AI and Society: Ethical Challenges of Algorithmic Systems in the Digital Age

By:
Tyler Robinson

Submitted to the School of Liberal Studies and Continuing Education in partial fulfillment of the requirements for the degree of Bachelor of Arts
Purchase College State University of New York
May, 2025

Table of contents

Abstract

AI has done wonders and changed many things in our daily lives. But it has caused significant challenges when embedded into various social media platforms. This aims to paper analyzes the different problems we have encountered due to various uses of AI. Things like Privacy concerns and how it could possibly affect people's mental/physical health. We look at the different technologies used to better understand what we are dealing with. This paper is a collection of other studies and thoughts. One thing that is identified as the paper's main difficulty within social media is the spread of misinformation. It discusses things dating back to 2020 and recent times. They use a SEDPNR model that was originally used to analyze the spread of viruses/ diseases and modify it to analyze the spread of misinformation. The paper's main job is to bring attention to these difficulties and offer solutions that may mitigate or eliminate these challenges.

Introduction

In this digital age, social media has played a huge role in how people communicate with others, get their information, entertainment, etc. However, the rapid advancement of artificial intelligence (AI) has transformed industries, economies, and daily life in unprecedented ways. As AI becomes more deeply embedded in our social structures, especially through social media platforms, its harmful consequences are becoming increasingly apparent. While AI algorithms in social media are designed to enhance user experience by personalizing content, curating advertisements, and moderating inappropriate content, they have also inadvertently fostered negative social impacts. These impacts range from the promotion of misinformation and polarization to mental health issues and privacy concerns. We will examine AI algorithms, how they work, and explore the different ways they can be harmful. The goal of this will be to come up with ethical approaches that ensure fairness, transparency, accountability, and alignment with human values.

Background of AI

AI algorithms are sets of instructions or rules that enable computers to perform tasks that typically require human intelligence. These tasks include recognizing patterns, making predictions, solving problems, and even learning from data over time. AI algorithms are foundational in fields like machine learning, natural language processing, computer vision, and more, where

they're used to analyze data, make decisions, or perform automated actions. AI algorithms in social media are complex systems that analyze vast amounts of user data to make decisions, predict behaviors, and personalize content. They operate by learning from patterns in data, like what users click on, comment on, or share to improve the user experience and keep people engaged. There are three main learning approaches for AI: Supervised Learning, Unsupervised Learning, and Reinforcement learning. In **Supervised Learning**, the algorithm is trained on labeled data, where inputs and their correct outputs are provided. The goal is to learn the relationship between them. In **Unsupervised Learning,** the algorithm finds patterns in unlabeled data without specific instructions. It identifies clusters or relationships within the data. In **Reinforcement Learning,** the algorithm learns by trial and error. It interacts with an environment and receives rewards or penalties for its actions. Social media platforms collect data about everything users do: the posts they like, the videos they watch, the time they spend on different types of content, and even their interactions with ads. This data is accumulated and used to train AI models to understand patterns in user behavior. Once trained, the algorithm applies its learned model to real-world data. It makes decisions, provides recommendations, or performs classifications. For instance, if someone frequently watches cooking videos, the algorithm identifies this pattern as a "you like this imma show you more". This is also attributed to Ad Targeting. By analyzing user behavior and interests, algorithms determine the most relevant ads for each individual. So apps like Tiktok and Instagram analyze your likes and posts and try to feed you things similar to that and new things you may like. This AI algorithm is continuously learning. Based on what you put in the search engine and click on, it takes on this new data and

updates its model; this is called model retaining. The majority of social media platforms use a combination of Machine learning and deep learning algorithms that are tailored to optimize user experience, engagement, and content moderation. Many different types of algorithms come together to make our apps today. It's important to specify the differences between simplified algorithms and AI algorithms because companies implement both. They differ in complexity and purpose. Simplified algorithms are basic, rule-based systems designed to solve specific problems or perform tasks in a predictable and straightforward manner. They operate in a linear, deterministic way; given the same input, they will always produce the same output and do not adapt or learn over time. Some key differences would be that simplified has fixed rules, doesn't learn from new data, and is limited to simple things like sorting and calculations. Comparing how they work in social media, a Simplified Algorithm makes a chronological feed that displays posts in the order they were published.

