



Council of the European Union
General Secretariat

Brussels, 18 March 2022

**DOCUMENT PARTIALLY ACCESSIBLE
TO THE PUBLIC (16.05.2022)**

WK 4034/2022 INIT

LIMITE

**COMPET
MI
JAI
TELECOM
CT**

**PI
AUDIO
CONSOM
CODEC
JUSTCIV
TTC**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

| | |
|----------|--|
| From: | European Commission |
| To: | Delegations |
| Subject: | EU-US Trade and Technology Council Working Group 5 Workshop 2: Algorithmic Amplification |

EU-US Trade and Technology Council Working Group 5

Workshop 2: Algorithmic Amplification

Friday, 4 March 2022

Participants

- [REDACTED] (Dublin City University)
- [REDACTED] (Sorbonne Nouvelle - Paris 3)
- [REDACTED] (University of Amsterdam)
- [REDACTED] (Vrije Universiteit Brussels)
- [REDACTED] (TU Delft)
- [REDACTED] (University of Texas Center for Media Engagement)
- [REDACTED] (AI Forensics)
- [REDACTED] (University of Amsterdam)
- [REDACTED] (Rutgers University, GMF)
- [REDACTED] (AWO)
- [REDACTED] (European Commission)
- [REDACTED] (US Government)
- [REDACTED] (US Government)

Introduction

The meeting began with introductory remarks from the representatives of the European Commission and the US Government, who highlighted the policy challenges and potential harms caused by algorithmic amplification. Both sides stressed the high stakes of the problem and were keen to discuss the broad term of algorithmic amplification and the key questions and challenges it poses for researchers and policymakers.

The Impact of Algorithmic Amplification

The discussion began with a historical overview of algorithmic amplification, noting that it began attracting special attention as a research category when ties to terrorism were investigated in the early 2010s. In terrorism studies, work has focused on recommender systems and online radicalization. Research on YouTube has been directed towards YouTube's recommender system because of the role it plays in extremism and radicalization. The global consensus around terrorism has made it easier to make decisions around recommender systems and its role in amplifying terrorist networks.

Earlier work on Facebook, and the impact that tweaks to its newsfeed have had on the content that is amplified, also shows the significance of recommender systems. These analyses are dynamic, as users then pivoted to private groups. These private groups have amplified QAnon and played

significant roles in events like the one that took place on January 6 in the U.S. Capitol. More recently, focus has shifted to high levels of activity and misinformation in Ukraine.

Participants noted that the role played by algorithms across a range of platforms and the amplification of broader polarizing issues should be examined despite significant data constraints. The objectives in mitigating risks associated with algorithmic amplification have expanded beyond terrorism to encompass broader societal risks and issues. Participants argued that while it was easier to make decisions surrounding terrorism, more complicated divisions have arisen regarding what type of growth is appropriate on platforms and whether the problem lies in amplification or publication. Recommender systems are designed to maximize engagement, which can lead to problems when the behavior of an algorithm interacts with the bias of users. Some participants felt that because the algorithms amplify the most polarizing and addictive issues, the population most at risk is not children, but rather adults with poor education and digital literacy skills and who lack the ability to upskill.

Mitigating Risks

Participants debated to what extent risks posed by algorithmic amplification might be mitigated and what should be addressed when looking to mitigate those risks. Examples such as employing bots to emulate specific conditions in order to observe subsequent recommendations could help provide more data to researchers. The lack of data is a significant problem which could also be addressed with user-donated data that could be used to analyze algorithms. This data could be used to establish baselines which are critical in establishing the difference between organic amplification and amplified growth.

Algorithms also pose problems of user empowerment, as users may not naturally engage with abstract notions of choosing among different options of potential algorithms. Participants argued instead that users' existing modes of engagement with algorithms should be studied and built upon. One of the challenges in mitigating risks comes from defining what risks should be mitigated and what tools are needed to do so. There is a lack of diversity amongst recommender systems and regulators need to establish if the responsibility of algorithmic amplification lies within the design, the amplification, or through growth. One recommendation would create a table of risks which would address the risks of harms caused by disinformation.

