

The Consumer Voice in Europe

THE MANIPULATED CONSUMER, THE VULNERABLE CITIZEN

BEUC's response to European Democracy Action Plan



Contact: Kasper Drazewski – consumer.rights@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND

Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2020-075 - 26/08/2020

Why it matters to consumers

Research shows how every aspect of consumers' online behaviour is being recorded and turned into profiling data. This data is then auctioned and used for behavioural manipulation based on real-time information about our preferences but also our fears, anxieties and emotional vulnerabilities. The resulting insights are then used to capture attention by adjusting what we see online, be it product information or news content.

In the digitalized world, the roles of consumers and of citizens as actors in society are increasingly blurred. Protecting democracy must therefore include protecting consumers against behavioural exploitation. Therefore, the EC's democracy Action plan matters to both consumers and citizens and this is why BEUC responds to this consultation.

Summary

BEUC welcomes the European Democracy Action Plan as a valid and necessary step towards addressing the threats against modern democracies. However, its assumption of an informed and rational citizen does not seem to sufficiently address the problems created by the online behavioural surveillance industry, feeding on data harvested on a massive scale from citizens in the online environment. Recent research demonstrates the mechanics of identifying and exploiting vulnerabilities of content recipients both in the traditional sense of personal characteristics and in a much broader understanding, taking into account situational vulnerabilities which render each individual susceptible to manipulation by way of anxiety and emotional choices. These practices seem to put in question the efficiency of the adopted model if not backed up by regulatory protection against business models built on the exploitative use of behavioural data.

BEUC recommends that the European Democracy Action Plan must be backed by a robust framework protecting citizens from business practices involving collection and use of data in ways which currently evade the protection framework afforded by the GDPR. A holistic approach is needed and should comprise, inter alia, strict enforcement of the GDPR, the adoption of a strong ePrivacy regulation and measures to fight disinformation at its source, including a competition law sector inquiry into the links between the advertising revenue of platforms and the dissemination of disinformation.

1. Context and summary of the Roadmap

The initiative presented in the Roadmap to the European Democracy Action Plan (**'Roadmap'**) seeks to address the distortions of public debate, erosion of trust in governments and media, which have all gained further momentum on account of the COVID-19 crisis. Aligning with already existing forms of distortion affecting the public debate, tidal waves of disinformation and misinformation, in part instigated by non-EU actors, contributed to a chaotic information landscape and demonstrated the potential for further damaging meaningful participation in democratic debate.

The Roadmap tackles areas crucial to modern democracies which were already in need of attention before the COVID-19 crisis. These include the information landscape, media freedom and pluralism, election integrity, civil society, as well as the international and hybrid nature of interference in European democratic systems. Seeking to protect the values enshrined in Article 2 TFEU and the Charter of Fundamental Rights, the Roadmap outlines a range of potential remedies. Chief among those are:

- increased transparency (including disclosure of sponsored content in the political context and financing rules of European political parties);
- capacity building and support of democratic infrastructures;
- support to education of active and aware citizens, including by promoting media literacy;
- increased protection of free media and media pluralism;
- taking action against hate speech;
- assessing and enhancing EU's capacity in detecting and exposing disinformation and other manipulations.

2. BEUC's response

All points made in the Roadmap are commendable in seeking to address the ongoing threats to European democracy by strengthening the position of citizens and enhancing their toolkit in dealing with disinformation and manipulative information practices, showing great care in handling issues which could otherwise lead to restrictions on the democratic process. The proposed safeguards in the context of political transparency, particularly in regard to politically sponsored content and the funding and sponsorship of political parties must also be seen as a necessary step towards increasing the robustness of the modern society and its democratic governance.

However, the main strength of the proposed approach appears to also be the root of a certain weakness. By reiterating the perennial paradigm of **information as the key tool of protection**, the onus is placed on citizens to be the **main line of defense** against the dangers to modern democracies. This builds on the assumption that the citizen, once handed the right tools (such as education, critical thinking capacity and unrestricted access to information) should be **expected to make rational choices** regardless of the circumstances, with no emotionally driven behavioural biases getting in the way.