- **Strength**: Simple, predictable, and easy to implement.
- **Weakness**: Does not prioritize relevant or interesting content for users.

Also, things like keywords can be easily filtered out with a simple Algorithm. An AI Algorithm creates a feed curated by machine learning, which ranks posts based on user preferences, engagement likelihood, and past behavior.

- **Strength**: Highly engaging, showing users what they’re most likely to interact with.
- **Weakness**: Can create filter bubbles, amplify harmful content, or reduce transparency.

AI can handle the immense volume of content and interactions on social media more effectively than simplified rules. Simplified algorithms in social media

provide predictable and transparent results, but are limited in handling modern challenges like content overload and user personalization. In contrast, AI algorithms enable platforms to deliver highly engaging and dynamic experiences. While the benefits of AI algorithms are significant, their transformative power also raises critical ethical and societal questions. The same algorithms that can optimize healthcare or improve efficiency can also amplify biases, invade privacy, and spread misinformation when misused or poorly implemented. This dual nature of AI highlights the need to critically examine its impact, as explored in this thesis.

This paper aims to identify several adverse effects associated with algorithmic systems. There are a lot of negative results that come from these Algorithms. The main concerns are the Amplification of Misinformation and Fake News, Impact on Mental Health, Privacy Infringement, and Data Exploitation.

Privacy Concerns

AI algorithms rely on vast amounts of user data to function effectively. While this data is used to enhance services, it often comes at the expense of user privacy. From targeted advertising to surveillance, the collection and misuse of personal data have sparked significant ethical and legal debates. AI algorithms are trained on large datasets collected from users' online activities, such as browsing history, search queries, social media interactions, and location data. Companies collect this information to:

- **Personalize Content:** Tailor recommendations, ads, and feeds to individual preferences.

- **Predict Behavior:** Anticipate what users are likely to engage with or purchase.
- **Monetize Data:** Sell insights to third parties, including advertisers and data brokers.

This extensive data collection often occurs without users fully understanding what is being gathered or how it is used. However, this could also be the fault of the users because most apps include clauses in their **terms and conditions** or **privacy policies** stating that they are allowed to collect, use, and share user data. These agreements often provide a legal framework for how a company handles user information, though the language used can sometimes be vague or difficult to understand. Types of data collected Personal Identifiable Information(PII): Data that directly identifies you, such as your name, email, or phone number, Behavioral Data: Data about how you use the app, like your browsing history, search queries, and time spent on specific pages and Location Data: Many apps, especially navigation and social apps, track your GPS location or approximate location through your IP address. Many people won't read these terms and conditions because they're so long and also very confusing. Therefore Users often unknowingly agree to terms of service that allow companies to harvest and share their information. Most recently, there was a case against TikTok, mainly regarding privacy. TikTok faced scrutiny for allegedly collecting biometric data and sharing user information with its parent company in China. This raised concerns about national security and privacy. These are valid concerns: What data are you taking, where is it going, and who are you giving it to? When you create an account on a social networking site, you enter into a deal where you give your data in exchange for networking and entertainment. The site then uses this data to make patterns,

observe your habits, and provide a platform for advertisers to sell their products. It's safe to say that they store data on physical servers only accessible from the company itself. In terms of sharing data, this mostly occurs when businesses exchange information for mutual benefit, such as improving services, targeting customers, or enhancing operational efficiency. The amount of data and the sources have no limit if you are online using your ID, your data is being gathered. For example, a their was a case where a girl who used Tinder for a while and found out that Tinder had so much information about her. Judith Duportail, a girl from Paris, recently got out of a relationship and decided to download Tinder. As most people know, Tinder is 1 of many popular dating apps where you make a profile that has your picture(s), info about yourself, and your interests. You see profiles of other people you might be interested in, and you swipe left or right for yes or no. If you swipe yes and they say yes, both people would start chatting to get to know each other, and then go on a date. That's pretty much how the app works. One day, she emailed Tinder to send her all the info they had on her. What came back was 800 pages of information with things like her Facebook likes, what/who she was interested in, conversations with other people on various apps, etc. In an article by the Guardian, she said “I was amazed by how much information I was voluntarily disclosing: from locations, interests and jobs, to pictures, music tastes and what I liked to eat.” That's horrifying but not surprising. Every company probably has the same, if not more, info on us. Having so much information, I imagined that it makes customers easier to manipulate. By manipulation, I mean convincing you to buy certain products, influence certain political opinions, and more. With that being said, since companies have so much information, another concern is hackers. A hacker getting hold of this

