OPEN SOCIETY
FOUNDATIONS

Regulating the Digital Public Sphere

Limits and Opportunities of Market Interventions

Dr. Mathias Vermeulen

June 2021

Table of Contents

224 West 57th Street
New York, NY 10019
P. +1 212-548-0600
opensocietyfoundations.org

About the Author

Dr. Mathias Vermeulen is the Public Policy Director at AWO, a data rights organization with three offices in Europe. The organization is made up of lawyers, policy experts, technology analysts and applied ethicists working at the intersection of technology and human rights.

Dr. Vermeulen oversees is a legal and public policy expert in information technology law, digital rights and emerging technologies, with a focus on EU-law. Dr. Vermeulen previously worked with the Mozilla Foundation, Luminate, the European Parliament, and at the Centre for Law, Science, Technology and Society at Vrije Universiteit Brussel. He has also worked as the main advisor to the UN special Rapporteur on human rights and counterterrorism, Prof. Dr. Martin Scheinin. He holds a Ph.D. in European privacy and data protection law from the Vrije Universiteit Brussel, and has a joint European Masters in Human Rights and Democratization from the European Inter-University Centre in Italy and the University of Hamburg.

1. Foreword

Platforms like Facebook and Google wield more power than most nation states over our public life, but with no genuine accountability. They are society's new operating systems, which profit from amplifying sensationalist content, undermine elections by opaque microtargeting of hateful messages, and eviscerate legitimate sources of news essential to a well-informed citizenry. Platforms are not the source of disinformation and polarization, but in their current incarnation they hugely exacerbate these toxic sides of public discourse. Crucially, the harms are not equally distributed, but instead disproportionally affect vulnerable communities not least because the harms are often directed at them.

The Open Society Foundations is working with partners around the world to re-imagine our digital public sphere to make it work better for open society and our communities. A priority is to bring the powerful platforms back under democratic control and allow digital infrastructures to emerge that again conceive of platforms as public goods, not as purely profit-making ventures.

With the competition workshop series we hosted in February 2021 together with AWO – a data rights agency with offices in London, Brussels and Paris – we wanted to shine a spotlight on the opportunities and limits of different competition law tools to create a more resilient public sphere. This paper is summary of the three workshops and a series of interviews and desktop research conducted by AWO. With major platform regulation planned in different parts of the world, we hope it will contribute to a better understanding of competition tools' impact on our information environment and the trade-offs involved.

Workshop participants concluded that there are a number of speech-related harms for which competition tools are not a sufficient answer. That said, most interventions were seen as strengthening better data governance and contributing to a more diverse ecosystem of platforms. Most importantly, competition law will fail us if it remains focused on the relationship between the dominant market actors and their competitors. Instead, we need policy makers and enforcers to recognize unprecedented political power of platforms and put the interests of users and their communities and questions of media diversity at the center of their action. Some in the competition establishment are starting to do so, but for a paradigm shift we need a more fundamental overhaul.

I want to thank AWO and our 40 participants, which included economists and practicing competition lawyers, information and media scholars, and digital rights advocates and community activists, for dedicating their time and energy to this project. We look forward to continuing this critically important reform effort with you and many others.

Vera Franz
Open Society Foundations
London, June 2021

2. Executive Summary[1]

Several governments increasingly expressed an interest in reining in the market power of a number of large online ad-funded platforms through new legislative frameworks and enforcement actions in 2020. Many of these interventions explicitly aim to weaken the dominant position of these platforms and enable the creation and scaling up of alternatives to the services of the dominant companies. These goals would be achieved on the one hand by limiting the ability for these platforms to excessively collect data, and on the other hand to open up some of the data they currently possess to other market players. While these interventions don't explicitly aim to address immediate 'downstream' societal harms such as increased polarization online or the spreading of disinformation, it is often said that some of these interventions might indirectly have a positive impact on the resilience of the so-called Digital Public Sphere[2].

This paper explores to what extent five often discussed interventions could potentially have such a positive impact on four perceived threats to the Digital Public Sphere[3].

From this exploration it became clear that no policy intervention offers a silver bullet to solve some of these challenges, but instead presents policy makers with a specific set of trade-offs that need to be surfaced in advance.

1 This study is the summary of a series of interviews and desktop research that took place in November 2020 and 3 separate workshops in February and March 2021 that were facilitated by AWO on behalf of OSF. In these workshops 40 participants exchanged thoughts with each other to explore which interventions, if any, would contribute to improve the resilience of the Digital Public Sphere. This paper is not an exhaustive treatise on these topics but rather aims to be an accessible primer for a broader audience, as requested by OSF. The publishing of this report does not mean that AWO is advocating for the conclusions reached or the recommendations within this report but solely is a reflection of the views that were expressed during the workshops.

