Economic & Social Council

Addressing the misuse of social media platforms

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Kiki Molenaar

Forum	Economic & Social Council
Issue:	Addressing the Misuse of Social Media Platforms
Student Officer:	Kiki Molenaar
Position:	Deputy Chair

Introduction

Social media has changed many lives, ranging from providing entertainment to a source of income. It has revolutionized the way we communicate and interact with our communities. Social media has started to influence the way people make decisions.

Social media platforms have many advantages, such as increased communication, entertainment, or even spreading awareness on certain topics such as the #MeToo movement. Social media has also become a place where users can speak out on certain things, such as racism, sexism, homophobia, etc. These platforms were made with the intention that the users will have positive experiences on them, but there are frequent cases of cyberbullying and sharing false information. There have been many cases of hacking or people threatening to leak private information, which could be detrimental to most individuals.

One of the main concerns with social media platforms is the spread of false information. False information can deceive people and shape opinions that are based on unsupported information. The sudden influx of fake news has led to many real-world consequences that have affected politics, health, and relationships between member states. The copious amount of fake news has made people wary of real and verified news sources (such as the BBC, New York Times, etc.).

After the spread of false information, the next concern that has impacted a lot of people is cyberbullying. There has been a flood of people who have realized that they do not have any consequences if they put a mean comment on a post made by someone or if they make a rude post about someone if they are shielded by the anonymity that social media offers. These individuals do

not take into account how people can act after getting harassed on the internet; in extreme cases, it can even lead to suicide.

Lastly, there has also been an increase in the exploitation of private data by the companies that own social media platforms. Social media platforms such as Instagram, Facebook, and other platforms owned by Mark Zuckerberg sell data to data collection companies, which then proceed to sell it to third party companies. The third party companies are usually advertisement companies, which then use that data to target people for certain advertisements. In fact, Facebook and Instagram make most of their money by selling user data. These companies track a lot of users' data without the user realizing it. Most of these companies look at the individual's messages, what they say in these messages, your IP address, all of the photos and videos on a user's phone, and so much more that they do not realize. This will go into more depth in the general overview.

Definition of Key Terms

Data privacy

Data privacy refers to a user's ability to control how much of their personal information is shared with social media sites or any other platform at all.

Cyberbullying

Cyberbullying is when someone sends threatening or abusive messages to other individuals via an electronic device. It is also possible to ridicule someone without messaging them directly, they can do this by writing a post about them on a social media platform.

Fake News / False information

It is the dissemination of false information, which can happen intentionally or accidentally.

Mental Health

An individual's mental health is a crucial component in their being that aids in coping with any pressures and issues they may encounter in life.

General Overview

Misleading information

Social media has revolutionized how people communicate with their societies, which also means that people have started to put things up on social media to try and deceive people and make them think that inaccurate information is true and factual. This can be extremely disorienting for certain people as they start to lose trust in the standard and verified ways to get news and information, such as newspapers, certified websites or apps, and news channels. Older generations have also become extremely naïve when it comes to the internet because they do not know how to properly use social media, so they tend to believe fake news much more than someone who is younger than them and grew up with social media platforms surrounding them and playing a big part in their lives. False information can cause a lot of damage to relationships, both domestically and internationally. Between 2020 and 2022, governments were alarmed when COVID-19 was very present, and there was a big influx of false information surrounding COVID-19, which convinced countless people about conspiracy theories involving COVID-19. This increased the reluctance people had when the COVID-19 va

Misinformation and Disinformation

Misinformation and disinformation are two different types of false information. Misinformation indicates that the information was spread unintentionally. While disinformation refers to the intentional spread of information to cause harm and deceive those who are receiving this information. Disinformation can affect the tension or even ruin a relationship between two states, which can be detrimental and even create conflicts that lead to casualties. Disinformation can arise when dealing with issues such as important elections, climate change, conflicts between states, or even public health.

