ASA Research Note

Social Media: Information communicator or destroyer?

Author: Harshita Chandgothia

Published: October 2022

Written: March 2022

Keywords: Social Media; Information Transformation; Communication; Weaponized Information

Abstract: This paper discusses the paradigm-changing impact of social media technologies have had on human communication and communication systems. It explores the both the position impact as well as the negative, including how information can be weaponized so easily on social media platforms. Humans may have to come to simply accept the risks, and do the best to prepare against them. One way or another, society must continue to adapt through this ongoing, massive technological evolution.

In this digital age, the number of ways to disseminate information has grown exponentially over the last two decades. The internet has gone from an era of Netscape browsers and dial-up connections to an infinite hydra of constantly updating social media sites, with thousands of hours of content uploaded by the minute. These social media platforms contain impossible amounts of footage that cannot be deciphered or verified. This paper will talk about whether these information distribution platforms are able to successfully communicate their content to the consumer or whether the real information gets destroyed along the way. Unconsciously, has the internet become a hub of services where information can be easily plastered? The question now is whether the damage is permanent to our communication systems: are social media platforms slowly transitioning to being adopted as information weapons?

Social media has taken over as the new form of communication. It entails platforms ranging from Wikipedia (a site that brings together human knowledge) to Instagram (a site for daily entertainment). In 2015, there were reportedly 2.07 billion users of social media globally. Fast forward to six years later, we see a jump of 2 billion in this internet engagement rate.[1] The tremendous growth of technology in recent decades has allowed this massive expansion of access. For instance, if we take the Philippines as an example of a developing country and the United Kingdom as a developed country, the historical usage rates in the two are significantly distinguishable but the gap is narrowing fast. From 2017 to 2026, the percentage of social media users is projected to rise by almost 40% in Philippines[2] and around 26% in the latter.[3] This difference highlights the increase in accessibility of information that has allowed lower socioeconomic populations to jump onto this bandwagon. Social media platforms are indeed talented profit-seeking businesses, working by securing strong relationships between the user and the machine interface, be it a smart phone, a tablet or a computer. As the expansion gathers momentum, firms' ability to extract profits multiplies, propelled by a much wider audience outreach. Monetization by selling advertisements that are cloned to a user's interests is an infamous but widely prevalent and extremely successful strategy employed by these digital experts.[4] A positive response from such sales incentivizes the producer to continue with the data inferencing, creating a virtuous cycle involving the platform owner, the product owner and the consumer, to a certain extent. However, the liberties of the internet do lead to forms of customer abuse at the hands of the platform owner. Misinformation and fake news have blinded many at the cost of information and entertainment. The phenomenon of matter is the social dilemma: are the benefits enough to outweigh the costs?

The growth of large tech-savvy companies has certainly played a role in enlightening minds. Facebook, Google, Twitter, have been strong communicators of information, whether through a general knowledge providing platform or a social networking site. In recent times, social media platforms have begun to do more to clear up misinformation and remove disinformation. These terms are often used interchangeably in the larger context though it is important to distinguish between them. Disinformation is intentionally made to fool the user, whereas misinformation is falsely published information, unknowingly passed on. Incorrect data is spread on the internet, which oblivious users are prone to accepting. To combat this dubiety, specific sites are increasingly employing AI (artificial intelligence) technology that can sense inappropriate and red herring commentary. In 2020, CBS (Columbia Broadcasting System) news released an article revealing actions taken by Twitter to block accounts associated with White supremacy groups. These accounts, posing under the name of Antifa[5] (a liberal anti-fascist and anti-racist group), were encouraging violence using the Black Lives Matter (BLM) movement as an excuse for their actions. The detection of such racism came through an algorithm Twitter implemented which automatically flags seemingly malapropos content. Influential political figures such as Donald Trump Jr. even spoke about the issue, recognizing its importance in aggravating the peaceful protests in support of George Floyd and the BLM movement.