What this approach does not take into consideration is the **nature of the threats** faced by modern citizens as they deal with information provided through Internet platforms and collaborating media. These are outlined below.

a) To websites and online platforms, content is product and the citizen is a consumer.

It is true that modern-day content recommendation systems vary greatly in their levels of sophistication and empirical studies have shown that quality recommender algorithm can ensure a diversity of outlooks that is greater than that provided by a human editor.¹ However, as websites are generally driven by profit from digital advertising, the least sophisticated algorithms prioritising simple maximisation of click-through rates can reasonably be expected to always remain the most accessible and attractive viral content will remain popular irrespective of its objective quality. As a result, platforms featuring content from websites which spread disinformation have little economic incentive to transition to a more pluralistic content selection model.

¹ Judith Möller, Damian Trilling, Natali Helberger & Bram van Es (2018) Do not blame it on the algorithm: an empirical assessment of multiple recommender systems and their impact on content diversity, *Information, Communication & Society*, 21:7, 959-977, DOI: [10.1080/1369118X.2018.1444076](https://doi.org/10.1080/1369118X.2018.1444076)

b) Consumer behavioural data is the lifeblood of business models designed for manipulation of choice.

Recent reports from regulators and NGOs² have demonstrated both the scale and implications of collection and use of behavioural data from consumers using online services and connected devices. This data is aggregated and used to build personality profiles allowing to identify habits, interests and weaknesses of each user, which are updated in real time and used for a range of purposes, ranging from maximisation of returns on advertising to **predictive analysis of behaviour** and **real-time behavioural modification experiments** with instant feedback. Recent changes in the adtech market, including Google's decision to phase out third-party cookies and federate processing, suggest that the consumers will continue to be faced with increasingly sophisticated and intransparent systems aimed at perfecting intelligent behavioural analysis and influence. Such business practices have as of yet remained largely unaffected by the introduction of the General Data Protection Regulation.

c) The citizens' susceptibility to certain themes and emotional vulnerability can be measured and exploited at any given time.

Thanks to availability of real-time **behavioural surveillance** data, such content can be prioritised that evokes a strong emotional response and then can be targeted to audiences which are the most susceptible to such stimuli at the given time.³ Such data is automatically harvested and exchanged between adtech companies to maximise click-through rates with **no regulatory protection** as to how it is used to prioritise and target content displayed to each user. It is important to note that such business practices are not necessarily a sign of influence by foreign actors as they can also be explained by plain maximisation of profits. This does not leave even the stronger market players unaffected⁴ even though these can be pressured by shareholders and public opinion to actively intervene in the content personalisation results that they offer.⁵ However, most recent research points out that, despite these actions, the very nature of how content is recommended means that e.g. users profiled as interested in conspiracies will still experience YouTube as a filter bubble, with all its consequences.⁶

d) Populist narratives feed on emotional sensitivities and rejection of the incumbents, thus undermining the information and disclosure paradigm.

The assumption that a citizen will make rational choices once equipped with access to knowledge and the skills for critical assessment may fail where this citizen is targeted with an emotionally charged message, selected on the basis of **behavioural data** harvested

² Norwegian Consumer Council, Out of Control, launched January 14th 2020, <https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/>; UK Information Commissioner Office, Update report into adtech and real time bidding, 20 June 2019 <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>; UK Competition and Markets Authority, Online platforms and digital advertising, 1 July 2020 https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

³ Think with Google, The Basics of Micro-Moments, <https://www.thinkwithgoogle.com/marketing-resources/micro-moments/micro-moments-understand-new-consumer-behavior/>.

