International Journal of Social Sciences
Caucasus International University
Volume 1, Issue 1

Journal homepage: http://journal.ciu.edu.ge/

კავკასიის საერთაშორისო უნივერსიტეტი
CAUCASUS INTERNATIONAL UNIVERSITY

INTERNATIONAL JOURNAL OF SOCIAL SCIENCES

საერთაშორისო ჟურნალი სოციალურ მეცნიერებებში

e-ISSN: 2720-8036

Conference proceedings - "Regulating Online Disinformation: Comparative Perspectives," organised by Caucasus International University and Dublin City University, held via platform Zoom on October 1, 2021.

Regulating Online Disinformation:
Reacting to digital problems or building a better Internet?

Dr. Eileen Culloty [a][1][2]

[a]n Institute for Future Media, Democracy and Society
Dublin City University (Ireland)

ABSTRACT

Focusing on the EU Code of Practice on Disinformation, this paper argues that European debates about regulating online disinformation need to be set against a broader perspective on regulating the digital environment as public infrastructure. Occupying the grey area of legal but "harmful" content, disinformation is challenging to define, poorly understood, constantly evolving, and entangled in the fundamental right to freedom of expression. Self-regulatory mechanisms to increase the accountability of digital platforms, such as the EU Code, have repeatedly failed to address these core issues. Moreover, there is little evidence to suggest that the co-regulatory framework envisaged by the EU's Digital Services Act will improve this situation. After reviewing these failures and weaknesses, this paper will suggest that policymakers can achieve better civic and democratic outcomes by focusing - not on a minority of large platforms and the content they host - but on regulating the digital environment as a public infrastructure through, for example, robust competition, data portability, and interoperability rules. Such actions have the potential to break the dominance of Big Tech while incentivising better and new services for citizens.

Keywords: *disinformation; EU; harmful content; digital platforms; co-regulation.*

1. Introduction

The COVID-19 pandemic heightened the sense of crisis surrounding online disinformation. Developing effective countermeasures for online disinformation is widely recognised to be an urgent

[1] Eileen.culloty@dcu.ie

[2] https://doi.org/10.55367/PXGB6863

goal, but it is also a challenging one. First, definitions of the problem vary considerably, and the boundaries between disinformation, opinion, and other kinds of problem content are often unclear. In many cases, the distinction between disinformation and ideological opinion may be hard to define because "political truth is never neutral, objective or absolute" (Coleman 2018:157). Second, there are practical impediments to developing fair and consistent moderation principles for enormous volumes of online content (Banchik 2020).

Moreover, communication technologies constantly evolve, and disinformation actors react to countermeasures by adapting their tactics and strategies. Third, there are significant concerns about the legal, ethical, and democratic implications of restricting free expression and granting platforms an (unaccountable) power to determine what is acceptable (Gillespie 2018). Fourth, and perhaps most crucially, there are major gaps in our understanding of online disinformation due, in part, to the nascency of the research area and, in large part, to the fact that platforms' have generally declined to provide relevant data to independent researchers (Culloty and Suiter 2021). As a result, there is broad agreement that disinformation countermeasures are necessary, but there is far less clarity about what can and should be done.

For their part, online platforms' have pursued ad hoc policies, but there is minimal oversight to ascertain whether those policies are effective or fair (Gillespie 2018; Gorwa, Binns, and Katzenbach 2020). Meanwhile, debates about policy responses to disinformation tend to be framed as a conflict between freedom of expression and authoritarianism. To be sure, authoritarian states and democratic states that are 'backsliding' into authoritarianism are exploiting disinformation concerns to silence critics and increase their control over the information environment (see Funke and Flamini 2021 for an overview of actions). In this context, many scholars and stakeholders have argued that democratic states should concentrate on capacity building initiatives - such as increasing support for media literacy and fact-checking - to increase citizens' resilience to disinformation while collaborating with online platforms through self-regulatory or co-regulatory mechanisms (HLEG 2018; Marsden and Meyer 2019).

