https://www.bizcommunity.com

Disinformation defences

BY: HOWARD PLAATJES

A war of words looks very different in the 21st century in a world dominated by agendas and ever more sophisticated technology. In fact, we have reached a point where very easily, 'words' and 'images' can start wars.

Photo by Joshua Miranda from Pexels.

Technology is also a double-edged sword. It can be used for upliftment and good, or, in the wrong hands, it can be used to spread dissension and division, such as ‘disinformation’ - false or misleading information (misinformation) spread deliberately to deceive.

Visual deception

Content is generated by the second and fed to us on digital platters to satisfy our rapacious appetites for being in the know. There is, consequently, an increasing need for measures to be put in place to help readers separate fact from fiction. This is especially pertinent when it comes to the fields of news, advertising, e-commerce and even politics.

Already, readers struggle to tell the difference between a genuine news item and an opinion piece, an authentic news site or a website made to look like one and that peddles half-truths or deliberate falsehoods. Add another layer to this, such as fabricated videos, for example, known as ‘deepfakes’ and it is no wonder there is growing concern over what could be termed next-generation information warfare.

People and technology: What the fakery?

Photo and image manipulation, as well as the generation of fake news, are no longer ‘news’. However, the deep learning capabilities of artificial intelligence (AI) and machine learning (ML) tools, is making it easier and faster, to create masterpieces of visual deception. This power can, of course, be abused, to create and spread large scale fear and confusion at a citizen and public level to the extent where it can affect national security. In today’s context, it is screen warfare that wins the hearts and minds of easily swayed people.

Whereas cybersecurity is the use of technologies, systems and processes mainly aimed at the protection of data, we need to go one step further by looking at the source material itself - before it is transmitted. We have to build robust forensic cybersecurity

defences, to help ensure that digital content can be source verified.

Safeguarding consumers from fake campaigns

> *"It is sad that digital media authentication is a necessity in this day and age. Media, including advertising, without the requisite crypto identifiers to cross-reference to the source in place, is deemed less trustworthy or considered fake otherwise."*

Incorporating crypto security identifiers into content is akin to SSL Security measures that test whether online form fillers are humans or robots. A prime example of where the placement of crypto identifiers would be is on advertising. Another is political campaigns. Their presence would immediately and clearly identify the source material and whether it was authentic and could, therefore, be reliable, or if it had been 'manufactured' to convey a differing perspective or offer up discrediting news to derail the opponents' efforts. This tactic, of course, is not limited to the political arena, as corporate competition has also been known to benefit from such measures…

2 most awesome ways AI can be used to fight fake news

Cryptographic identifiers are also essential to assure the authenticity of news, marketing and advertising engines, to safeguard consumers from fake campaigns, but also increasingly, to help them distinguish whether external influence is getting in the way – such as foreign powers interfering in domestic issues for example.

Worryingly, studies are showing that many learners can't distinguish between sponsored content and news stories on social media and e-commerce platforms. Even more concerning, is the growing need to authenticate some of the material used in the learning environment itself.

Bolster media literacy

We, therefore, need to bolster media literacy in schools and tertiary institutions, with workable and scalable solutions that can authenticate materials and resources. Additionally, there is a growing need to develop the appropriate tools to train students themselves on how to evaluate trustworthy media on social media and e-commerce platforms.

Media literacy: Five fact-checking tips for the fake news era

Cybersecurity is not a nice to have or confined to businesses and governments, it has become an essential life tool for everyone, whether connected to the digital ecosystem or not. Faced with the post-Covid era of remote working, e-learning, e-commerce, slowing economic growth and even dissatisfied corporate boards, overwhelmed security systems, and the constant pressure and need to get ahead, we can expect information warfare to heat up, and therefore, the need for deep disinformation defences.

Of course, this is all semantics if the will for content producers to verify their sources before posting their content is not there.

About Howard Plaatjes

Howard Plaatjes is the CEO of AYO Technology Solutions.

- Disinformation defences - 14 Jul 2020

View my profile and articles...