Social Media – Recommendations for Change

Adopted by the IEEE-USA
Board of Directors (16 February 2024)

Internet Social Media in its various forms has created opportunities, and concerns in many areas. It can be a highly selective and presumably efficient advertising channel. It creates opportunities for dialogue among diverse communities. Unfortunately, social media also can foster division, inflame rhetoric, and isolate individuals into "filter bubbles." Isolation and bullying at the individual level can trigger teen-age self harm.[1] Misinformation and inflammatory rhetoric at the national level can foster hate groups, social unrest and even genocidal activities.[2]

Recommendations

Some potential ways to address the challenges posed by social media and big data include:

Liability for known algorithmic harm – Platform managers are often aware of the harm associated with their algorithms. Internal efforts to rectify these problems have been rejected.[3] Clearly removing any Section 230 protection for the mediation of content that is promoted/recommended by algorithms or related corporate decisions would establish a basis for liability in these situations. Situations leading to significant harm to persons or property should be subject to prosecution of individuals involved for criminal negligence, including corporate management.

Verified Users – User accounts can be verified for being held by a human or a legitimate entity. Such verification can be conducted using uniform and accepted protocols to reduce abuse. Platforms and users should have tools to determine when to filter for "verified persons." This can also create a path to hold users accountable for the many forms of abuse and malfeasance that can occur. Transactions should be traceable to a verified identity, and logs retained for adequate duration, subject to criminal and civil legal

---

[1] https://www.theatlantic.com/ideas/archive/2021/11/facebooks-dangerous-experiment-teen-girls/620767/ retrieved 9 Nov 2022

[2] https://www.reuters.com/article/us-myanmar-rohingya-facebook-idUSKCN1GO2PN retrieved 9 Nov 2022

[3] https://www.theguardian.com/technology/2018/feb/02/youtube-algorithm-election-clinton-trump-guillaume-chaslot retrieved 9 Nov 2022

discovery. Where anonymity is appropriate, such as witness protection, explicit designations should also be provided and available for filtering.

Transparency – Users should be able to easily identify paid content when it is presented and the source of both the content and the funding for that content. Archives of paid content should be maintained and also be publicly accessible to enable analysis that can identify issues and abuses that might not be visible individually but can be discerned from the collective information. Content sources should also be clearly identified.

Informed Consent and Control of data compilations. Users should be able to understand what data is being retained by platforms,[4] including data "inferred" about them, data obtained from third parties as well as data shared or sold. Original compilers and third-party aggregators should be subject to information handling laws similar to that which applies to credit rating services. Users should be able to trace what personal information is being shared/stored where, to verify the information is correct, to prevent ("opt out" of) the collection and storage of specific information, and to appeal decisions by an information handler that affects the user's personal information.

Integrating Time Limits – Sites should provide parental/individual control for the maximum number of continuous hours, total hours in a day, and excluded hours of the day for individual use. This can reduce the potential for addiction and support individual time management.

Algorithmic Choice – users should be able to determine and control what the impact of a service's algorithms will be on them. Users should be enabled to select algorithm objectives used to manipulate their experience. This includes not only the ability to positively accept specific information processing rules, but also providing methods for users to exclude specific sources, types of content and use of their personal data/profile.

Collaborative collective filtering – Just as "Like" has become a method to promote popular content, all services should also uniformly adopt and utilize a "block/flag" feature to provide a crowd-sourced way to train the algorithms to lower the priority of some content, or flag it for human review. Both 'like' and 'flag' should only be usable by verified users to avoid manipulation of results.

The value of data is significant in today's information-driven economy – With such high value comes the responsibility to regulate to maintain fairness, transparency and

---

[4] The European General Data Protection Regulation (GDPR) provides an example here: https://gdpr.eu/data-privacy/ retrieved 16 Feb 2023

competition. Government should provide the relevant agencies the funding and legal clout necessary to oversee this vast and growing market.