type of information is very dangerous. Even though people may have concerns, the terms and conditions are most of the time always available for you to view at a later date. For example Instagram, you would go into your profile tab and scroll to the very bottom. In Instagram's Privacy Policy section, it states that they are allowed to collect data across all Meta products. When dealing with third parties, Meta states, "We don't sell any of your information to anyone, and we never will." They only use your information to personalize your feed, send ads you might like, etc. So if you pay attention, then you will be able to see how all the companies you are connected to handle and process your data. Some types of regulations are critical for ensuring responsible data storage and sharing practices.

Mental Health

One of the most important topics today is mental health. There are many problems in our world but having the privilege of living in America, they aren't as "serious". Something that has been talked about a lot is the effects of social media platform's effects on mental health, especially among the younger generation. As we know, the systems are designed to maximize user engagement, often at the expense of emotional and psychological well-being. It has contributed to various mental health challenges, including anxiety, depression, and low self-esteem. Prioritize visually appealing and engagement-heavy content, often showcasing idealized versions of reality. This phenomenon is particularly evident on platforms like Instagram and TikTok, where curated images and videos dominate user feeds. This is not the full fault of the Algorithm because the content is posted by the user. But AI-driven filters and editing tools allow users to present unattainable versions

of themselves, further exacerbating the social comparison cycle. Studies link heavy social media use to body dissatisfaction, particularly among adolescents and young adults. AI algorithms are designed to keep users engaged for as long as possible by using techniques like infinite scrolling and personalized recommendations, also known as doom scrolling. Its Dopamine-driven engagement cycles make it difficult for users to disengage. These AI-driven addictions cause excessive screen time, which contributes to poor sleep quality, increased stress, a decrease in physical health, and social isolation. Platforms like YouTube and TikTok leverage recommendation systems that trap users in hours-long content consumption spirals, often at the expense of real-world connections and responsibilities. A term coming back is echo chambers. The promotion of misinformation could increase users' anxiety and stress. The lack of balanced viewpoints can lead to increased hostility and distrust among different groups, further contributing to emotional distress. A big example of this would be during the pandemic, when different content on what to do and others' opinions either conflicted with what they thought or affirmed their worries, causing increased anxiety. AI algorithms have fundamentally reshaped how individuals interact with technology, but their design often prioritizes engagement over well-being. The psychological effects—ranging from social comparison to addiction and exposure to harmful content—highlight the urgent need for ethical considerations in AI development. It's hard to accurately calculate the mental health struggles of people without a study. Many people don't openly share their problems because of pride or privacy. But it has become a trend to say you have certain mental health struggles on the internet. The problem with this is you can't accurately count these as truthful because it's a trend; people do trending

things to get clicks. By implementing thoughtful changes, society can harness AI's potential while minimizing its harm to mental health.

Misinformation

In terms of misinformation, a consequence of AI algorithms is their role in the spread of misinformation and fake news. Though the terms rumors, misinformation, disinformation, and fake news sound similar, each term has notable differences. Rumors are stories passed down from person to person, frequently with no evidence to back them up. Misinformation is similar in that it refers to disseminating incorrect information, not purposely created to harm. Disinformation, conversely, refers to the intentional fabrication and broadcast of erroneous content by individuals with the clear objective of inflicting harm. Fake news is a type of deception designed to appear as actual news. It is widely disseminated on social media and can be difficult to discern from genuine news. Misinformation in social media is characterized by its viral nature, often spreading faster and further than accurate information. Misinformation, especially on hot topics(topics that are currently trending), tends to get clicks more than accurate information. Social media algorithms prioritize content based on engagement rather than the accuracy of the content, leading to the widespread dissemination of misleading or false information. It is optimized for clicks, shares, and likes, which often means promoting sensational, polarizing content that is more likely to spark user interaction. An article on how social media has changed news says, “Today, more than 8 in 10 Americans get their news on digital devices – beating out TV, radio, or print. Among 18-29 year olds, social media is the most common news source.”(1)