In the EU, disinformation is not illegal, but it is recognised as a potential threat to democracy and the health and security of EU citizens (EC 2018a). In many respects, the EU's evolving position on disinformation may be understood as a reaction to a series of crises: from the Russian-Ukrainian conflict through fears of election interference to recent concerns about the public health implications of COVID-19 and vaccine disinformation. However, there is also a clear recognition that disinformation is symptomatic of wider societal issues, including "economic insecurity, rising extremism, and cultural shifts [that] generate anxiety and provide a breeding ground for disinformation campaigns to foster societal tensions, polarisation, and distrust" (EC 2018a: 4). To address this, the 2018 Action Plan against Disinformation aimed to reinforce EU-wide capabilities in four key areas: improving disinformation detection, coordinating responses by member states, cooperating with platforms, and empowering EU citizens (EC 2018b). Despite these ambitious goals, a review by the European Court of Auditors concluded that "a piecemeal monitoring and reporting framework and the lack of long-term funding undermine the EU action plan's accountability" (ECA 2021:15). As outlined below, establishing mechanisms is insufficient without also ensuring well-resourced structures are in place to monitor the implementation of those mechanisms.

This paper is specifically concerned with the EU’s self-regulatory mechanism for holding online platforms accountable: the EU Code of Practice on Disinformation. Focusing on original data about the COVID-19 monitoring program established under the Code, it aims to highlight the failures and weaknesses of the EU's current approach. This narrow and ineffective approach to the disinformation problem is then contrasted with the potential benefits of regulating the digital environment as public infrastructure.

2. The EU Code of Practice on Disinformation

The Code of Practice on Disinformation was established in 2018 as an accountability mechanism for major digital intermediaries[3] and online advertisers (EC 2018c). It emerged from the recommendations of a High-Level Expert Group on Fake News and Disinformation (HLEG 2018) and the Sounding Board of a Multistakeholder Forum on Disinformation. However, the Sounding Board heavily criticised the structure of the Code for having "no common approach, no meaningful commitments, no measurable objectives or KPIs, no compliance or enforcement tools and hence no possibility to monitor the implementation process" (Sounding Board 2018). To a large extent, these early criticisms have been borne out by successive evaluations of the Code's implementation (Culloty et al. 2021; EC 2020b; ERGA 2020).

The European Regulators Group for Audiovisual Media Services (ERGA) was tasked with evaluating the implementation of the Code for the European Commission. However, monitoring digital platforms was a new departure for ERGA and the national broadcasting regulators it represents. Many national regulators lack the resources and capacity to carry out a review of the Code's implementation, and only a few countries have contributed to the assessment reports.

Adopted ahead of the 2019 European Parliament elections, the Code's platform signatories originally agreed to implement measures to disrupt advertising revenues for disinformation, address the prevalence of fake accounts, and make political advertising more transparent, among other areas. Subsequent assessment reports criticised the platforms' ambiguous definitions of political advertising and found their efforts to increase advertising transparency to be underdeveloped, incomplete, and bug-ridden (ERGA 2020; Kirk et al. 2019). A 2020 review by the European Commission concluded that while the Code was successful in establishing "a common framework to tackle disinformation", there were significant shortcomings regarding compliance and a lack of clarity around the scope and the definition of key concepts (EC 2020a). It recommended that self-regulation should be replaced with co-regulation along with sanctions and redress mechanisms to ensure compliance.

These criticisms intensified during the COVID-19 crisis. In June 2020, the EU called on the six platform signatories of the Code to participate in a special monitoring program for COVID-19 disinformation (EC 2020b). Platforms were asked to report on their policies and actions in relation to promoting authoritative content at the EU and Member State level; improving users' awareness; manipulative behaviour; advertising linked to COVID-19 disinformation; and cooperation with fact-checkers. In anticipation of the roll-out of vaccination programs, the platforms were subsequently asked to provide information on actions taken to combat false information about vaccines. In all these

[3] Initial signatories included Facebook, Google, Mozilla, and Twitter. Microsoft joined in May 2019, TikTok joined in June 2020

areas, they were specifically asked to provide data about the EU and at a Member State level. The monitoring program began in August 2020, with platforms submitting monthly reports outlining their actions in the above areas.