Technological advancements have risen the appeal towards social media, extending to industries beyond entertainment. For example, AI is playing an immensely important role in the control of crime. Decades ago, if an individual committed a robbery during broad daylight, pushing charges was difficult in the absence of a physical, human witness. On the other side too, victims lacking an alibi found it harder to defend themselves. However, with the growth of the Internet of Things, justice has been brought to many. CCTV (Closed circuit television) technology was first introduced 60 years ago and its importance has only increased over time in spotting violence. In fact, presence of CCTVs acts as a deterrent in some respect. The difference between the CCTVs of yesteryears and today's is that AI based security cameras are advanced versions of internet protocol (IP), with an enhanced ability to detect more intricate criminal activity. Extensions including face recognition, voice detection, or shadow sensing are important additions that have been successful in spotting or even preventing danger. NBC Chicago recently released footage revealing an attempted break in by a burglar into a woman's accommodation.[6] The visual evidence, a video, was posted on social media, making the news viral. A chain of a hundred reposts, tags, comments and likes created the necessary attention to bring justice to the matter. This form of communication system that social media provides us is important in internal situations and larger contexts. It aids organizations like the FBI and the CIA to get the intelligence they need to fulfil their roles on a global scale.

Over time, advancements in technology and in a greater awareness of the human biases that could influence the way machines think, algorithms being run on social media are getting programmed better, in ways that aim to prevent bias and prejudice. A lot more needs to be done, but there is little doubt that programmers behind the screens are increasingly instructing the machines to filter for racist words (e.g. blacklist or slave) to reduce the spreading of sensitive commentary.

Social media has become a profound platform for voices to be heard. It has allowed oppressed individuals to freely express their experiences without judgement. Popular movements such as "Black Lives Matter" and "Me Too" demonstrations gained pace and popularity through attention on social media itself. However, strong censorship rules in some countries (e.g. China) has made it difficult for victims to vocalize their support for such global movements without challenging the authority of their government. If we analyze the situation of the Me Too movement specially, English words "Me" and "Too" were banned from social media in China. As a consequence, women activists were forced to adopt unique ways to continue to communicate their support. Advocates began posting messages with similar sounding words from the Chinese regional language (e.g. Mi Tu translated to rice bunnies).[7] It showed that despite the domination placed in such countries, citizens were able to use social media as a medium to successfully convey their passion and determination to support a global cause.

Steering away from entertainment and criminal indulgence, social media has extended its prominence onto political grounds that involve tension between countries. Alarms ring the loudest when disinformation is released onto the internet to a level that interrupts public thoughts. One of the most intimate topics of the current time is the ongoing dispute between Ukraine and Russia. Researchers have claimed that Russian actors are being encouraged to flood social media sites with messages and comments representing Western alliances as aggravators. These tactics are being used to perhaps temporarily swing the justification behind Russian actions and hinder other forces from the realities of the military actions taken by Russia. The Russian government is employing this new strategy to further their agenda and justify their military actions since the AI of various social media websites has been taking down overt disinformation campaigns propelled previously by fake accounts and bots. Actors have been used for this activity as their fame has itself been driven by popularity spread through social media.[8] This highlights that the holistic applicability of social media is a global phenomenon. Therefore, while social media has definitely progressed in its attempt to enhance communication across borders, it also comes with an almost infinite amount of misleading information, which has to be filtered in order for the knowledge gained to be truly worthwhile.

Within our daily lives, communication through social media has become such a conventional approach that its dependence goes by unnoticed at times. Undeniably, it is at the worst of times that humans realize how grateful they are for the applications that allow constant reassurance: WhatsApp, Facebook, Google, Twitter, Instagram etc. Unfortunately though, when the internet becomes consumed of clutter, the naïve get blind-sighted from reality. On the 4th of March, a news article was published by BBC titled “Ukraine war: ‘My city’s being shelled, but mum won’t believe me’”. On first thought, from the perspective of a common man, I refused to believe what I read. How can a family member act so flippant about their child’s life? Upon closer reading of the article, it was understood that the daughter’s mother was misled by specific nationalist information. One line especially, “…they still say it probably only happens by accident, that the Russian army would never target civilians.”[9] demonstrated the power of confirmation bias in such a situation. Biases inherently come with a grudge. In this scenario, a mother was brainwashed against her own child. The reluctance to accept realism, to solely stick by a current belief can create situations of danger that compromise lives. It acknowledges one of the most threatening aspects about social media: the damage to real connections. It is true that the reliance individuals have on technology nowadays has disrupted the way relationships were made in the physical world. Decades ago, people would send handwritten letters to each other, whether for casual contact or in hardship. There was so much faith within the communication system that one could write highly personal content without the fear of information leakage. Soon after, the pen pal system got introduced where people began writing letters to strangers across the world to create new friendships. Now, with the passage of time, people have adopted to the surrounding technology. Internet friends have become the new norm, creating a shift in consumer base places through Flickr, Tumblr, Facebook. For many, internet friendships are elevated to an equivalent level of connection as relationships gained through in-person interactions. However, the distinction is the burden cybercrime brings to a rising healthy online relationship. It demonstrates one of the most prominent weaknesses of social media where data breaches allow hackers to easily spill onto internet servers. Especially for large corporate organizations that work with thousands of data simultaneously, the damage can result in huge costs, both in terms of money and reputations. In 2012, Saudi Aramco (a Saudi Arabian public petroleum and natural gas company) was attacked by the Shamoon computer virus. The damage caused an exorbitant number of hard drives to be deleted. The hack also programmed computer screens to present a picture of the American flag getting burned down.[10] With the destruction of more than 30,000 laptops and intangible internal property, the company faced a mountain to shift to a manual system requiring pen and paper in a dire situation. Cybersecurity needs significantly more awareness not just in an institutional context through protection of systems and data, it is equally important in an individual context, given the amount of time our young minds spend on the internet. Innocent activity from young users who continuously post selfies, repost comments or share videos may not know what category of information they are spreading, whether racially or politically fraudulent.

