manipulate public opinion. And

[2] https://www.pri.org/stories/2016-12-08/long-and-tawdry-history-yellow-journalism-america

it was pervasive: 76 percent of Americans surveyed said that they have come across fake news when browsing the Internet. (source: DCA survey, February 2017).

What occurred during the 2016 election went well beyond typical political tricks. A BuzzFeed investigation found that a small town in Macedonia, a country in the Balkan peninsula of Europe, was a key source for a torrent of political fake news. In all, Buzzfeed traced 140 political websites promoting mostly pro-Trump conspiracy theories all emanated from the town of Veles in Macedonia.

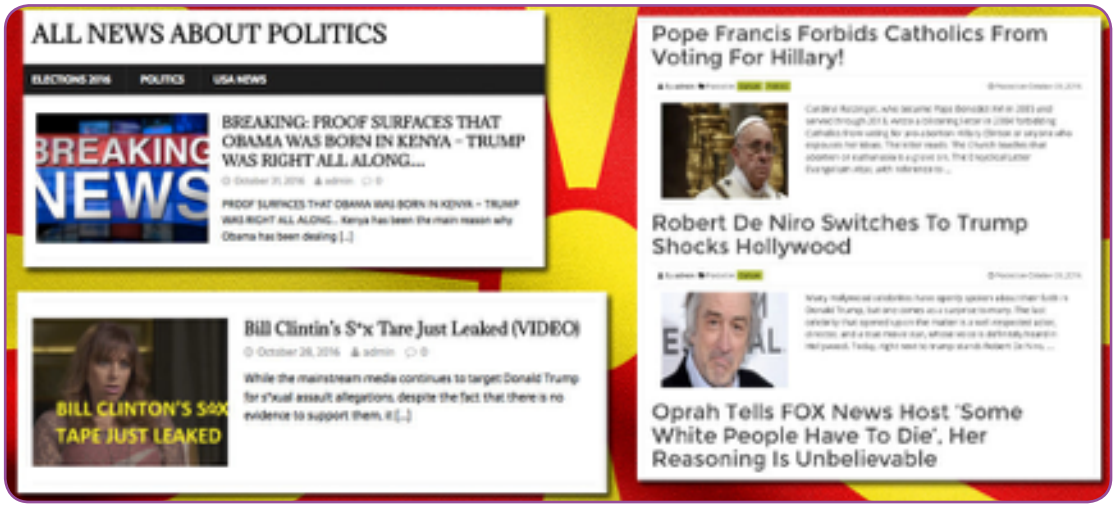


IMAGE 01
Source: BuzzFeed, November, 2016

The motivation? Money.

The sensational stories were click-bait, which led to advertising revenue flowing into these hyper partisan websites. "Yes, the info in the blogs is bad, false, and misleading but the rationale is that 'if it gets the people to click on it and engage, then use it,'" a Veles university student who started a political website told Buzzfeed.

In other instance, the BuzzFeed investigation found that a Miami-based company, American News LLC, was peddling outrage for both sides – utilizing *its Liberal Society* website to fan the flames against conservatives while deploying its *Conservative 101* website to fan the flames against the left.