Concurrent with this, the Commission was overhauling the 2000 E-Commerce Directive with a new Digital Services Act, which threatened to introduce new rules for digital platforms. In addition, the Commission issued guidance on revising the Code of Practice in light of evident shortcomings (EC 2021). Consequently, one might expect that platforms had a vested interest in participating in the COVID-19 disinformation monitoring program in good faith and in fear of tougher regulation coming down the line.

In May 2021, ERGA published an interim report, which found that the platforms had intensified their efforts to counter COVID-19 disinformation and had provided a useful overview of their actions in the transparency reports. However, ERGA observed that the reported actions could not be verified at the country level and that the absence of country-specific data impeded efforts to monitor and assess the effectiveness of the reported actions. ERGA had separately asked the platforms to provide country-specific and disaggregated data. Although the platforms did provide additional context for the transparency reports, the information provided fell short of what was requested.

The Broadcasting Authority of Ireland (BAI) was one of the ten national regulators participating in ERGA's wider evaluation of the COVID-19 monitoring program. It commissioned the Institute for Future Media, Democracy and Society at Dublin City University (DCU FuJo) to undertake research on the platforms' transparency reports. This appears to be the only systematic effort to assess the program by a national authority, which points to an inherent weakness in the oversight role ascribed to ERGA and the national audio-visual regulators. The following section summarises the key findings and recommendations identified in the DCU FuJo report.

3. Assessing the COVID-19 monitoring program

The DCU FuJo report was based on four components. First, the researchers manually coded 47 reports submitted by Facebook, Google, Microsoft, Mozilla, TikTok, and Twitter between August 2020 and April 2021[4]. The manual coding identified the individual actions reported by each platform and any associated information provided about those actions. Second, an automated analysis was conducted to assess broad trends in each platforms' style of reporting, including overall relevance and levels of repetition. Third, the researchers undertook a case study of platforms' reporting on the use of AI and automation. Fourth, to verify whether the reported actions were implemented, the researchers undertook a detailed case study of Facebook in cooperation with the Institute for Strategic Dialogue and a smaller case study of TikTok.

In summary, 1114 individual actions were identified. Only 351 or 32% of these were new actions; the remainder were continuations of existing actions. A quarter of all actions focussed on the promotion of authoritative content, such as providing links to information by the WHO or national

[4] In this period, Facebook, Google, Microsoft, TikTok, and Twitter submitted nine reports each, while Mozilla submitted just two. Mozilla does not operate a social media platform and has a substantially different operation from the other signatories.

health authorities. The next most common action areas were advertising responses (17%) and blocking, removing or demoting content (13%). In some cases, the reported actions were unrelated to COVID-19 or disinformation. More than a quarter of the actions reported by Facebook and by Twitter were deemed irrelevant to the Code. For example, such actions included the provision of marketing workshops to support start-ups during the pandemic.

The Commission specifically requested information relevant to the EU and its Member States. However, it was often difficult to discern which regions were covered by the reported actions. Sometimes, no specific region was mentioned, or geographic reach was vaguely defined as "available in 32 countries". As a result, the regional application was unclear or unstated for 40 percent of actions. The regional application was unclear for the majority of actions reported by Twitter (70%), Facebook (67%) and TikTok (51%). Only 34 percent of all actions were clearly stated to apply to all EU Member States.

Only 32 percent of the 1114 actions were reported with any outcomes or data. When signatories did report actions with outcomes, EU data was often not included or presented in vague aggregates. Only Google, Microsoft, and Mozilla reported any action with a full breakdown by the Member States, but the overall numbers were very low: 16 actions in total.