2 It is important to stress that the results of this exercise were influenced by the starting point of the analysis, which aimed to rethink threats to the Digital Public Sphere as market failures, given that market interventions primarily aim to remedy such failures. This analysis would likely have been different if the end goal would have been to work towards a pre-identified 'ideal' Digital Public Sphere, as opposed to thinking about remedies that address the current harms of our Digital Public Sphere.

3 The geographical scope of this paper was limited at this point in time to the EU and the US, given that some of the most significant market interventions were being contemplated or rolled out in these jurisdictions.

2.1 Regulate platforms as public utilities

The introduction of US-style 'public interest' obligations for Big Tech could translate into a limited positive impact on the Digital Public Sphere by introducing safeguards against non-competitive behavior such as non-discriminatory access, interoperability and fairness. A ban on targeted advertising as part of this approach could attempt to alter the revenue-generating strategy of platforms and remove incentives to harvest data through surveillance.

However, this option could risk imposing an overly rigid and inflexible regulatory regime that may fail to address specific problems related to different platforms, given the diversity and heterogeneity of problems in this space. These shortcomings are often cited in EU policy debates.

2.2 Impose a structural separation of dominant companies ('break them up')

Structural separation can take many forms, but in most cases this approach would seek to correct non-competitive behavior stemming from a concentration of power derived from, for example, misappropriation of data from third parties, leveraging dominance to force favorable terms in business negotiations, creating user lock-in and using excessive profits to subsidize entry into other markets.

In particular, separating platforms' communications networks from their advertising businesses could potentially have a positive impact on the Digital Public Sphere by reducing incentives to amplify and spread content based only on whether it generates attention (and therefore increased advertising revenue), regardless of the impact this content could have on society more broadly. It could also divert more advertising revenues towards publishers and thereby promote media diversity.

However, this approach could lead to trade-offs between providing sufficient incentives for innovation, investment, economic efficiencies and consumer welfare. This approach could also be limited by political motivations and is considered by many to be complex and slow. It remains, however, a viable option to be considered as a last resort when behavioral remedies do not achieve their intended effect.

2.3 Prohibit excessive data collection via third party trackers

Prohibiting excessive data collection via third party trackers could contribute to creating a fairer, less exploitative Digital Public Sphere by protecting users' privacy and reducing incentives for platforms to impose misleading consumer terms that could even be considered as a stand-alone abuse under the heading of unfair trading conditions.

However, limiting the prohibition to third party trackers risks ignoring the increasing movement by some dominant platforms to focus on first party tracking, which could potentially further reduce competition in the online advertising market. At the same time, an outright ban on all types of data collection could limit publishers' ability to generate revenues through other types of advertising e.g. contextual. Overall, most of these options are potentially not future proof enough as they don't remove one of the fundamental problems at stake: platforms' ability to manipulate the public by selecting and amplifying targeted content. In the future, data collection may no longer be the determining factor to grow and reach a dominant position.

2.4 Prohibit dark patterns

Prohibiting dark patterns could reduce the ability of dominant companies to collect more data than a competitive market would allow by deceiving users into sharing more personal information than they intend to, or making it more difficult for them to select more protective privacy options.

However, in order to have an impact, policymakers would need to explore regulatory options which go beyond existing data protection legislation such as addressing dark patterns as unfair commercial practices or banning a specific set of practices by dominant platforms. This would also be relevant to other areas where dark patterns could restrict user action, such as flagging illegal or harmful content, algorithmic transparency, labelling online advertisements or data portability.

2.5 Impose interoperability requirements on dominant companies

Interoperability emerged as a potentially effective tool to overcome the network effects and high switching costs that tend to cement dominant positions in the Digital Public Sphere. This approach could stimulate the production of alternative tools for citizens to connect to these dominant

services, thereby providing users with more choice and control over the information they see and share.

However, this decentralized model could pose governance problems and make it more difficult to moderate or take down content, potentially increasing the proliferation and amplification of harmful content. These challenges could actually lead to a convergence of content moderation standards, ultimately reducing diversity and choice for users. Policymakers will also need to navigate a high level of technical and legal complexity to make this approach workable.

3. The state of the Digital Public Sphere: from the promised wealth of networks to black box societies

At the outset of the project OSF proposed a working definition of a resilient Digital Public Sphere.