Cyberbullying

This generation places a lot of emphasis on their social media presences since it may be utilized as a means of self-discovery, which is a concern that everyone faces their entire lives. People are beginning to be judged based on how many followers they have or what they have put on social

media, rather than using it as a constructive tool and letting everyone have a positive experience. Many users of social media can remain anonymous, which might increase their sense of security when using the internet, but it can also enable individuals to abuse other users in secret. All of these obligations and demands, as well as others, can have an impact on a person's mental health, which can result in self-harm or mental diseases such as depression or anxiety, among others. A person's mental health has a major impact on their daily life; it can have an impact on their interests, schoolwork, relationships, and so much more. Numerous studies and polls have suggested that 7 in 10 young people have encountered cyberbullying. Cyberbullying frequently involves discrimination of some kind, such as that based on race, gender, sexual orientation, or outward appearance. This demonstrates that cyberbullying frequently has a societal undertone of discrimination.

Anywhere other than school—like the victim's home, the library, or the park—was a safe haven for them before social media enabled bullying to become a widespread problem. Since bullying can now occur at home, in the library, or even in the park, there isn't really a place that is safe from it anymore. They become victims all the time, which can be mentally distressing and exhausting and increase a person's propensity for self-harm or even suicide. One in ten bullied people has attempted suicide, and one in three bullied people has hurt themselves. Additionally, it has been discovered that 50% of victims keep their abuse hidden out of humiliation or a lack of confidence in the help they can get from others.

Cyberbullying has assisted in bullying being spread to people of all ages. Any individual can be cruel to anyone online if they are protected by the veil of anonymity, which protects the abuser from any repercussions and prevents them from realizing what they are really doing to their victim.

Cybersecurity

Cybersecurity is a very prevalent topic in most governments, and now that social media has become very popular, the conversation is about how they will keep their citizens safe and allow them freedom while also making sure that hacking and illegal data collection do not occur.

Data Privacy

Data privacy has always been a very controversial topic between big social media platforms and governments. There needs to be a lot of security and firewalls put in place to keep all of the data in compliance and not let it be accessed by hackers. In August 2013, Yahoo had problems with their security systems, which led to a group of hackers getting access to more than 3 billion accounts. They had managed to collect most of their data, such as passwords and personal information, but fortunately, they did not manage to collect any bank details or payment information. This occurred when Yahoo was being sold to Verizon; this incident did not affect the deal with Verizon, and it was completed. The CISO of Verizon at the time, Chandra McMahon, stated, "Verizon is committed to the highest standards of accountability and transparency, and we proactively work to ensure the safety and security of our users and networks in an evolving landscape of online threats. Our investment in Yahoo is allowing that team to continue to take significant steps to enhance their security, as well as benefit from Verizon's experience and resources." after the deal was made successfully. Since then, security on all social media platforms has been continuously improved and worked on in all branches of the company, mainly security, as it is the biggest risk factor.

There was another incident that has had a much bigger impact on the security of over a billion Indian citizens' data. The Aadhaar system in India is a 12-digit code that holds all of the biometric and personal information. The citizens of India or the individuals that have been in India for 182 days or more in the last twelve months have one of these codes that they can access whenever they want. This code holds a lot of information that should not be shared, such as names, addresses, photos of the person, phone numbers,and emails. They also hold biometric data about the citizens, such as their fingerprints and iris scans. In January 2018, a group of hackers invaded the database; they got a hold of 1.1 billion digital codes and had access to all of their data. This put them all at risk as they now have most of their data, which increases the risk of identity theft or the perpetrators coming to their house, which can be extremely dangerous.

There have been so many more incidents, which is why it is extremely important that all countries make sure that the social media platforms in their countries are up-to-date in their security and make sure that these incidents do not happen.