The case study of Facebook focused on Irish Pages and Groups known to propagate Covid-19 vaccine disinformation. There were numerous inconsistencies in the application of factchecks. In some cases, factchecks were available but were not applied, or they were not applied consistently across different content formats. Sometimes factchecks were applied to posts, but not to the same false claims appearing in the comments associated with those posts. Finally, Facebook’s decision not to factcheck political actors allowed disinformation to be posted unchecked. Similar inconsistencies were evident in the application of content labels and the application of content removals policies. The case study of TikTok found similar inconsistencies in the application of content labels. Overall, 43 percent of TikTok’s reported actions were about the promotion of authoritative content. However, the top results for “vaccine” and “vaccination” returned disinformation content, and the majority of the top 20 posts available under the hashtags #covid, #vaccine and #vaxx were not labelled as stated in the reports. These inconsistencies, coupled with a lack of information about the use of AI and automated systems, suggest that the platforms' technological systems are not as effective as they claim. Importantly, the case studies were conducted on English-language content, and automated systems tend to be more developed for English, which raises questions about capabilities for other EU languages. The overall conclusions regarding the operation of the Code are summarised in the following paragraphs.

***A lack of standardised reporting*:** In the absence of a standardised reporting format, each platform reported in an idiosyncratic manner. Although some variance is to be expected given the differences in the services offered, the current reporting mechanism is not conducive to an assessment of the platform's actions. Considerable effort was required to extract a clear picture of what actions were undertaken, how those actions related to the platform's policies, whether those actions were new, and whether they were relevant to the Code and EU Member States. In particular, the free-text nature of the reports afforded platforms the opportunity to produce repetitive and irrelevant information. Notably, some signatories copied company press releases and self-promotional announcements without any effort to tailor the information for the Code or the EU.

Regarding the transparency reporting envisaged in the Digital Services Act, Dot Europe, the lobby group representing tech companies, cautions that: "there is no “magic button” which will enable a service provider of any size to automatically pull and deliver the data in the right structure and format of a transparency report" (Dot Europe 2021:15). Nevertheless, a certain level of standardisation is necessary to ensure relevant information is provided and in a manner that facilitates monitoring.

A lack of clarity surrounding policies and definitions*:* It is often difficult to discern how the reported actions relate to a platform’s policies, whether those policies relate to disinformation per se, and whether those policies apply across all EU Member States. In addition, generic terms, such as "content' and "label", are often cited but without clarification about what is included and excluded. For example, many signatories apply content labels, but there are important differences between the application of generic labels (e.g. read the facts about COVID-19 vaccines) and the application of specific labels to pieces of content (e.g. this claim has been rated false). Similarly, when a platform’s service facilitates multiple content types (e.g. posts, comments), the term ‘content’ needs to be clearly defined to indicate what is included and what is excluded from a policy or action. To facilitate monitoring, platforms need to provide clear definitions of relevant policies to combat disinformation, clear definitions of common terms, and how those terms are operationalised on their services.

A gap in addressing user comments**:** User comments have been overlooked as a source of disinformation. The Code asked signatories to address content “in search, feeds, or other automatically ranked distribution channels.” Platform policies typically prioritise posts rather than the comments that accompany them. Moreover, factcheckers concentrate their limited resources on posts as the potential reach of comments is much lower than the potential reach of posts. However, the case studies of Facebook and TikTok found that user comments facilitated the fermentation of harmful disinformation. The inattention to comments also created notable contradictions whereby disinformation claims that appeared in posts were labelled, factchecked or removed, but the same claims appearing in the accompanying comments were not. On Facebook, Page and Group administrators are tasked with exercising oversight over user comments. However, there is an obvious contradiction in the expectation that the administrators of disinformation Pages and Groups will take responsibility for the veracity of user comments.

To address these issues, platforms and relevant stakeholders should introduce a framework to address disinformation in comments that is consistent with Article 10 of the European Convention on Human Rights and the principle of freedom of opinion. For example, a mechanism to address hateful and inappropriate comments has been introduced by some platforms[5][6] whereby users are prompted to re-evaluate their comment based on its potentially harmful nature or, alternatively, such comments are hidden or filtered.