Definition: Resilient Digital Public Sphere

In a resilient Digital Public Sphere (1) data is governed responsibly in line with data protection rules, (2) free expression is upheld while fragmentation and polarization of discourse is reduced and (3) disinformation and hate speech are mitigated in a timely and decisive manner. In this Digital Public Sphere, (4) real possibilities for alternative social media networks can emerge in which citizens would have the ability to connect outside the dominant platforms

The notion of a public sphere runs through modern democratic theory as a realm in which public discourse and participation takes place.[4] In its tolerance of opposing views and opinions, its belief in the power of rational argument, free expression and the autonomous individual, it is embedded in our public institutions and in a media that holds power to account.[5]

The digital or 'networked' public sphere is a concept that gained traction after Yochai Benkler published his 'Wealth of Networks' in 2006, which broadly referred to the Digital Public Sphere as the new emerging media landscape that democratized (political) communication and provided new modalities for civic participation and engagement processes.[6] The two fundamental differences with the traditional public sphere that he identified at the time are still relevant today: a networked architecture, and the practical elimination of communications costs. Both differences result in an abundance and diversity of human expression available to anyone, anywhere, in a way that was not feasible in a mass-mediated environment.

4 Habermas, The Structural Transformation of the Public Sphere. MIT Press, 1962.

5 Papacharissi, The virtual sphere. New Media & Society, 2002, 4, pp.9-27.

6 Benkler, The Wealth of Networks. Yale University Press, 2002.

However, this evolution decreased the gatekeeping power of traditional media, which led to fears that this absence, coupled with "information overload", would lead to fragmentation of discourse, polarization, and the loss of political community. These fears were most prominently articulated a decade ago in the US by Cass Sunstein, who predicted the emergence of personalized news feeds and recommendations that would offer "no common ground for political discourse or action, except among groups of highly similar individuals who customize their windows to see similar things".[7] This fragmentation of discourse would lead to polarization in his view since people would cluster into groups of self-reinforcing, self-referential discussion groups, which tend to render their participants' views more extreme and less amenable to the conversation across political divides necessary to achieve reasoned democratic decisions.

Benkler rebutted these critiques in 2006 by comparing the advantages of the Digital Public Sphere not to "a nonexistent ideal public sphere" but to a public sphere that was dominated by mass media. Yet in 2021 the Digital Public Sphere is de facto a privatised public sphere that is dominated by a small number of large online platforms, whose ad-driven business models and infrastructures result in a number of new harms on top of the harms that Sunstein already identified.

Platforms became the de facto gatekeepers of the Digital Public Sphere since they have the ability to shape public debate by elevating and promoting specific pieces of content or authors. This assessment is shared by the European Commission's proposal for a Digital Services Act, which argues that it is necessary to impose specific obligations on 'very large online platforms' given their importance due to their reach, "in particular as expressed in number of recipients of the service, in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas and in influencing how recipients obtain and communicate information online".[8]

These platforms weren't designed as a space for civic discourse, but they are said to be optimized to capture our attention and our personal data in order to increase our engagement with content or users on these platforms. These engagements can subsequently be used to make inferences about individuals and groups, in the form of assumptions or predictions about future behavior[9],

7 Sunstein, *Republic.com*. Princeton University Press, 2001.

8 Proposal for a digital services act, §53 https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN

9 Wachter, Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI,* Columbia Business Law Review, 2019. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

which can be offered as a service to advertisers. Every action we take on these networks results in data that is used to accumulate ever-more-intimate profiles of users, which are then monetized and used to predict human behavior. Pasquale and others have argued that decisions to elevate or promote content are based in particular on "virality metrics", which "promote material that has received a good deal of attention or seems to match a sub-public's personalization profile, regardless of whether it is true or even minimally decent". In his view, this reduces pluralism by

> *elevating profit considerations over the democratizing functions of public discourse, and effectively automating the public sphere. Decisions that once were made by humans with plural aims and aspirations are now made by profit-maximising algorithms, all too prone to self-reinforcing logics of rapid, vapid, viral dissemination.*[10]

The Council of Europe has highlighted how these manipulative techniques and dark patterns can be seen as a threat to the "cognitive sovereignty" and personal autonomy of citizens, since they interfere with the freedom to receive information and the right to privacy. Ultimately these practices, deployed at scale, can undermine the very foundations of democratic orders, since they can distort what is an essential precursor for any form of democratic participation, including voting behavior.[11] A resilient digital sphere then is a sphere which is free of manipulation and which allows us to have meaningful choices to structure our current complex information environment.[12] This means that a certain degree of personalization of our information environment is not inherently bad, but it does mean that the current tracking and optimization tools used by dominant market players require a thorough re-assessment.