⁴ See e.g. Jack Nicas, How YouTube Drives People to the Internet's Darkest Corner, Wall Street Journal, Feb 7, 2018 <https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478>; Andy Meek, Siri loves spreading conspiracy theories, New York Post Sep 26, 2018 <https://nypost.com/2018/09/26/siri-loves-spreading-conspiracy-theories/>; Jon Porter, Safari's suggested search results have been promoting conspiracies, lies, and misinformation, The Verge Sep 26, 2018, <https://www.theverge.com/2018/9/26/17904826/safari-siri-suggested-results-conspiracy-theory-pizzagate-holocaust-denial>

⁵ Charlotte Jee, YouTube has nearly halved the number of conspiracy theory videos it recommends, MIT Tech Review, <https://www.technologyreview.com/2020/03/03/905565/youtube-halved-conspiracy-theory-videos-recommends/>

⁶ Marc Faddoul, Guillaume Chaslot, Hany Farid, A longitudinal analysis of YouTube's promotion of conspiracy videos, <https://farid.berkeley.edu/downloads/publications/arxiv20.pdf>

earlier, **delivered in a moment of susceptibility** (a 'micro-moment', in Google's own terminology)⁷. If this message is internalised, counterbalancing false information by supporting fact-checkers making real information available (such as via the portal Euvdisinfo.eu) may not be sufficient as the foundation of many partisan narratives lies the rejection of the mainstream media narratives along with the legitimacy of the incumbent political elites.⁸ In this context, merely enforcing disclosure of sources of funding as proposed by the Roadmap is likely to be insufficient. This is due to a phenomenon which consumer law scholars refer to as the '**disengaged consumer**' where the consumer assumes that all providers apply abusive practices in one way or another and chooses not to be concerned by them.⁹ Similarly in this case, it would be easy to adopt the stance that 'all information is paid for by someone' leading to a similarly apathetic response, thus rendering the approach ineffective.

e) Information does not equal knowledge.

As demonstrated in the area of data protection following the introduction of the GDPR, simply providing detailed information does not lead to the data subjects making informed privacy decisions, particularly under the conditions of a market dominated by one or two large service providers, often using privacy-friendly language in their frontend communications. This is due to a number of factors, from plain cognitive limitations, to cognitive biases and the lack of time to read, analyze and memorize relevant information. In the context of safeguarding the democratic process, this points to another weakness of offering access to impartial and relevant information as remedy to a manipulative and distorted message: just as privacy friendliness PR campaigns carried out by tech companies are likely to disincentivise users from diving too deep into their obscure privacy policy and settings, to a news-reading citizen, when faced with a simple and attractively framed partisan narrative, the true explanation to the given phenomenon will likely require more time to analyze and more effort to dissect, even assuming that the citizen is still willing to explore both sides of the coin after having been exposed to the partisan message. Therefore, the damage done by partisan content which has been intelligently selected and delivered is unlikely to be remedied by simply providing access to factually correct information.

3. BEUC's recommendations

The problems outlined in this document must be seen as interlinking three areas of EU law:

- a) consumer protection, due to being rooted in the consumer-trader relationship;
- b) data protection, in view of being based on privacy-invasive business practices;
- c) competition law, given the limitation of choice in a market dominated by a small number of large Internet companies.

To account for the aspects of digital vulnerability of citizens subjected to business practices built on surveillance, data harvesting and behavioural manipulation, the framework proposed in the Roadmap should be complemented by a robust toolkit aimed at prevention of such practices. Due to the interdisciplinary nature of the issue, a holistic approach is in order if the aim is to safeguard our democracy against manipulation built on exploitative use of consumer data. This approach should include, inter alia, guaranteeing a strict enforcement of the GDPR and the adoption of a strong ePrivacy Regulation. It should also promote measures to fight disinformation at its source, including a sector inquiry to investigate the link between advertising revenue policies of platforms and dissemination of disinformation.

⁷ *The basics of micro-moments*, supra note 3.

⁸ Enrique Peruzzotti, Laclau's theory of populism, (in:) Carlos de la Torre (ed) *Routledge Handbook of Global Populism 2018*, 10.4324/9781315226446.

⁹ Siciliani, Paolo & Riefa, Christine & Gamper, Harriet. (2019). *Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement and Policy Making*. 10.5040/9781509916887.



This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.