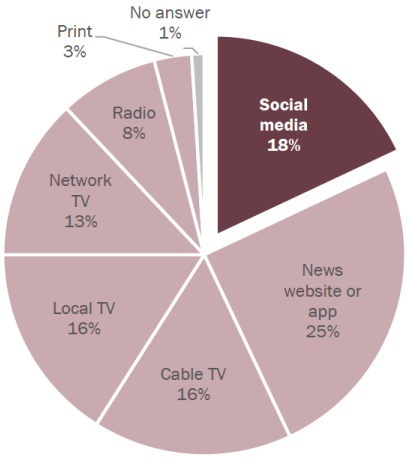

Figure 1: A graph showing what is most commonly used to get info. Image taken from Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable.

Yes, there are restrictions set in place to avoid certain things being posted, which can be helpful, and there is also a system in place where you can report these things, but that's only if you take the action to do so. Recommendation systems use collaborative filtering to suggest content similar to what users have previously engaged with. Over time, this can lead to "echo chambers," where users are exposed only to viewpoints that reinforce their beliefs, isolating them from diverse perspectives. It's gathering all the interests/thoughts on topics that people display. Most people say that social media is their common way of receiving election and political information are among the least likely to be following news about the 2020 presidential candidates. (1) Political misinformation spreads more rapidly in echo chambers as individuals are continually exposed to biased or false narratives without contradiction. During events such as elections or global health crises, this can have severe real-world implications by shaping public opinion based on misinformation. For example, during the 2020 U.S. presidential election,

platforms like Facebook and Twitter were heavily criticized for their role in spreading conspiracy theories. Studies show that false news spreads six times faster than factual content, largely because algorithms amplify posts with higher engagement metrics. Nowadays, it's hard to discern the news from the real facts, especially if you don't take the time to look more into it. Not only do you have to be wary of news, but also health and wellness content is a big thing on many social media platforms. Information is abundant on these platforms, and some things contradict each other. Telling us that these foods are bad or that this diet is good for you, etc. Studies have shown that misinformation spreads faster than verified news. This is because false stories are often crafted to be surprising or sensational, which increases their likelihood of being shared. A 2018 study by MIT found that false news stories are 70% more likely to be retweeted than truthful ones, largely due to algorithmic amplification. According to the article, “the scholars found, the spread of false information is essentially not due to bots - Instead, false news spreads faster around Twitter due to people retweeting inaccurate news items.” Addressing this issue requires rethinking algorithmic design to prioritize factual accuracy and ethical considerations. Platforms must develop robust content verification systems and offer greater transparency about how their algorithms function. However, addressing this problem requires more interaction in the algorithm, which I don't think companies would do.

Epidemic Modeling in Misinfomation

Speaking of 2020, the COVID-19 pandemic had to be what I think had the most impact on digital usage. If you don't know, COVID-19 was a global

health crisis that started in China and quickly spread worldwide. The virus primarily spreads through respiratory droplets, and symptoms range from mild (fever, cough) to severe (pneumonia, organ failure, and death). Governments implemented lockdowns, travel restrictions, and social distancing measures to prevent the spread, which in turn significantly impacted various aspects of life. The pandemic accelerated digital transformation across industries and personal lifestyles due to lockdowns and remote work. This has exponentially increased the use of social networks among all categories of people during the pandemic era. In “Epidemic modeling for misinformation spread in digital networks through a social intelligence approach,” Scientific Report. The report explores how misinformation spreads online using **epidemiological models** (commonly used to study diseases) while incorporating social intelligence factors. The different types of models used were SIR, SIS, SIER, SEDPNR, and SEPNS models. These models are mathematical frameworks used to study how diseases spread. The models are adapted to digital networks to analyze how misinformation spreads similarly to a virus. They believe it is an efficient technique to regulate misinformation and rumors by increasing fake news screening and cutting off the source of infection. Isolating fake news, like infectious disease, can generate fruitful results. The isolation is intended to keep fake news from exposure to other people and keep the content away from vulnerable groups. Once isolation measures are implemented, the system model parameters will be reduced. Just like a virus, misinformation has:

- **Susceptible (S)**: People who haven't encountered the misinformation yet.
- **Infected (I)**: People who believe and share the misinformation.