A lack of granular data**:** In many instances, the reported data was aggregated at the global level. When EU data was provided, it was frequently presented in aggregate, which is of little use when assessing implementation across the EU Member States. Moreover, the current reporting format allows platforms to report broad data that may or may not be relevant. For example, some platforms

[5] https://blog.twitter.com/en_us/topics/product/2021/tweeting-with-consideration

[6] https://support.tiktok.com/en/using-tiktok/messaging-and-notifications/comments

reported metrics about hate speech violations without clarifying how many, if any, of those violations were related to COVID-19 or COVID-19 disinformation. Expanding on Article 23(2) of the Digital Services Act, which requires more detailed data regarding platforms' active users, clear parameters need to be defined for the reporting of granular data about specific action areas and in relation to the EU Member States.

***A lack of meaningful KPIs*:** When platforms did provide data, it tended to be in the form of engagement metrics. However, these metrics rarely provide much insight into the effectiveness of an action. There are two dimensions to this problem: First, the reported engagement metrics are often too broad. For example, when reporting on a media literacy campaign, platforms typically report the number of people who clicked on the campaign link. As it seems likely that many people will click on a link by mistake and decline to engage with the content, more meaningful metrics would provide information about how many people remained on the campaign page and the time spent on the page relative to the volume of content. Second, engagement metrics reveal little about the effectiveness of the action in terms of combating disinformation. For example, to understand the effectiveness of actions such as media literacy campaigns, it would be instructive to know whether those who engaged with a campaign were less likely to engage with disinformation as a result. To address this, meaningful KPIs are required for the reporting of results and outcomes in relation to key areas, including content labels, content and account removals, factchecking, and media literacy campaigns. Moreover, platforms should report on their own efforts to measure the efficacy of these actions and provide data to independent researchers to verify that efficacy.

A lack of expert oversight: In the 2018 Code, platforms committed "to select an objective 3rd party organisation" to review the self-assessment reports and to evaluate progress, "which would include accounting for commitments" platforms agreed to under the Code. However, this commitment was not implemented. The lack of a well-resourced and independent auditor to review the quality of what has been reported is a significant weakness. Current and proposed oversight structures - ERGA and the European Digital Media Observatory (EDMO) - appear inadequate to address this gap and the needs of ongoing monitoring. For example, the DCU FuJo research required considerable resources in terms of funding, personnel, and time and it relied on the research infrastructure of an academic institute. The original commitment to an independent auditor should be implemented under the revised Code. Further, we recommend that signatories provide adequate funding and resources to support this position, which will contribute to the monitoring work of ERGA and EDMO.

A lack of verification: The case studies of Facebook and TikTok indicated that the reported actions were not applied consistently. The reporting of engagement metrics - when they are made available - does not address this issue. For example, providing country-level metrics about content removals or engagement with COVID-19 information centres does not provide any indication about whether those actions were applied consistently and appropriately. Consequently, there is a major gap in the monitoring of the Code as it assesses what actions the signatories have reported without the certainty that those actions have been implemented across the EU Member States and are working as stated. Standardised procedures are needed to verify the implementation of actions. This will ensure consistency in monitoring and provide an important counterpoint to the signatories' reported metrics.

***A lack of information about automated systems*:** The platforms' reports provided only limited insight into the use of AI and automated systems to combat disinformation. Yet, many of the reported actions, such as the application of generic content labels, presumably rely on automated systems. In some instances, signatories may be using AI to identify harmful content. In other instances, they may be using automated tools to match policy-violating content against a blacklist of known instances. Consequently, it is important to discern how automated systems are deployed against disinformation and what datasets are used to develop these systems. As AI solutions are typically not equally advanced in all the languages of the EU, there may be regional gaps in the application of actions. Moreover, given major concerns about the transparency of automated content moderation and the potential implications for freedom of expression, the need for risk assessments should be stipulated in the revised Code.

***A lack of research data*:** The European Commission has acknowledged the need for greater access to data that will allow independent researchers to better understand the role platforms play in various domains, including disinformation. The Digital Services Act introduces obligations for platforms to make data available to "vetted researchers" and this provision is echoed in the Guidance on Strengthening the Code. Some social media platforms have made access to their data available either through APIs (e.g. Twitter) or through curated services (e.g. Facebook's CrowdTangle). While the former certainly affords greater opportunities for analysis, the latter is also welcome for its ease of use and more accessibility. However, platforms should not be left to decide the criteria for accessing data nor their format, as evidenced by Facebook's recent decision to block a team of New York University researchers studying disinformation from accessing its services (Bond 2021). To address this, the Commission should create a clear regulatory framework for accessing data for research on disinformation and further expand the scope of its current proposal to include more stakeholders, including members of civil society organisations, rather than just university-affiliated researchers.