Cyberattacks

Cyberattacks are extremely serious and can cause an extreme amount of damage to the databases of governments and the performance of social media platforms or websites on the internet. The first cyberattack was in 1988, which was also the year that the World Wide Web was launched. The cyberattack affected computers at Stanford, NASA, Princeton, and many other places. Since then, there have been so many major cyberattacks that they have only gotten worse and worse while people figured out what they could do to prevent them. In December 2015, a Russian hacker group that goes by the name of SandWorm launched an attack on the Ukrainian infrastructure, which led to the power grid being shut down for a portion of the country. This cyberattack was the first ever to get into a government's infrastructure, and it left 200,000 citizens without electricity for several hours. Since this was the first cyberattack ever on a government, this immediately made other member states paranoid, and they started working to improve the cyber security that they have in all aspects of their country, such as social media platforms, websites, and other things, to protect the wellbeing of their citizens. There have been many more cyberattacks that have caused and continue to cause damage to societies and the governments that surround them.

Major Parties Involved

European Union

The European Union has been closely regulating all social media platforms, and they have recently been making a lot of big steps in regards to the General Data Protection Regulation (GDPR). The GDPR has firm rules on how social media platforms should handle users' data and what they can collect.

United States

The U.S. government has been pressuring the big social media platforms to handle the users data better, and they have started paying more attention to possible antitrust issues that these social media platforms might bring upon the traditional news systems.

The United Nations

The United Nations (UN) has made countless resolutions on data privacy and misinformation. They have also had many discussions about cyberbullying and other elements of social media platforms that have been mistreated.

Russia

Russia has been involved in multiple cyberattacks against countries all around Europe, but specifically against Ukraine, since the war started. Their main target has been the Ukrainian military, but wind farms and internet users in central Europe have also been affected by cyberattacks.In 2014, the Russian government introduced a new law that all data from Russian citizens that has been collected from foreign companies be stored within the borders of russia. This has given the Russian government direct access to and control over this data, increasing the risk of surveillance for all Russian citizens.

China

China also established a data localization law that forces all companies that record the data of Chinese citizens to store that data within the Chinese border. This makes it easier for the Chinese government to access this data and sell it to third party companies or to find the location of certain people or the activities that their citizens are partaking in. China has also been found to have targeted American citizens using fake accounts on social media platforms such as Twitter, Instagram, and Facebook. They have been using these social media accounts to persuade citizens to vote in favor of Donald Trump by accusing Joe Biden of corruption. The social media accounts have also been found spreading messages under false pretenses, but they have been banned for breaking the policies of the social media accounts.

Timeline of Key Events

Date	Description of event
January 1st, 1989	The internet is invented
May, 1997	The world's first social networking site is made, it is called 'Six Degrees'
February, 2004	Facebook is launched by Mark Zuckerberg
March, 2006	Twitter is launched
May, 2010	Protests are organized all over Spain using Facebook and other social media platforms in response to debt crisis
October, 2010	Instagram is launched by Kevin Systrom, and Mike Kreiger
August, 2013	Yahoo's major security breach which lead to a hacking group accessing the data of 3 billion accounts.
October 15th, 2017	The #MeToo movement started which was to show the magnitude of people that have been sexually harassed.
January, 2018	Aadhaar system gets hacked and 1.1 billion indian citizens data has been accessed, including biometric data such as fingerprints and iris scans
March, 2018	Facebook goes on trial for harvesting data from 50 million users with Cambridge analytics
October, 2021	Meta was created, which merged Instagram, Facebook, and WhatsApp together.

UN involvement, Relevant Resolutions, Treaties and Events

- The right to privacy in the digital age, 18th December 2014 (A/RES/69/166)
- Report on countering disinformation for the promotion and protection of human rights and fundamental freedoms

Previous Attempts to solve the Issue

Facebook's fact-checking initiative

Facebook launched a fact-checking initiative in December 2016. This project has expanded to multiple countries where Facebook works with qualified third-party fact-checking organizations. It has been very successful so far and is constantly expanding to more and more countries.

Twitter spotlights credible information

In 2020, a plethora of false information was being spread about COVID-19, so Twitter started to add a new page for information on COVID-19 and the verified updates that were coming through on the situation. This helped a lot of people know which information to trust, as all of the verified information would be on a separate page for people to check.

Facebook's bullying prevention hub

Facebook has a separate subdivision in their resource panel dedicated to stopping cyberbullying, it has multiple resources in it including infographics, scripts on what people can say to people struggling with cyberbullying, and even things to say to the perpetrators. It also has a section where you can report the aggressors.