Cybersecurity goes hand in hand with privacy. It is imperative that privacy rights be provided to users, where they are not tricked into disclosing personal information for hackers to feast on. One of the largest confessions of privacy contravention known was the scandal behind Cambridge Analytica and Facebook. The news disclosed that Cambridge Analytica, a British consulting firm, was given access to Facebook users' personal information without any disclosure or informed consent. As more information came out about the magnitude of the data sharing, the number of victims increased from 50 million to 87 million users.[11] When such major companies undergo surreptitious data sharing agreements with third party users, legislations should get stronger and renewed to ensure companies are held accountable. Cambridge Analytica was charged with a penalty of about 500,000 pounds under the rules listed by the Data Protection Act 1998. However, if the charge was under the new protection laws posted by the UK in 2018, the same company would have suffered a penalty multiple times higher, in the region of 17 million pounds.12[12] The transactions made between the user of the computer and the user on the other side of the screen have become a money making business where an identity is exchanged for complete access. Unfortunately, a majority of the time it is at the customer's vulnerability that the information is taken away right in front of their eyes. From a business point of view, the process begins with a social media company selling a consumer's data in return for a data analysis service. Companies such as Acxiom and BeenVerified have the infrastructure and capital to engage in such an operation. Their software is able to navigate consumer history and make predictions based on previous consumption patterns. Marketing companies begin their probing by presenting the terms and agreement page to users during the creation of new profiles. In Section 3.2 of Twitter's Privacy Policy page, Twitter simply indicates out that the personal information of a user may be shared with a third party to increase the platform's effectiveness. In reality, Twitter has ties with Google Analytics who receive the information, breakdown consumer activity on the application and remodel its services according to consumer experience.[13] There are multiple social media platforms who engage with metadata and justify it through the excuse to improve efficiency and instructiveness. By luring a diverse cohort of companies, social media has made a prominent appearance in almost all spheres of life – personal, social, political and financial. Investment banking firms (e.g. JP Morgan, Morgan Stanley, Bank of America etc.) rely heavily on the advertisements posted on various platforms to attract their consumers. LinkedIn has become the starting point to check on potential professional recruits ahead of the formal interview process.

With the introduction of the GDPR in April of 2016, companies dealing with any information affecting the citizens of the EU have been forced to comply with data privacy laws. The GDPR, or General Data Protection Regulation, is a security law that levies harsh fines on those that fail to comply with the privacy standards under the written legislation.[14] Major social media companies have now started obliging with global privacy settings that line up with the GDPR compliances. Companies like LinkedIn and WhatsApp have now agreed to provide more detailed privacy notices that inform the user about the how their information could be handled.[15] This provides some relief to social managers around the world as there is reduced tension about platforms collecting information from sites without consent. Greater customer say in the choice of data usage by platforms indirectly helps in strengthening defenses against data breaches as there is less data floating on sites that have weak defense systems to thwart attacks.

With all the disinformation, misinformation, fake news, propaganda, and misleading insights on the internet, it can become quite overwhelming for a user while navigating it on any given day. Yet, there is no denying that social media and its various contours are here to stay and are integral parts of the social ecosystem. Therefore, it is in our best interests to adapt to the current flow of technology. As a society, we must accept the possibility of mishaps such as cybercrime and viruses, and do our best to prepare against them, much the same way we try to keep biological disorders at bay through food, exercise, and other preventive means. An estimated 24% of the PCs worldwide have not yet been protected from online anti-virus software.[16] There is a significant population in the world that have their computers unprotected from viruses. One of the only ways that humanity can make progress in combating the malfunctions from the IT department is to be self-aware and self-protective.