4. Conclusion: beyond co-regulation

In popular discussions, there are wide-ranging calls to regulate online platforms. What people want from regulation and what it would mean in practice often remains unelaborated. Many scholarly and NGO calls for regulation are underpinned by ideas about protecting democracy and human rights and serving the public interest (Jørgensen 2019). The current European Commission, which will serve until 2024, has outlined three priorities in this area: strengthening media freedom, making platforms more accountable, and protecting the democratic process (Stolton and Makszimov 2020). A major component of this is the Digital Services Act, which will mark a significant shift from a self-regulatory framework towards a co-regulatory one. The Act aims to improve incentives for addressing illegal and harmful content, including disinformation, by harmonising oversight mechanisms and introducing due diligence obligations and risk assessments for "very large online platforms."[7]. However, the experience of the Code of Practice has shown that some very large platforms have not participated in good faith even with the threat of stricter enforcement rules.

If policymakers aim to reduce harm to citizens and mitigate threats to democracy, it may be more beneficial to rethink how the online environment operates as public infrastructure (Rahman 2018).

[7] Defined as services reaching 45 million active monthly users in the EU or 10% of the EU population.

The advent of the internet was widely welcomed as a democratising force that greatly expanded access to information and freedom of expression. Led by the US, democratic states championed a global internet and advocated lax regulation to allow online companies to flourish. Internet governance was largely conceived in terms of managing technical standards, while online companies were treated as neutral platforms and exempt from liability for the content they hosted. In the early 1990s, few could have anticipated how online technologies would evolve, but the expectation that public goods and democratic values would follow from digital innovation proved to be a delusion with significant consequences (Morozov 2011).

Far from the vision of a 'free and open internet' (Clinton 2011), the online world is dominated by a small group of companies, including Amazon, Google, and Facebook. While these companies began with a niche focus - online shopping, web search, social networking - they have grown into vast infrastructures upon which entire sectors of social and economic life are dependent (Plantin and Punathambekar 2019). Part of their power lies in their ‘intermediation bias’ whereby platform algorithms influence the content people see and are likely to engage with (Calvano and Polo 2020). Consequently, as traditional industries moved online, their business models were subsumed by the platforms’ model of ‘surveillance capitalism’ (Zuboff 2019). Within this model, internet users are offered free access to content while platforms accumulate users' personal data, often without their knowledge, and generate revenue through personalised advertising and other data-based services.

In addition to taking on "the characteristics of infrastructure," online platforms also exhibit strong network effects that reinforce their dominance (Rahman 2018:240). Competition and consumer protection authorities have struggled to keep pace with these developments (Wu 2017). The platforms have been given free rein to buy-up competitors and new entrants to the market. For example, Google has acquired more than 230 companies, including YouTube, while Facebook has acquired more than 80 companies, including Instagram (Lemoine 2020). Viewed from the lens of surveillance capitalism, disinformation and related problems cannot be isolated from the platforms' wider system of data harvesting, targeted advertising, 'attention brokerage,' and anti-competitive acquisitions (Wu 2017).

With an ability to manipulate the flow of information and with entire sectors, such as the news industry, heavily dependent on platforms, it is clear that platforms do not “play a neutral, merely technical and passive role towards” content, as specified in the EU’s E-Commerce Directive from 2000. Yet, they continue to be regulated as though they are neutral services. Notably, in updating the E-Commerce Directive, the EU’s Digital Services Act did not reverse the platforms’ exemption from content liability.