Possible Solutions

Frequent checks are made to verify information

Introducing frequent checks on all social media platforms to verify information that is being spread on major accounts can really reduce the number of cases of fake news and people being led to believe propaganda. This can be a challenging task for humans to do due to how tedious it is. It would be recommended to use an IA to check over this information, as it can be done swiftly and 24/7.

Banning the use of social media platforms for children below the age of 12

Banning the use of social media for children below the age of 12, can help with a child's real-life social skills, and they will also not be targeted for cyberbullying and getting hacked due to how naïve children can be.

Install a law where cyberbullying is banned

Installing a law or rules against cyberbullying would be extremely beneficial, as people would be more afraid to say or post something rude.

Bibliography

Balram, Dhruva. "Social Media and Human Rights: A Timeline - EachOther." *EachOther*, 10 Aug. 2021, eachother.org.uk/social-media-and-human-rights-a-timeline/. Accessed 28 July 2023.

Fox, Jacob. "8 Biggest Cyberattacks in History | Cobalt." *Cobalt.io*, Cobalt, 7 Oct. 2022, www.cobalt.io/blog/biggest-cybersecurity-attacks-in-history. Accessed 3 Aug. 2023.

"General Data Protection Regulation (GDPR) – Final Text Neatly Arranged." *General Data Protection Regulation (GDPR)*, 27 Sept. 2022, gdpr-info.eu/. Accessed 29 July 2023.

Hill, Michael. "The 15 Biggest Data Breaches of the 21st Century." *CSO Online*, CSO Online, 8 Nov. 2022, www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html. Accessed 3 Aug. 2023.

"ODS HOME PAGE." *Documents-Dds-Ny.un.org*, documents-dds-ny.un.org/doc/UNDOC/GEN/N22/459/24/PDF/N2245924.pdf?OpenElement.

"Russia behind Cyber Attack with Europe-Wide Impact an Hour before Ukraine Invasion." *Ncsc.gov.uk*, 2023, www.ncsc.gov.uk/news/russia-behind-cyber-attack-with-europe-wide-impact-hour-before-ukraine-invasion. Accessed 1 Aug. 2023.

Samur, Alexandra. "The History of Social Media in 33 Key Moments." *Social Media Marketing & Management Dashboard*, 6 Apr. 2023, blog.hootsuite.com/history-social-media/. Accessed 28 July 2023.

Scott, Mark. "China Influence Operation Targeted US Midterm Elections." *POLITICO*, POLITICO, 27 Sept. 2022, www.politico.eu/article/china-us-midterm-election-influence-meta-facebook/. Accessed 1 Aug. 2023.

Sherman, Justin. "Russia Is Weaponizing Its Data Laws against Foreign Organizations." *Brookings*, 27 Sept. 2022, www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/. Accessed 1 Aug. 2023.

Team, ODS. "ODS HOME PAGE." *Documents-Dds-Ny.un.org*, documents-dds-ny.un.org/doc/UNDOC/GEN/N14/707/03/PDF/N1470703.pdf?OpenElement.

"Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017) - DigiChina." *DigiChina*, 16 Aug. 2022, digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/. Accessed 1 Aug. 2023.

Vigderman, Aliza. "How Much Would You Sell Your Social Media Data For?" *Security.org*, Security.org, 23 Jan. 2023, www.security.org/blog/how-much-would-you-sell-your-social-media-data-for/. Accessed 28 July 2023.

"What Are Popular Platforms Doing to Stop the Spread of Fake News Online? | Internet Matters." *Internet Matters*, 16 Nov. 2020, www.internetmatters.org/hub/news-blogs/stopping-the-spread-of-fake-news-on-popular-online-platforms/. Accessed 29 July 2023.

"What Is Data Privacy? | Privacy Definition." *Cloudflare*, 2023, www.cloudflare.com/en-gb/learning/privacy/what-is-data-privacy/. Accessed 29 July 2023.