Metaverse, a hub of 3 dimensional virtual worlds, looks to be the newest addition to the digital age. It conjoins a multitude of AI characteristics and takes social media interaction to another level, using augmented reality, virtual reality and blockchain. Social media had its first birth in 1997 and it was not until 2005 that the platforms really started blossoming. Now, in 2022, social media is getting more wings, and climbing to a more integrated and immersive space which fulfils the potential of new digital technologies. However, with the upbringing of the metaverse, the questions surrounding security, ethics and diversity have become even more serious and require even more attention, particularly from users that embrace it.

Tech Billionaire Elon Musk is working with Starlink to provide users with high-speed internet using low orbit satellites in places with little to now connectivity to flatten the world further. Social media must be commended for bringing the world closer. Efforts to remove waste from the internet and make it a cleaner platform for individuals to get a holistic form of entertainment are also to be applauded, though customer protection efforts need continuous improvement. The limits of human ingenuity are endless and the possibilities through smart use of technology boundless, not just in creating connections, but in helping humanity progress. Yet, both sides of the story must be acknowledged. The race between social media as an information communicator or information weapon is a challenge that will likely never end. One must adapt and learn to stay on the right side of this massive technological revolution.

SOURCES

[1] Dean, Brian. "Social Network Usage & Growth Statistics: How Many People Use Social Media in 2022?" Backlinko. Accessed 4 Mar. 22 <backlinko.com/social-media-users>.

[2] "Number of social media users in the Philippines from 2017 to 2020, with forecasts until 2026." Statista. 12 Aug 2021. Accessed 5 Mar. 22 < www.statista.com>

[3] Number of social media users in the United Kingdom from 2017 to 2020, with forecasts until 2026." Statista. 12 Aug 2021. Accessed 5 Mar. 22 < www.statista.com>.

[4] Garcia A, Adam. Socially Private: Striking a Balance Between Social Media and Data Privacy. IOWA Law Review. 2021. Accessed 8 Mar. 2022. <www.ilr.law.uiowa.edu>

[5] Kates, Graham. "Twitter says fake "Antifa" account was run by white supremacists." CBS. 2 June. 2020. Accessed 6 Mar 2022. <www.cbsnews.com>.

[6] Ngyuen, Vi. "Chicago Police Investigating After Attempted Break-In Caught on Camera." NBC Chicago. 5 Feb. 2022. Accessed 6 Mar 2022. <www.nbcchicago.com>.

[7] Minhaj Hasan, "Saudi Arabia + Censorship in China | Patriot Act with Hasan Minhaj | Netflix," YouTube video, Netflix Is A Joke, 27:15. 10 Feb 2019. <www.youtube.com>.

[8] Lima, Christiano, "LikeWar: The Weaponization of Social Media," Youtube video, 56:38. 5 Oct 2018. <www.youtube.com>.

[9] Goodman, Jack and Korenyuk Maria. "Ukraine war: 'My city's being shelled, but my mum won't believe me'". BBC. 4 Mar. 2022. Accessed 6 Mar. 2022. <www.bbc.com>.

[10] "Saudi Aramco facing $50 million cyber extortion over leaked data." CNBC. 22 JUL. 2021. Accessed 8 Mar. 2022 <www.cnbc.com>.

[11] Garcia A, Adam. Socially Private: Striking a Balance Between Social Media and Data Privacy. IOWA Law Review. 2021. Accessed 8 Mar. 2022. <www.ilr.law.uiowa.edu >

[12] Zialcita, Paolo. “Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal.” National Public Radio. 30 Oct. 2019. Accessed 8 March 2022. <www.npr.org>.

[13] Garcia A, Adam

[14] “What is GDPR, the EU’s new data protection law?” GDPR.EU. Accessed 8 Mar. 2022. < https://gdpr.eu/what-is-gdpr/>

[15] “What does GDPR Mean for Social Media Strategies?”. Digital Marketing Institute. 13 April 2018. Accessed 8 Mar. 2022. <digitalmarketinginstitute.com>.

[16] Miesner, Jeffrey. “Latest Security Intelligence Report Shows 24 Percent of PCs are Unprotected.” Microsoft. 17 Apr. 2013. Accessed 9 March 2022. <blogs.microsoft.com>.