Policy Recommendations on Tackling Disinformation Online

November 2021

The European Commission has the chance to effectively minimize the negative impact of disinformation through proper enforcement of existing rules and where needed draft new pieces of legislation such as for transparency requirements of content delivered to users. Targeted advertising is the core of disseminating disinformation. In order to prevent the spread of disinformation elaborated in "fake news factories" we should aim to regulate the distribution and the targeting techniques.

Phase-out advertising based on personal data, including tracking and other inferred data. In order to target the core of the currently toxic business model, targeting in advertising can only be based on the information that people provided voluntarily and explicitly, and they should be able to access, review and change what the platforms knows about them when they are targeted with specific content or ads. The advertising model and content curation should be based on contextual-based information and only personalise it more based on the preferences that people provide voluntarily without being nudged via forced "consent". In order to ensure this, dark patterns practices[1] must be banned, and automated signals (Do Not Track-like) and other privacy-by-design and by-default features must be imposed on browsers, OS, hardware and apps to guarantee people's security and privacy.

The European Union should establish minimum safeguards for users' default settings to require an "opt-in" to personalised content recommendations systems rather than the current default "opt-out." Platforms should design "consent" and privacy policies in a way that facilitates informed choice for users and is compliant with data protection laws. Users have to be able to exercise minimal control over recommendation systems that can be secured by an "opt-in" mechanism. Making content recommender systems available via "opt-in" by default would be a desirable mechanism because even those users who are less aware of how these systems operate will not be treated less favourably. Those users who decide to receive content recommendations should be able to:

- Exclude certain content from their recommendations;
- Exclude certain sources of content from their recommendations;
- Ask for profiles to be deleted and access the service even when refusing to use content recommendations, to ensure the opt-in is meaningful. Users should be able to do so in an easy and free manner, and at any time they wish.

[1] See more on dark patterns in Norwegian Consumer Council, 2020, Out of control, https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

A robust risk assessment must fix the weaknesses of self-evaluation by online platforms and empower regulators and civil society to effectively hold them to account.

Transparency of online targeted advertisements serves as a safeguard to ensure proper oversight. Online platforms should be subject to meaningful and qualitative transparency obligations supported by proper oversight. This includes mandatory disclaimers on all political and issue-based advertisements, including detailed information on why, how, and by whom advertisement recipients are targeted, as well as mandatory archives with detailed information on paid content. The archive should contain, among other things, the advertisement's content, the targeting criteria used to reach out to online platform users, the amount spent, the time it started and the time it stopped and the performance of the advertisement. The archive must be publicly available, easy to navigate, and designed to facilitate research and analysis. Public access to information related to direct and indirect payments or any other remuneration received to display advertisement must be ensured. We are of the opinion that civil society, independent researchers, relevant authorities, national electoral commissions, other public authorities, and regulatory bodies should be able to monitor and evaluate political advertising and better understand its impact on democracy and fundamental rights.

As a part of meaningful transparency, it is necessary to ensure that content-recommender models are being adequately explained to users. Explanation of the family of models, input data, performance metrics, and how the model was tested should be communicated to users in tangible and comprehensible language. Such an explanation will allow users to contest the algorithmic decision-making and/or to opt-out. The right to oppose the use of automated decision-making systems should apply even if a human is involved in the process.

Strong enforcement of the GDPR and adoption of a strengthened ePrivacy Regulation are key to eliminate targeting techniques and limit the spread of disinformation. The European Commission and national Data Protection Authorities (DPAs) must properly enforce the GDPR. The GDPR safeguards EU residents' rights and prevents the misuse of their personal data for targeting purposes. It can eliminate black and grey patterns that online platforms use to trick users into sharing their data, such as "I agree" buttons that users click to get rid of annoying pop-ups or banners. Well-informed consent on behalf of the user is needed prior to processing personal data for targeted advertising. Even though the GDPR provides solid ground for valid consent requirements, the lack of enforcement creates a reference in new pieces of legislation, such as the Digital Services Act (DSA), ePrivacy Regulation and the relevant upcoming proposal for targeted political advertising.

Ensure that online platforms properly disclose that a user is or will be subjected to algorithmic decision making, including personalised content curation. Meaningful

awareness enables individual users to opt-out if they wish to do so. However, users have to be able to exercise control over recommendation systems that can be secured by an "opt-in" mechanism by default. Platforms should design consent and privacy policies in a way that facilitates informed users' choice, in line with the GDPR.

Strengthen data protection rules through DSA and ePrivacy Regulation. The Commission and national DPAs should elaborate guidance to clarify how the GDPR should be applied to targeted dissemination of advertisement. The draft ePrivacy regulation and the draft Digital Services Act offer the possibility to fine-tune GDPR rules in this field. In addition, the Commission should urge the Member States to provide DPAs with the funds necessary for the tasks they are expected to undertake providing them with expertise and services. We encourage the quick adoption of a strengthened ePrivacy Regulation that includes strong privacy by design and by default protections.

Conduct Data Protection Impact Assessments and ex ante mandatory Human Rights Impact Assessments (HRIA). In fulfilling their transparency obligations, political parties, interest groups, and platforms should be required to conduct and publish Data Protection Impact Assessments and a Human Rights Impact Assessment relating to online political campaigns hosted on relevant platforms. We advocate introducing a HRIA[2] that analyses the effects that business activities have on users. An HRIA follows a human rights-based approach, which integrates human rights principles such as personal data protection, non-discrimination, freedom to access information into the assessment process.

Empower people. There is a severe power imbalance between online platforms and users. Users should have more control over their news feed and their personal data online. They should be allowed to decide whether they want to receive targeted political advertisements or not. For this to happen, and in accordance with EU data protection rules, online platforms should receive users' explicit consent via an opt-in. To limit pop-up fatigue, automated binding signals (as mentioned above) must be used by default; furthermore, there should be rules that limit how often online platforms can ask users to opt-in and that ban dark patterns. A mechanism where online platforms must answer users' (data subject) requests about their targeting methods, the data processed, and the rights set out in Article 15 of the GDPR. Online platforms should have 15 days to answer such requests.

Limit targeting methods to the minimum. Regulators should limit the targeting methods that online platforms make available. Targeting methods based on behavioural data, both observed (e.g. what sort of content users like and share) or inferred data (assumptions that algorithms make about users' preferences based on their online activity) should be fully prohibited. It is only legitimate if the data subject consents to use these data sets for targeting. This limitation of targeting criteria would reduce the possibility that political actors tailor different messages to

[2] The Danish Institute for Human Rights, https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox, August 25, 2020

different groups of people and manipulate or even mislead the electorate. Instead, we believe that non-surveillance methods such as contextual advertising[3] offer the best way forward.

For more information, please contact:

Eliska Pirkova, Access Now, *eliska@accessnow.org*

Eva Simon, Civil Liberties Union for Europe, *eva.simon@liberties.eu*

Diego Naranjo, European Digital Rights, *diego.naranjo@edri.org*

[3] Ryan, J. "(Six Months of Data): lessons for growing publisher revenue by removing 3rd party tracking" Brave, https://brave.com/publisher-3rd-party-tracking/, July 24, 2020.