Research Access – Anonymized data should be made available for research. The dominant online service providers should make their data available without cost to accredited researchers to provide transparency, assure compliance, and competition. This will allow researchers to verify claims, identify issues and to balance the scales of unlimited data harvesting.

The U.S. is behind Europe on this topic

Whistleblower Frances Haugen explained to Time Magazine, "The new U.K. and E.U. laws have the potential to force Facebook and its competitors to open up their algorithms to public scrutiny, and face large fines if they fail to address problematic impacts of their platforms." European lawmakers and regulators "have been on this journey a little longer" than their U.S. counterparts, Haugen says diplomatically. "My goal was to support lawmakers as they think through these issues."[5] E.U. fines are sufficient that few businesses would consider them an acceptable cost for doing business. Harmonization with E.U. regulation can reduce the provider costs of separate U.S. regulation, while taking into consideration the existent impact in the E.U.

Background

We recommend reviewing our IEEE-USA whitepaper on Social Media Challenges and Considerations which expands on the context for our recommendations, so we highlight specific additional context here.

Failure to effectively address the destructive potential of such activity as online bullying, propagation of disinformation and misinformation, and promotion of hate groups can result in self-harm to young persons,[6] impacts to the safety and security of individuals,[7] malicious destruction of corporate and personal reputations,[8] ill-informed social movements,[9,10] and

---

[5] https://time.com/6121931/frances-haugen-facebook-whistleblower-profile/ published 22 Nov 2021, retrieved 4 Jan 2023

[6] https://counseling.northwestern.edu/blog/effects-social-media-teen-girls/ retrieved 1 Nov 2022

[7] https://www.cnn.com/2022/10/28/politics/pelosi-attack-suspect-conspiracy-theories-invs/index.html retrieved 1 Nov 2022

[8] https://www.snopes.com/articles/402899/what-was-gamergate/ retrieved 1 Nov 2022

[9] https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections retrieved 1 Nov 2022

[10] https://www.nytimes.com/2018/03/08/technology/sri-lanka-facebook-shutdown.html ; retrieved 24 Jan 2023

unrest;[11] as well as concerns about unfair competition, fraud, deception and illegal trade practices[12]. Policy actions can significantly reduce their frequency and severity while providing for accountability and prosecution of wrongdoing.

Advertising and engagement are primary sources of revenue for key internet sites and services.[13] Such services also track online individual behavior to sell ads and promote content. Cross-platform integration of user behavior is used to prepare detailed psychodemographic[14] profiles of individuals, which enables very sophisticated psychological targeting of unaware individuals. The profitability of grabbing and holding individual engagements, often through fake, outrageous or hateful content is a significant incentive to continue these activities. These incentives as well as the opportunities for abuse to the detriment of individuals and the social good are key justifications for policy and enforcement action.

Both platform managers[15,16] and interested parties such as foreign governments[17] have taken notice, and in the latter case, advantage of these characteristics.[18]

This statement was developed by IEEE-USA's Committee on Communications Policy and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of the nearly 150,000 engineering, computing and allied professionals who are U.S. members of IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE, or its other organizational units.

---

[11] https://insights.bu.edu/when-influence-goes-too-far-social-medias-effect-on-the-capitol-riots/ retrieved 1 Nov 2022

[12] https://www.nytimes.com/2021/06/04/business/facebook-eu-uk-antitrust.html retrieved 16 Feb 2023

[13] https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html retrieved 24 Jan 2023

[14] Meaning from Merriam-Webster.com: market research or statistics classifying population groups according to psychological variables (such as attitudes, values, or fears)

[15] https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress retrieved 1 Nov 2022

[16] https://www.wsj.com/articles/the-facebook-files-11631713039?mod=bigtop-breadcrumb retrieved 1 Nov 2022

[17] https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections retrieved 1 Nov 2022

[18] https://intelligence.house.gov/social-media-content/ retrieved 1 Nov 2022