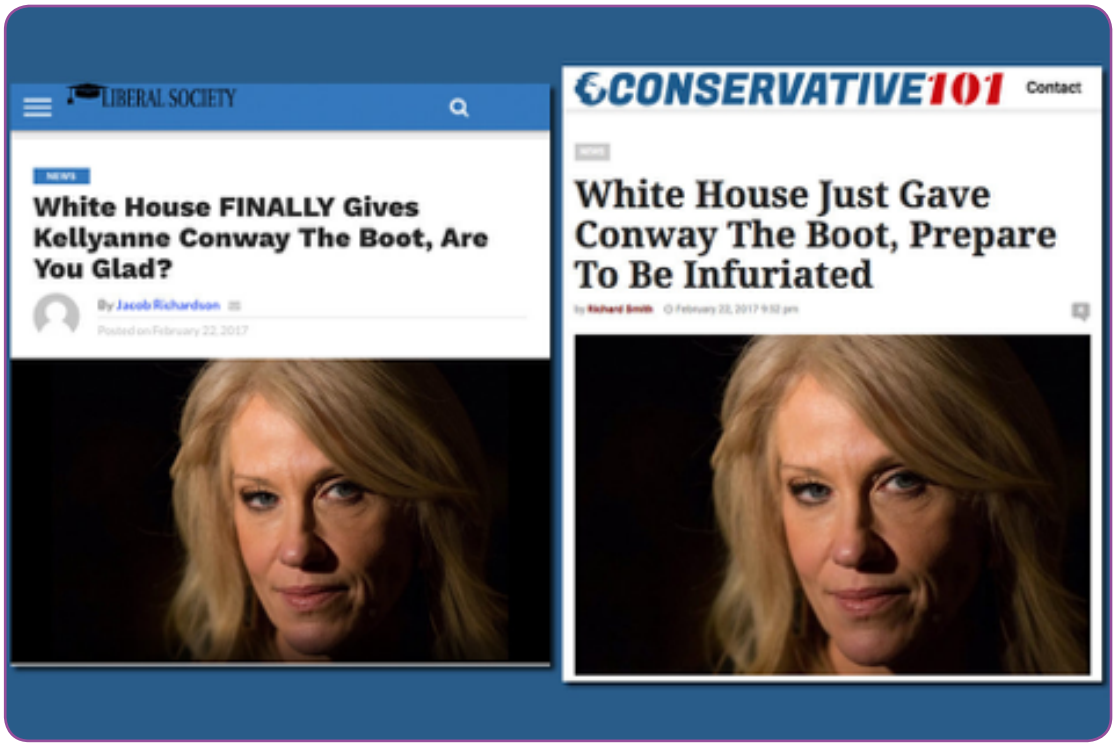


IMAGE 02
Source: BuzzFeed, February, 2017.

And social networks are the perfect breeding ground to formulate a falsehood and then watch it spread. According to the Digital Citizens Alliance research survey, this is where Americans have been most likely to encounter fake news:

Facebook	73%
Conservative-leaning websites	29%
Twitter	24%
Liberal-leaning websites	23%
Google	17%
Yahoo!	16%
Instagram	14%
Established U.S. websites (NY Times, WS Journal and Washington Post)	14%
International news websites	11%
Bing	6%
LinkedIn	4%

The news may be fake, but its impact is real. 61 percent of Americans report that fake news has made them less likely to rely on the Internet as a source of information (source: DCA survey, February 2017).

Part of the problem is Internet users don't always catch on that its fake right away. According to the DCA research survey, just under half (49.8 percent) of Americans said they would know something was fake when they see it. And one in four Americans said they have posted or forwarded a story, only to find out later it was made up.

Part of the challenge is the role advertising plays. Clicks mean ad revenue, so there is an incentive for fake news websites to be sensational.

But at the same time these websites are attracting mainstream advertising, which lends the appearance of legitimacy to websites peddling fake news or anything else. In fact, 61 percent of Americans said that mainstream advertising that shows up next to fake news makes it more likely that readers will be tricked into thinking the news is credible.

Here's an example of a Gap ad and Norton ad both appearing around and next to a fake news story about California Democrats legalizing child prostitution. In fact, the legislation labeled a minor who engaged in the sex trade as a "victim."