Whereas these are necessary improvements to arrive at a more resilient Digital Public Sphere, it needs to be stressed that using this concept results in a specific framing that indirectly creates a priority in the societal harms that

10 Pasquale, The Automated Public Sphere. U of Maryland Legal Studies Research Paper, 2017.

11 Council of Europe at 35 https://rm.coe.int/responsability-and-ai-en/168097d9c5. The Council of Ministers of the Council of the European Union even adopted a declaration on the (manipulative capabilities of algorithmic processes) in which they warn against the risk of using algorithmic processes to manipulate social and political behaviour. https://www.coe.int/en/web/data-protection/-/declaration-by-the-committee-of-ministers-on-the-manipulative-capabilities-of-algorithmic-processes

12 See also Edwin Baker's work on why the structure of media markets is so crucial to preserving democracy. Baker, Media concentration and democracy. Cambridge University Press, 2006.

need to be fixed. The 1960s concept of a public sphere has always been flawed, as it didn't include the perspectives of historically marginalized groups.[13] Access to that public sphere has never been evenly distributed to all citizens, especially in an environment where mass media acted as the main gatekeeper. Some of the harms of our current online media ecosystem are disproportionately experienced by historically marginalized groups, who are the primary targets of online harassment, abuse, and hate speech. A common US perspective which claims that a 'resilient' digital sphere should be characterized by more freedom of speech would not address this particular category of harms, and neither would a traditional European vision of a resilient public sphere, which would predominantly aim to impose limits on how dominant tech companies use data to manipulate our information ecosystem.

13 Fraser "Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy", in Calhoun, Craig (ed.), Habermas and the Public Sphere, Cambridge Mass.: MIT press, 1992, pp. 109–142.

4. Potential market interventions to facilitate a resilient Digital Public Sphere

There is an ongoing political debate in both the EU and the US about the extent to which competition law should be strictly limited to addressing the negative economic impacts of market power or whether it also should pursue a broader range of socio-economic goals beyond market deficiencies and consumer welfare. An increasing range of scholars and activists argue that the goals of competition law should not remain static through time and should be responsive in the face of new business strategies by platforms, new forms of interaction with consumers and the accumulation of data, which increasingly blur the distinction between economic and non-economic interests. Ezrachi points out that in the context of the digital economy, "the value of plurality, democratic values and freedoms may support intervention in cases where firms distort markets, information flows, and subsequently impact on consumers' freedom".[14] Others argue that when competition law is entrusted with the duty to "rein bigness", it is also relevant when bigness is used to corrupt the democratic process or undermine consumer privacy.[15]

A similar discussion can be seen in calls from a range of prominent voices, particularly in the US, ranging from Elizabeth Warren to Steve Bannon to regulate "Big Tech companies" as public utilities. As such they advocate to embrace a more expansive concept of what have traditionally been considered as public utilities.

Essentially these market-related interventions are seen as a medium-term solution to some of the problems that characterize our current Digital Public Sphere. They don't aim to address the immediate 'downstream' harms to the Digital Public Sphere, but they can address at least two underlying structural causes by:

1. enabling the emergence of alternatives to the services of dominant companies, which enables user choice and which could decrease the dominant position of some of these firms - thereby limiting their role as gatekeepers of the Digital Public Sphere

14 Ezrachi, *EU competition law goals and the digital economy*. Oxford Legal Studies Research Paper, 2018.

15 Wu, *The curse of bigness*. Columbia Global Reports, 2018.

2. prohibiting excessive or exploitative data collection practices, which provide unprecedented tracking opportunities and competitive advantages for dominant ad-driven platforms vs traditional publishers

While a range of market interventions could potentially tackle these broad causes, the following often cited proposed market interventions by activists and politicians were identified by desktop research and our interviewees as potentially resulting in a positive side effect on the resilience of the Digital Public Sphere. The first two are options that are often invoked in the US debate, but which can cover a variety of interpretations: (1) regulate platforms as public utilities and (2) impose structural separations on dominant platforms ('break them up'). The next three are more detailed options which could be imposed as new obligations or behavioral remedies on dominant platforms, for example in the context of the EU's Digital Markets Proposal: (3) ban excessive data collection via third party trackers, (4) ban dark patterns and (5) impose interoperability requirements on dominant companies.