- **Recovered (R)**: People who stop sharing, either because they learned the truth or lost interest.

Here are examples of the epidemic models. Straight from the article

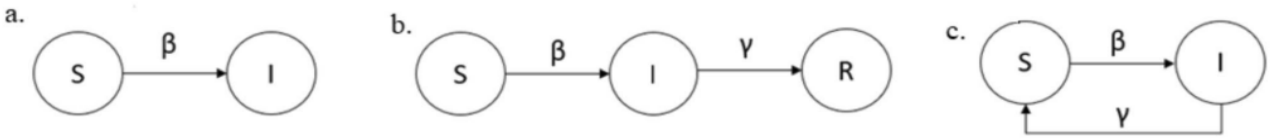

Figure 2: Shows the traditional epidemic models (a) SI model. (b) SIR model. (c) SIS model. Taken from Epidemic modeling for misinformation spread in digital networks through a social intelligence approach(1)

β (Infection Rate): Probability of a susceptible user encountering and believing misinformation. **γ (Recovery Rate)**: Probability of an infected user stopping the spread (either by learning the truth or disengaging).
It's very interesting how they were able to use math models that calculate virus spread to calculate the rapid spread of misinformation.
Here are the differential Equations for the SIR model

$$\frac{dS}{dt} = -\ \beta SI$$

$$\frac{dI}{dT} = \beta SI\ -\ \gamma I$$

$$\frac{dR}{dt} = \gamma I$$

The problem with this model is that it assumes that once recovered, they don't encounter misinformation again. While models can provide valuable insights, it's important to remember that user awareness is a crucial factor in combating misinformation. Future research on this can play a significant role in developing media literacy initiatives. These initiatives are crucial in equipping users with the skills to evaluate the information they encounter

online critically. We mustn't take everything at face value. We need to educate people to take in information that interests them and research more about that claim before they support it. As stated previously, there are lots of different models we can use to study how information is spread like a virus. According to the article, when it comes to how information is dispersed and user belief states are represented, the SEDPNR model differs greatly from the SIR and SEIR models. SIR/SEIR is more concerned with biological processes, whereas SEDPNR is more concerned with user psychology and social effects on information. It's an extension of classical epidemic models like SIR (Susceptible-Infected-Recovered), but is adapted for misinformation dynamics. SEDPNR comprised of

- (S) Susceptible -Individuals who have not encountered the misinformation but can be influenced by it
- (E) Exposed- Individuals who have encountered the misinformation but have not started spreading it yet.
- (D) Doubters- Individuals who have seen the misinformation but are skeptical and hesitant to spread it.
- (P)Promoters- Individuals who actively believe and spread the misinformation.
- (N)Negators- Individuals who have seen the misinformation and reject it, possibly trying to counteract it.
- (R)Recovered/Removed- Individuals who no longer participate in the misinformation spread, either because they lost interest or were convinced of the truth.

How this differs from the SIR Models: It incorporates hesitation instead of instant belief, includes a Negator class to model counter-misinformation

efforts, and is more realistic for digital networks, where misinformation can be questioned, rejected, or promoted rather than just "infecting" users. This leads to more accurate predictions of how rumors will evolve and defuse in these networks. By diving deeper into this model, future research can uncover the circumstances in which rumors will either thrive or die. The SEDPNR model can help guide the development of debunking tactics by providing a sophisticated understanding of user behavior and information spread. The Doubt function is an important realization. The model highlights the Doubter state as an essential area for intervention. Policyholders can encourage the dissemination of factual counter-narratives that dispel people's particular doubts. Here is a proposed model:

The problem with this model is that it assumes that once recovered, they don't encounter misinformation again. While models can provide valuable insights, it's important to remember that user awareness is a crucial factor in combating misinformation. Future research on this can play a significant role in developing media literacy initiatives. These initiatives are crucial in equipping users with the skills to evaluate the information they encounter online critically. We mustn't take everything at face value. We need to educate people to take in information that interests them and research more about that claim before they support it. As stated previously, there are lots of different models we can use to study how information is spread like a virus. According to the article, when it comes to how information is dispersed and user belief states are represented, the SEDPNR model differs greatly from the SIR and SEIR models. SIR/SEIR is more concerned with biological processes, whereas SEDPNR is more concerned with user psychology and social effects on information. It's an extension of classical epidemic models like SIR

(Susceptible-Infected-Recovered), but is adapted for misinformation dynamics. SEDPNR comprised of

- (S) Susceptible -Individuals who have not encountered the misinformation but can be influenced by it
- (E) Exposed- Individuals who have encountered the misinformation but have not started spreading it yet.
- (D) Doubters- Individuals who have seen the misinformation but are skeptical and hesitant to spread it.
- (P)Promoters- Individuals who actively believe and spread the misinformation.
- (N)Negators- Individuals who have seen the misinformation and reject it, possibly trying to counteract it.
- (R)Recovered/Removed- Individuals who no longer participate in the misinformation spread, either because they lost interest or were convinced of the truth.

How this differs from the SIR Models: It incorporates hesitation instead of instant belief, includes a Negator class to model counter-misinformation efforts, and is more realistic for digital networks, where misinformation can be questioned, rejected, or promoted rather than just "infecting" users. This leads to more accurate predictions of how rumors will evolve and defuse in these networks. By diving deeper into this model, future research can uncover the circumstances in which rumors will either thrive or die. The SEDPNR model can help guide the development of debunking tactics by providing a sophisticated understanding of user behavior and information spread. The Doubt function is an important realization. The model highlights the Doubter state as an essential area for intervention. Policyholders can encourage the

dissemination of factual counter-narratives that dispel people's particular doubts. Here is a proposed model:

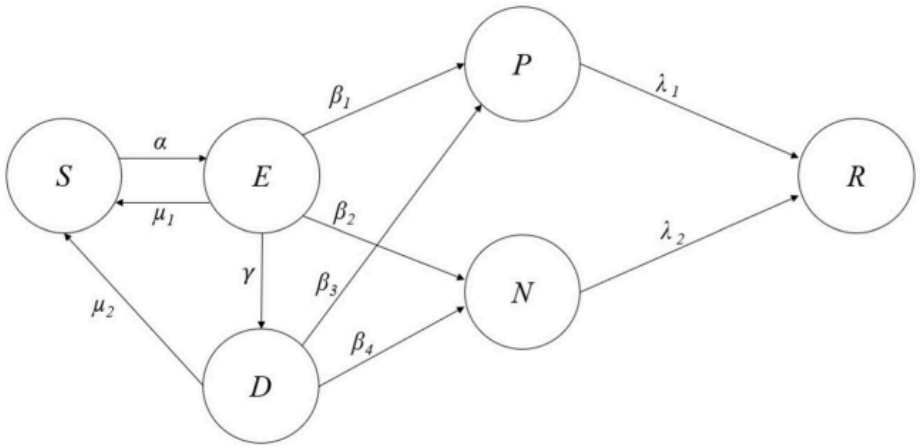

Figure 3: This is the SEDPNR model. (1) Taken from Epidemic modeling for misinformation spread in digital networks through a social intelligence approach

- **β** (transmission rate) – How easily misinformation spreads.
- **α** (exposure rate) – How quickly exposed individuals move to different states.
- **δ** (doubt rate) – The rate at which exposed people become doubters.
- **γ** (negation rate) – The rate at which people reject misinformation.
- **μ** (recovery rate) – How fast people stop engaging with the misinformation.