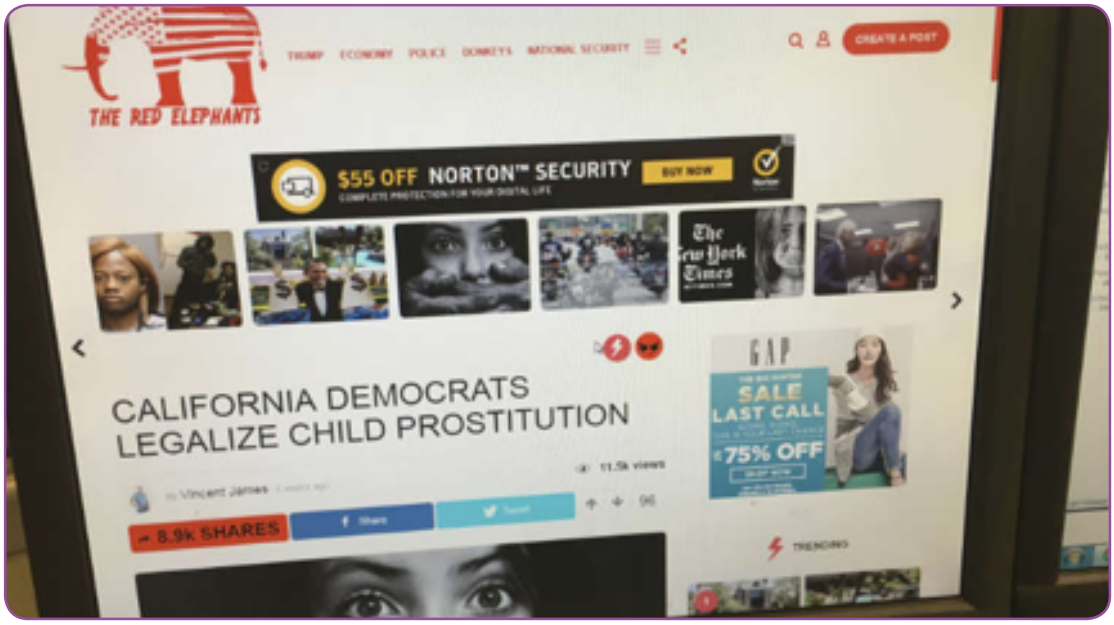


IMAGE 03
Source: Bing

This advertisement for Dodge RAM trucks appeared next to a bogus story that artist Yoko Ono claimed to have had an affair with Hillary Clinton during the 1970s:

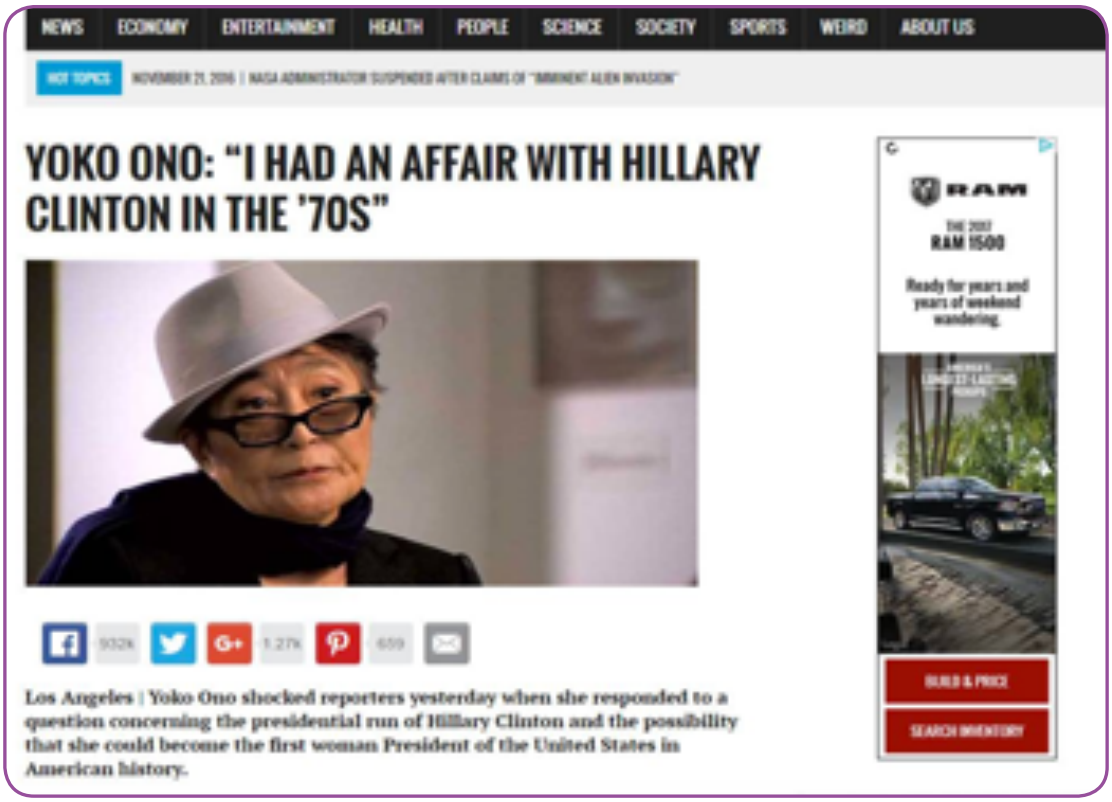


IMAGE 04
Source: Wall Street Journal

Digital Citizens reached out to the three companies whose ads appeared around or next to the fake news examples included in this report. A representative from Gap declined to comment while requests for comment from Norton's parent company, Symantec, and Dodge's parent company, Fiat Chrysler Automobiles, went unanswered.

Just as fake news existed since the beginning of the written word, it will never be completely eradicated. But unless we as a society get a handle on it, it will go beyond simply undermining our belief in news to casting doubt on the democratic institutions, such as elections, that are our foundation.

Like-Farming

Everyone has felt compelled to help after hearing a poignant tale of loss and hardship. It speaks to our generosity to want to help. Unfortunately, that fountain of goodwill is being poisoned by a new scam on Facebook called "like-farming," where criminals use tales of woe with a plea (example: "Share this image and Mark Zuckerberg will donate $5 to a children's hospital") to simply like or share information. By creating a "pool of likes," scammers have a list of potential targets that they can then try to trick. In some cases, the scammers will dangle a prize to collect a users' personal information.

These like-farming efforts are intended to create false credibility around philanthropic efforts by getting tens of thousands of Facebook users to click "like" in support. Just like mainstream advertising can make fake news seem real, a Facebook post with several hundred thousand likes can fool a person into taking it seriously. Once they have built up enough likes and shares, the scammers have an array of options on how to monetize them:

- Solicit donations to the "worthy cause." Once you have made a donation, they have access to your credit card and other personal information.
- Once they have created a critical mass of likes, they add advertising in order to monetize the support.
- The likes and shares are harvested and sold to marketers. In this case below, scammers dangle the prospect of a free Apple iPad mini:

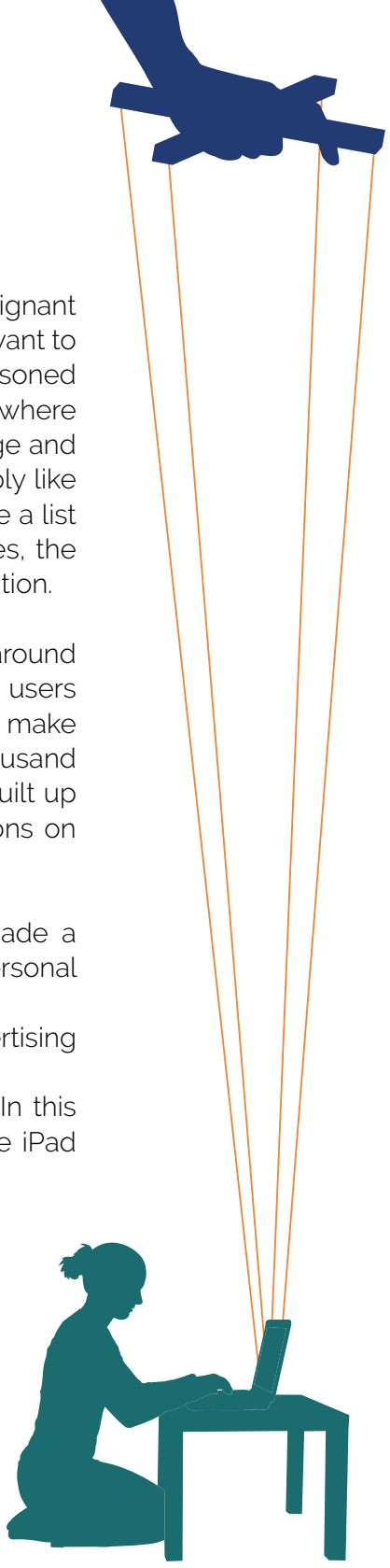


IMAGE 05

The post reads: "We have 2,425 Apple iPad Mini's which can't be sold because they're unsealed so we are giving them out for free to some lucky people!