The U.S. and Europe's approaches to protecting rights and freedom of expression online differ, and participants agreed on the importance of clearly defining which public interest principles regulation or mitigation is seeking to protect before then comparing such measures to the principles platforms are optimized for. These platforms are doing business across various cultures and nations, but a universal agreement on what constitutes good behavior does not exist. Participants ultimately questioned if algorithms and platforms can act in the best interests of users, as they are better at

respecting the interest of advertisers, clients, and investors than of users. Users could be brought in via instituting participatory models.

The imposition of data access requirements via legislation should be accompanied by a funding mechanism to hold stakeholders accountable. Participants agreed that civil society and NGOs cannot be expected to become platform watchdogs without support. Tech accountability on every level requires funding, but a consensus was not reached as to where it should come from, whether through taxing companies or public spending.

Participants also laid out various ways in which platforms could be held accountable to mitigate the risks associated with algorithmic amplification. They first considered how platforms could incorporate different signals and tools to intervene and editorialize the process of amplification. This could include stricter duties of care to editorialize more extreme amplification. Others argued for more complex and sophisticated transparency which could show how and where amplification takes place. Sharing of internal tools is critical to holding platforms accountable, as platforms give relatively little information about audience to non-paying users (i.e., non-advertisers).

Some participants looked at changes to platform Terms of Service as a way to mitigate risks, offering various ways to edit Terms of Service to better address concerns. By working on editing Terms of Service, the problem is solved before content moderation becomes necessary. Some felt that algorithmic amplification was a fundamental platform design problem, one that cannot be solved with content moderation. They cited smaller platforms as models to show how community-based platforms and social moderation were able to stop the effects of algorithmic amplification. One solution would be to focus on building up healthy online communities rather than trying to address legal problems that would arise from algorithmic amplification. One participant cited WhatsApp Brazil as an example of successful changes to technical design which then mitigated the risks of algorithmic amplification. WhatsApp Brazil input a feature that only let users forward to two contacts, which helped bring down the spread of misinformation. With platforms redesigning to be better and safe, due process could be reinstated when it comes to the removal of content, as harmful content will be caught earlier.

Participants agreed that regulation is key to ensure trustworthiness. Regulation should start with the assumption that the platforms are not trustworthy, and their integrity cannot be relied upon. Participants cited Facebook limiting CrowdTangle and giving data to select actors when the findings did not present well for Facebook. In addition to regulation, some participants believed that all data provided by platforms should be audited. Data access is important in shaping the ability of regulators to respond, and participants were adamant in protecting access to it. Regulation could consider a liability framework parallel to the broadcasting context. A platform's duties and responsibilities should increase with amplification, with implementation of a sliding scale for different platforms such as Facebook and 4chan. Some participants, however, debated the usefulness of regulation, noting that they felt that the European media regulators had no real idea of what was happening on

platforms. They felt that regulators lacked data, info, and substance on which to regulate. Finally, it was agreed that platforms should pay fines, but participants did not reach a consensus as to the payment recipient.

While platforms should implement measures to mitigate risks, participants also addressed voluntary measures that could be taken by users alongside platforms. In terms of data access, users could donate their data for analysis. Participants felt that digital literacy was key, as well as exposure to public service media to counter algorithmic entrapment. Users, especially adult users, need to be informed of the consequences of amplification and how it nudges their decision-making. By exposing users to public service media, users can counter amplification harms. Participants also noted that public media principles could be applied in a platform context and used to counter content on platforms. Participants also noted that content creators could be used to mitigate risks as well through being empowered to choose the content recommended with their own, similar to the choices available to advertisers. In general, the consensus was that voluntary measures should empower users, civil society, journalists, and others who can employ the output of transparency measures around recommender system choices to achieve greater accountability. This could be especially useful in a context where structural funding mechanisms to create capacity, such as public auditors, are missing, but also necessary to get objective statements.

Final Remarks

Participants closed the meeting by noting that amplification can ultimately play a positive role as well. Platforms should respect users as the audience and speaker when deciding to act on amplification and downranking. Participants also noted that despite the focus on amplification of harmful content, some of the worst content online comes from rudimentary websites that don't optimize or algorithmically rank content at all. Websites such as Stormfront, 4chan, or messaging services like WhatsApp, all of which lack ranking or recommendation systems, can still amplify risky content. It is therefore important to continue to distinguish between organic amplification and that which stems from platform design or algorithms.