In this context, proposals to impose greater accountability mechanisms - around algorithms, risk assessments, automated systems, and related areas - on existing platforms appear weak. Not only do these actions fail to address the dynamics of the digital environment, they also present core challenges for monitoring capacity. As noted in relation to the Code of Practice, the body charged with monitoring the Code’s implementation generally lacks the capacity to do so. Increasing the transparency requirements placed on platforms will achieve little if the structures and resources needed to provide accountability are not also well established.

A more systematic approach to the problems of the digital environment could address the dynamics of the markets in which platforms operate. For example, policymakers could legislate to encourage innovation and increase competition. By doing so, they would return to the earlier vision of an innovative digital environment. Another advantage of this approach is that regulators are tasked with overseeing the structures of the digital environment rather than engaging in complex and controversial interventions at the level of content. For example, data portability and adversarial interoperability rules could alter the dynamics of the environment.

Data portability allows individuals to obtain their personal data and transfer it elsewhere. A lack of data portability means that new or alternative platforms struggle to compete with the established platforms. When people have accumulated data on one platform for many years, the burden of migrating to a new platform is great because all the data is left behind. Data portability reduces that burden and thereby creates an incentive for new platforms to emerge. A lack of data portability also means individuals are denied the freedom to use and analyse the data that is held about them. For example, the latter would allow people to submit their data to third-party services that investigate how platforms use personal data for microtargeting. The EU's 2018 General Data Privacy Regulation (GDPR) recognises a right to data portability but in a very limited way. This could be strengthened in ways that encourage competition in the market and increase accountability through new third-party services.

Interoperability means a product or service works with existing products or services. Adversarial interoperability allows a new product or service to integrate with an existing service without the permission of that service. It encourages competition and better services for consumers. The dominant online platforms often gained their position through adversarial interoperability, but they now exploit the law to prevent new entrants from doing the same. Both data portability and interoperability must be balanced against a right to privacy and security concerns. In an online context, one person’s personal data may have implications for another person’s privacy. Technology platforms typically oppose both by arguing that it will compromise their users’ privacy and security. These are legitimate but not insurmountable concerns.

Such structural interventions will not have an immediate impact on the flow of disinformation, but if there is no effort to intervene at the structural level, policymakers and the public will continue to be at the mercy of a small group of companies who have come to dominate the online environment. Meanwhile, alternative visions of how to organise digital life and information will struggle to compete. If policymakers truly believe disinformation is public harm and a threat to democracy, regulating the underlying dynamics of the digital environment is a logical step. Of course, any such regulation will face fierce opposition from the tech lobby, which currently outspends the pharmaceutical, fossil fuel, finance, and chemicals industries in EU lobbying spend (Bank et al., 2021). The alternative to infrastructural regulation is to continue on as we are in the hope that the dominant platforms will transform themselves into good faith participants in a co-regulation framework.

References

Banchik AV (2020) Disappearing acts: Content moderation and emergent practices to preserve at-risk human rights-related content. *New Media & Society*: 146144482091272. DOI: 10.1177/1461444820912724.

Bank, M. Duffy, F. Leyendecker, V. and Silva, M. (2021). T*he Lobby network, Big Tech's web of influence in the EU*. Brussels: Corporate Europe Observatory and Lobby Control

Bond, S. (2021) NYU Researchers Were Studying Disinformation On Facebook. The Company Cut Them Off. NPR August 4. Available: https://www.npr.org/2021/08/04/1024791053/facebook-boots-nyu-disinformation-researchers-off-its-platform-and-critics-cry-f?t=1628525534571

Calvano E and Polo M (2020) Market power, competition and innovation in digital markets: A survey. *Information Economics and Policy*: 100853. DOI: 10.1016/j.infoecopol.2020.100853.

Clinton, H. (2011) *Internet Rights and Wrongs: Choices and Challenges in a Networked World*. Washington, DC.

Coleman, S. (2018) The elusiveness of political truth: From the conceit of objectivity

Culloty, E. and Suiter, J. (2021) *Disinformation and Manipulation in Digital Media: Information Pathologies*. Routledge: New York.

Culloty, E., Park, K., Feenane, T., Papaevangelou, C., Conroy, A., and Suiter, J. (2021). CovidCheck: Assessing the Implementation of EU Code of Practice on Disinformation in relation to COVID-19. Dublin: Broadcasting Authority of Ireland.