Want To Get One? Just "Share" this photo and "Like" our page.

Competition ends on the 24th May 2013, Good Luck.
-Apple

Source: hoax-slayer.com

In these cases, scammers are exploiting a new dynamic created by social media: the ability to change a Facebook posting from its original entry. It can be edited to reflect advertising or completely change it's meaning, but the likes and shares aren't affected. In that way, unscrupulous operators can claim support for a cause, product or post that it doesn't actually have.

IMAGE 06

The photos used for this post were taken from a news story a few years back about a baby with a bad case of chicken pox.

Source: Source: bbc.com

"Liking" or clicking the link in a fraud post may also expose the user to malware by redirecting the user to a site that automatically downloads some type of malware or virus on his or her device.

GoFraudMe

There are numerous heart-warming examples of wonderful GoFundMe stories, from funding the 24/7 care of the world's oldest living **World War II veteran** to helping a **Liberian orphan pay** for life-changing surgery. In all, GoFundMe campaigns have raised over $3 billion for those in need.

But unfortunately, there is a dark side to GoFundMe: numerous efforts to use fake stories to dupe well-meaning donors into giving away their money.

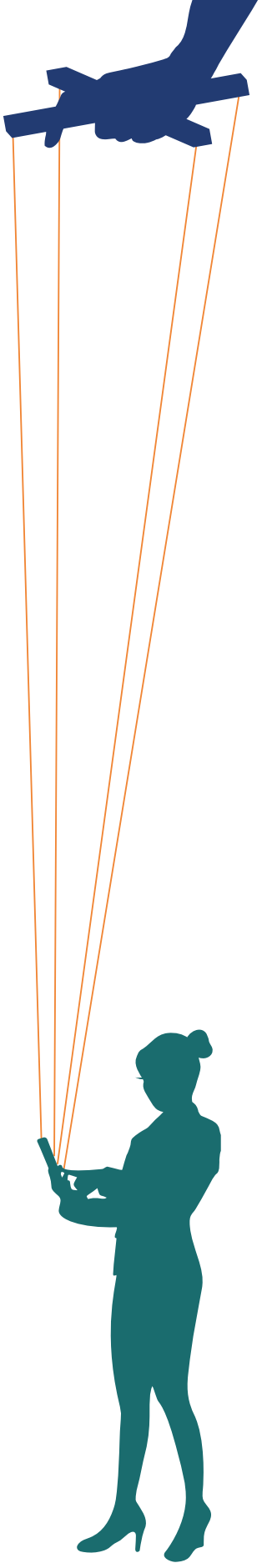
Who can resist the plea to help a sick child? For a scammer, all you need is a **good story about rare pediatric cancer and a photo of a cute child stolen from the internet**. On February 28, 2017, a GoFundMe account was set up to raise money for "Bailey", an eight-year-old girl with pediatric cancer. In reality, there is no Bailey and the adorable photo used was taken from the internet.

A similar scam involved the **creation of an account using a family's photo and details of a previous legitimate GoFundMe account**. In this instance, a North Carolina family who, in 2014, raised necessary funds through GoFundMe following an accident discovered in 2017 that their story and family photo were being used for a fake GoFundMe account.

Fortunately, both these scams were shut down within a few days. However, too often, the scammer succeeds.

The case of Sadey and her recovery from motorcycle accident is unfortunately just one of many where the plea for help was not what it seemed. In November 2016, Daniel G Gutierrez set up a fund seeking $10,000 to help Sadey with her recovery. But Daniel apparently **began almost immediately withdrawing** the money and Sadey's sister said her family never saw a dime.

In another instance, the father of a young California girl killed in a car crash **found multiple online websites** claiming to raise money on his family's behalf. In one instance, $4,000 was raised before it was taken down – but by then the scammer's had already absconded with the money. While the father also created his own GoFundMe page to pay for her funeral costs, the prospect of bogus sites certainly did not help with his fundraising efforts (although fortunately he was able to raise the necessary funds after a USA Today story drew attention to his plight).