I thought this was a very interesting way of understanding the spread of misinformation or just information in general. You think about how it relates to virus spread. We see who it starts with, if they are "immune" or susceptible. The people who are infected might spread or they can heal. While the SEDPNR model can offer valuable insight into the spread of misinformation, it doesn't necessarily enhance our control over it. We can't control free speech, and we don't want to, but when something is wrong or fully truthful, we want to

address that and show the other side. And with models like this, we can maybe address where this is coming from and implement things like fact-checking. In future work, if the plan uses this more effectively, they would have to improve on some aspects of the models. The model's transition between user belief states (like Doubter to Infected) is a complex process, and the model's current approach could benefit from more empirical backing. One of the main limitations of the model is that it treats transitions as binary events based on encountering information or social influence. Real-world transitions are not like that. They are likely influenced by various factors like the information's content, user experience, and individual psychology. Moreover, validating the model requires data on user belief states, which can be challenging to collect ethically on social media platforms. Additionally, self-reported data might need to reflect internal beliefs accurately. By considering this, future work can be focused on conducting controlled studies where users are exposed to different types of misinformation, which can help understand how factors like content, source, and user experience influence transitions between belief states. Additionally, analyzing user engagement (likes, shares, comments) alongside sentiment analysis can provide indirect insights into user belief states.

The following recommendations aim to mitigate the harm caused by AI systems, particularly in contexts such as misinformation, privacy invasion, and mental health impacts. These strategies focus on promoting transparency, accountability, and ethical design while emphasizing the importance of regulation and oversight. A significant challenge with AI algorithms is their "black box" nature—users and regulators often cannot see how these systems work or make decisions. Since humans create these algorithms, it is important

that we embed societal values into social media algorithms. Even though values can differ between cultures, they are things that are agreed upon everywhere or should be. Transparency ensures that stakeholders understand how algorithms function, what data they use, and the logic behind their outputs. So, things like requiring companies to explain in clear terms how their AI systems operate, or providing tools that allow users to view and modify algorithmic recommendations. An example of this would be the Judith case of the European Union's Digital Services Act (DSA) or the Data Protection law that mandates transparency and allows European citizens to acquire their data from American companies. Companies should simplify platform policies so users understand how their data is used and how AI influences their experience. Another solution is to have more ethical designs on the line to ensure that AI systems prioritize human well-being and fairness over mere engagement or profit. Human-Centric Algorithms: Redesign systems to prioritize positive societal outcomes rather than clicks or shares. An example would be Algorithms that could promote verified, balanced news over sensational or polarizing content. The most important solution, and one that I believe could be easily implemented, is promoting public education on these topics. Something like a media literacy campaign to teach users how to critically evaluate content and recognize manipulative tactics driven by AI. So, schools are offering digital literacy, especially since they have started to implement more technology in their schools.

Conclusions

The potential harms of AI algorithms on social media highlight the urgent need for ethical AI development and regulatory oversight. As these

algorithms continue to shape how we access information, interact with others, and perceive the world, their impact on individuals and society cannot be ignored. A concerted effort by policymakers, technology companies, and civil society organizations is necessary to address the ethical challenges posed by AI. Solutions might include transparency in algorithmic decision-making, data privacy protections, mechanisms to detect and reduce bias, and regulations to prevent the spread of harmful misinformation. Ultimately, the goal should be to create AI systems that prioritize human well-being over profit and that contribute positively to society rather than eroding it. Without such measures, the harmful effects of AI in social media will only continue to grow, affecting not only individual users but also the very fabric of society. Hopefully, this has sparked a discussion within you. Further work is needed for us to say we strive for a better future.

References

(1) Mitchell, A. Jurkowitz, M. Oliphant, B. and Shearer, E. (2020)**Americans Who Mainly Get Their News on Social Media Are Less Engaged, Less Knowledgeable**
https://pewrsr.ch/30bullp

(2) (2024)**Embedding Societal Values into Social Media Algorithms**
https://tsjournal.org/index.php/jots/article/view/148

(3) Sreeraag G. & Shybu Padinjappurath G.(2024) **Epidemic modeling for misinformation spread in digital networks through a social intelligence approach**
https://www.nature.com/articles/s41598-024-69657-0#Abs1

(4) Julia Ostheimer& Sarfraz Iqbal(2019) **Privacy in online dating: does it matter?**
https://www.researchgate.net/publication/332384729_Privacy_in_online_dating_does_it_matter

(5) **The official website of the European Union4**
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

(6) **Terms of Use**
https://help.instagram.com/581066165581870/

(7) **Meta Privacy Center**
https://privacycenter.instagram.com/policy/