

What Online Integrity Will Look Like In 2022

Opinions expressed by *Entrepreneur* contributors are their own.

While the internet has opened up a wealth of new opportunities, there is no denying that many have been able to use it to cause significant harm. For example, the FBI's latest Internet Crime Report revealed 791,790 reported internet crime complaints in 2020, a substantial increase over 2019's numbers. Similarly, the FTC received 4.8 million fraud or identity theft complaints in 2020. But, of course, many online crimes are never reported.

Crime – be it in the form of fraud or child predators – is hardly the only issue facing the internet. The spread of disinformation, hate speech, and extremism also poses genuine threats.

Not surprisingly, governments, tech companies and others are taking increased measures to keep the internet safe for all users. Their response to these ongoing challenges will undoubtedly shape the future of online integrity in 2022 and the years to come.

Current challenges facing the online world

When most people think of online integrity issues, they focus on the aforementioned problems like fraud and identity theft. These are certainly no small matter. From fake social media accounts being used to steal information to scam emails and malware, there are many tools that bad actors are using to

steal private information.

However, harmful content has become even more widespread in the last few years. In the United States, this can be most easily seen in the disinformation spread regarding the 2020 election and the Covid pandemic.

As a report from CBS detailed, even areas as seemingly benign as the wellness community (which includes yoga instructors and other wellness practitioners) have seen their social media feeds flooded with conspiracy theories designed to sow mistrust. Even after QAnon conspiracy theories have been repeatedly debunked, this pernicious source of disinformation continues to make its influence felt in conversations regarding election fraud.

As problematic as disinformation can be when shared by a friend or family member, loopholes or oversights in platform policies have resulted in even more significant problems on a global scale.

After the Taliban regained power in Afghanistan, the terrorist organization used social media to strengthen its grip, largely because the Taliban was smart enough to ensure that their uploaded content did not violate the platforms' rules.

The re-emergence of the Taliban has been further complicated by the fact that the United States doesn't officially designate the group as a terrorist organization, even though the UN Security Council does.

In India, anti-Muslim allegations that have come to be known as "Jihad conspiracies" have been able to spread disinformation and sow discord in local communities in large part because of Facebook's failure to regulate such content.

For platform holders and government officials, finding appropriate measures to fact-check and eliminate such harmful content has become increasingly complicated, especially in

relation to free speech arguments. The global, international reach of online platforms makes such efforts even more challenging.

Related: 3 Reasons Why We Fall for Conspiracy Theories

What is being done to enhance online integrity?

Most of the efforts to improve online integrity must ultimately come from the platform holders themselves. In an ongoing effort to combat disinformation regarding the pandemic, vaccines and other related topics, social media platforms have continually updated their policies regarding which content is or isn't acceptable. Some platforms use specific wording for issues such as election disinformation, while others prefer broader phrasing.

As a white paper from ActiveFence, a service designed to proactively detect harmful content and counter bad actors, explains, "As we've learned, content policies should first and foremost protect the safety of platform users. Policymakers must be aware of all relevant regulations and legislation to ensure that policies are in accordance with the law. Policies should be rigorous and detailed, but they should also be non-exhaustive. The challenge faced by policy builders is building a system for evaluating content that protects the spirit of the wording and can respond to new and evolving threats. In addition, companies must understand their place within a dynamic digital environment – both as it is today and as it will be in the future."

Notably, such efforts must be mindful of domestic and foreign policies and trends as they strive to reduce the influence of bad actors.

The government is also increasing its efforts to mitigate the

potential harm caused by the internet, particularly regarding children. For example, recent Congressional hearings have emphasized the responsibility platforms such as YouTube and Snapchat have to protect vulnerable youth and teenagers on social media. Concerns over data-driven advertising and potential harm to mental health have played a large role in driving these discussions.

While no firm actions have been taken yet, there seems to be a growing consensus among both parties that additional regulation of social media is needed. Bills have already been introduced to make these platforms more transparent, and it is likely that such governmental pressure (both within and outside the United States) is expected to increase in 2022.

Related: Preventing the Spread of Conspiracy Theories in Times of Crisis Requires Effective Leadership

Creating a safer online future

The challenges related to maintaining online integrity are immense.

Ultimately, keeping the internet safe will require a concerted effort from tech platforms, government agencies, brands and NGOs to minimize the potential harm that malicious individuals can cause.

<https://www.entrepreneur.com/article/399686>