Dot Europe (2021) DOT Europe Questions and Recommendations on DSA. Available: https://doteurope.eu/library/dot-europe-questions-and-recommendations-on-dsa/

ERGA (2020) *ERGA Report on disinformation: Assessment of the implementation of the Code of Practice*. Brussels: European Regulators Group for Audiovisual Media Services.

ERGA (2021). *Interim Report on Monitoring of the COVID19 Disinformation*. Brussels: European Regulators Group for Audiovisual Media Services.

EU Disinfo Lab (2021) How the Digital Services Act (DSA) Can Tackle Disinformation. April 1. Available: https://www.disinfo.eu/advocacy/how-the-digital-services-act-%28dsa%29-can-tackle-disinformation/

European Commission (2018a) *Tackling Online Disinformation: A European Approach*. COM(2018) 236, 26 April. Brussels: European Commission.

European Commission (2018b) *Action Plan against Disinformation*. Brussels: European Commission.

European Commission (2018c) *EU Code of Practice on Disinformation*. September 26. Brussels: European Commission.

European Commission (2020a) *Assessment of the implementation of the Code of Practice on Disinformation*. May 8. Luxembourg: European Commission.

European Commission (2020b) T*ackling COVID-19 disinformation – Getting the facts right.* Brussels: European Commission.

European Commission (2021) *Guidance on Strengthening the Code of Practice on Disinformation*. May 26. Luxembourg: European Commission.

European Court of Auditors (2021) *Disinformation affecting the EU: tackled but not tamed*. Available: https://www.eca.europa.eu/ga/Pages/DocItem.aspx?did=58682

Funke, D. and Flamini, D. (2021) A guide to anti-misinformation actions around the world. *Poynter*. Available at: https://www.poynter.org/ifcn/anti-misinformation-actions/.

Gorwa, R., Binns, R. and Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1), p.2053951719897945.

High-Level Expert Group on Fake News and Online Disinformation (2018) Report to the European Commission on A Multi-Dimensional Approach to Disinformation, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

Jørgensen, R.F. (ed.) (2019) *Human Rights in the Age of Platforms*. Information policy series. Cambridge, MA: The MIT Press.

Kirk, N., Culloty, E., Casey, E., et al. (2019) *Elect Check: A Report on Political Advertising Online During the 2019 European Election*. Dublin: Broadcasting Authority of Ireland.

Lemoine L (2020) Competition law: Big Tech mergers, a dominance tool. In: *European Digital Rights*. Available at: https://edri.org/competition-law-big-tech-mergers-a-dominance-tool/.

Marsden, C. and Meyer, T., (2019) *Regulating disinformation with artificial intelligence*. European Parliament European Science-Media Hub.

Morozov, E. (2011) *The Net Delusion: The Dark Side of Internet Freedom*. New York, NY: Public Affairs.

Plantin, J. and Punathambekar, A. (2019) Digital media infrastructures: pipes, platforms, and politics. *Media, Culture & Society* 41(2): 163–174.

Rahman, K.S. (2018). Regulating informational infrastructure: Internet platforms as the new public utilities. *Georgetown Law and Technology Review, 2*: 234-251.

Sounding Board on Disinformation (2018) The Sounding Board of The Forum on Disinformation Issues their Unanimous Final Opinion on the So-called Code Of Practice. Available: https://www.aereurope.org/jointpressstatement_soundingboard_disinformation/

Stolton, S. and Makszimov, V. (2020) Platform regulation ‘needed’ as part of Democracy Action Plan, Jourová says. *Euractiv*. Brussels. Available: https://www.euractiv.com/section/digital/news/platform-regulation-needed-as-part-of-democracy-action-plan-jourova-says/.

to intersubjective judgement. *European Journal of Communication* 33 (2): 157-171.

Wu T (2017) Blind spot: The attention economy and the law. *Antitrust Law Journal* 82: 771–806.

Zuboff S (2019) Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum* 28(1): 10–29.