In yet another instance, a family friend set up a GoFundMe account for the family of a civilian contractor who was killed by a car bomb in Afghanistan and then **stole the funds.** The family received only $400.00 of the nearly $4,800 raised.

Responding to Fake Information: Good First Steps

In recent months, there has been a concerted effort by digital leaders to combat the fake news phenomenon. The questions remain: is it enough and will it work?

Google announced in November that it would ban websites that offer fake news from participating in its online advertising service: "Moving forward, we will restrict ad serving on pages that misrepresent, misstate, or conceal information about the publisher, the publisher's content or the primary purpose of the web property."[3]

By banning fake news websites from its online advertising services, Google is removing the incentive these manipulators have to create the content. But that is not all that Google has done. The company has also expanded its "fact check" service.

These are good steps, for which Google deserves credit, but the company has the opportunity to go further. It could create a broader manual review of what content gets promoted on Google platforms. Google can also be more transparent in what is manually reviewed and what is not. To do so, however, the company may have to forego some advertising revenue for the sake of news credibility. Google could also take more steps, through its algorithm, to promote news reports from credible websites while demoting news stories from less credible websites – even when those news stories go viral due to their false sensationalism. Certainly Google could face criticism that it is gaming the news, but as long as it is transparent in how it approaches specific websites it could mitigate that concern.

[3] http://www.reuters.com/article/us-alphabet-advertising-idUSKBN1392MM

Facebook is most at risk by the threat of fake news. By a 3-1 margin Americans said they came across fake news more on the social media site than any other platform. And to the company's credit, it announced in November new steps to combat fake news by identifying potential fake news, creating a fact check process and labeling misleading reports as "disputed."

No leader has been as outspoken on the threat of fake news than Facebook CEO Mark Zuckerberg. "If this continues and we lose common understanding then even if we eliminated all misinformation, people would just emphasize different sets of facts to fit their polarized opinions. That's why I'm so worried about sensationalism in media,"[4] Zuckerberg wrote in early 2017 outlining the importance of combatting fake news.

Zuckerberg articulated a vision where, by tweaking Facebook's algorithm, fake news will be less prevalent as it's diluted with more credible information. "Our approach will focus less on banning misinformation, and more on surfacing additional perspectives and information, including that fact checkers dispute an item's accuracy,"[5] he wrote.

For example, Facebook is asking its community to help root out fake news:

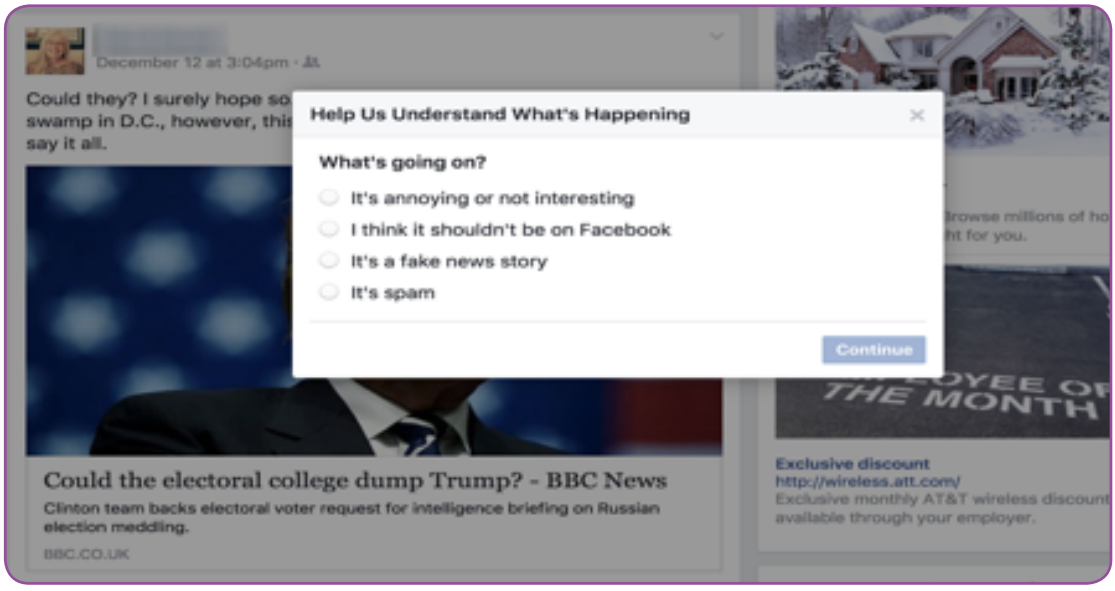


IMAGE 07.

Source: Droid-life.com

[4, 5] http://www.upi.com/Top_News/US/2017/02/17/Facebooks-Mark-Zuckerberg-Fake-news-creates-polarization-in-beliefs/6871487342178/

And learning from it's 2016 experience in the 2016 U.S. presidential election, Facebook announced it is working with eight media organizations in France in advance of the country's upcoming elections to fact-check news articles flagged by users.

Facebook's initial steps have earned the company respect: 79 percent in the Digital Citizens research survey said it's a "good thing" that the company has taken steps to flag fake news on its site.

A Community Problem Demands a Community Solution

Just as with other illicit activities, the facilitators of commerce play a vital role in protecting citizens and preserving the integrity of the Internet. For example, when credit card companies such as Visa and MasterCard refuse to process payments to disreputable online pharmacies, it goes a long way to suffocating their revenue streams. The same is true with advertising. The advertising networks must step up to their role and limit reputable brands from showing up next to fake news stories.

It is complicated – the system breaks down with the weakest (least reputable) link in the ad chain – but just as major brands insisted that their advertising not be associated with ISIS terrorist YouTube videos or on content theft websites, so too must brands ensure that they aren't inadvertently giving credibility to fake news. Americans want to see this: by a nearly 2-1 ratio (53 percent to 30 percent) those surveyed said it is the advertisers' job to make sure their ads don't appear next to fake news.

Just as the cure to malfeasance is transparency, the best way to combat fake news is to flag it. The digital platforms facing this issue must come together to create a better and more robust system of fact checking that can quickly identify and address fake news quickly. There is a model for this: a decade ago a Google-led effort to combat malware led to the creation of Stopbadware.org, a community effort to expose websites that endangered Internet visitors. That community effort is needed here.

The manner in which digital platforms approach issues of contention – whether fake news, content theft, counterfeits and other illicit online activities – is often an enigma because of the mysteries of their algorithms. Providing greater insight into how they approach these issues would lift that fog – and create a greater community effort to understand how to combat issues such as fake news.

The best defense against fake information is giving Internet users the skill sets to identify and avoid it. Communities, schools and law enforcement should consider creating education programs on Internet citizenship, especially for older people who are digital immigrants and the youngest users who may be more likely fooled by misleading or sensational information.

Internet at a Crossroads

016 was the most turbulent year in the 20-year history of a consumer Internet. Allegations of overseas influence, election rigging and divisiveness over politics is at a high point. The Internet and all that flows from it – e-commerce, social media, news, and education – are at risk of losing credibility if users can't trust it. The most fundamental level of trust – is what I am reading fake or not? – is core to the future growth and well being of what now makes up our national fabric.

Americans are looking to these platforms to lead the way to a solution – an overwhelming 77 percent in the DCA research study said that if these platforms want to be seen as responsible, they will address the fake information issue.

Let's be clear: this is not an easy issue. Facebook, Google and others must walk a tightrope of addressing the challenge of fake information while not becoming censors. It won't be solved with one move, and new threats will arise. But we look to these digital platforms to be open, inclusive and transparent as they – and us – learn from our experiences to strike a balance that works for all of us.

Digital Citizens intends to remain active on this issue, as it goes to the core of what Internet users seek when they are online: a reputable, safe place where they can connect with others, conduct business, and remain informed citizens.

About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer- oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders— individuals, government, and industry—to make the Web a safer place.

Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. Visit us at digitalcitizensalliance.org

digitalcitizens alliance