4.1 'Regulate platforms as public utilities'

Historically, public utility regulation is a non-market-based approach that has been used to regulate private ownership of critical infrastructure (such as railways or telecoms) or natural monopolies (such as electricity, water or gas providers). Usually there is one main physical infrastructure network that provides the good or service. Governments have in the past regulated these infrastructure networks in order to impose public interest obligations on their private owners. In general, this amounted to a duty for those owners to provide a reliable and fair service at a reasonable price on a non-discriminatory basis. The classic economic rationale for such regulation is that without such regulation the most probable outcome would be that a small number of enterprises (or perhaps one) would dominate the market and set prices at economically unjustified levels. But beyond that rationale, public utility regulation has also been used to address the power imbalance that stems from private control of essential infrastructure and ensure the accountability of private actors towards the public good.[16]

Proponents of regulating Big Tech companies as utilities argue that these companies benefit from similar economies of scale and network effects and act as gatekeepers to goods and services that one must have access to if one wishes to participate fully in society.[17] For some, the Covid-19 crisis has

16 Teachout and Rahman, From Private Bads to Public Goods: Adapting Public Utility Regulation for Informational Infrastructure. Knight First Amendment Institute, 2020.

17 Ghosh, Don't Break Up Facebook — Treat It Like a Utility. Harvard Business Review, 2019.

further demonstrated the essential public function that Big Tech companies to varying degrees have played, for instance by "providing a one-stop-shop for people in dire need of information, communication and other basic online services".[18] Hence, they rebut criticisms from opponents that Big Tech companies are not natural monopolies, don't provide physical infrastructure or are not "on the same level of necessity" as power, communications lines or water. [19]

Simons and Ghosh argue that Facebook and Google in particular are private companies whose algorithms have become "part of the infrastructure of our public sphere", since they "rank and order vast quantities of content and information, shaping how we consume news and access information, communicate with and feel about one another, debate fundamental questions of the common good, and make collective decisions".[20] In their view, both companies should be treated as "a new kind of public utility — utilities for democracy". On these utilities, four new kinds of obligation could be imposed: (1) a requirement to respect public values (equal access, non-discrimination, public safety, and consumer privacy), (2) targeted transparency requirements, (3) firewalls to separate functions (such as the commercial imperatives of digital advertising from other functions) and (4) democratic governance tools.

Rahman and Teachout go one step further and argue that a ban on targeted advertising can also be part of such a public utility regulation. Like fair pricing requirements on dominant platforms, such a ban would alter the revenue-generating strategy of the firms themselves and remove the incentives to harvest data through surveillance.[21]

4.1.1 European 'ex ante regulation' as public utility regulation

The option to regulate platforms as utilities or common carriers is mainly a US discussion, based on American doctrine. In the EU, references to public utilities occur far less frequently as most of the goals that such public utility regulation would want to achieve can be dealt with by so-called 'ex ante'

18 Scott, Coronavirus crisis shows Big Tech for what it is — a 21st century public utility. Politico, 2020.

19 See for instance, Crawford, Calling Facebook a Utility Would Only Make Things Worse. Wired, 2018.

20 Simons and Ghosh, Report - Utilities for democracy: Why and how the algorithmic infrastructure of Facebook and Google must be regulated. Brookings, 2020.

21 Zephyr Teachout and K. Sabeel Rahman, From Private Bads to Public Goods: Adapting Public Utility Regulation for Informational Infrastructure, ibid.

regulation, which prohibits certain conduct across the board.[22] Many of the broader, speech-related policy goals that underpin US proposals for public utility regulation would be addressed in the EU by the future Digital Services Act, for example.

When references to public utilities emerge in EU policy documents on regulating the digital economy, they mainly highlight some of the risks that are associated with setting up a new type of public utility regulation for the digital economy. In an influential report for the European Commission, Cremer, de Montjoye and Schweitzer argue that "the risks associated with such a regime – rigidity, lack of flexibility, and risk of capture – are too high".[23]

One separate discussion in the EU focuses on applying the so-called "essential facility doctrine" to online platforms. Under this theory, competition enforcement authorities can impose essential facility-like remedies in cases where a dominant firm refuses to give access to a type of infrastructure or other form of asset that forms a 'bottleneck' for rivals to be able to compete.[24] In the platform economy, refusal to provide access to data can be anticompetitive if the data are an 'essential facility' to the activity of the undertaking asking for access. This could be the case when the data owned by the incumbent is truly unique and there is no possibility for the competitor to obtain the data that it needs to perform its services.[25]

Elements of the broader public utility doctrine can be found in proposals for new ex-ante regulatory models tailored to gatekeepers or "structuring platforms". This is the case of the recently proposed Digital Markets Act in the EU[26], which does not aim to regulate infrastructure monopolies by setting clear access terms for competitors, but - as Caffara and Scott-Morton point out "more broadly wants to ensure fair and contestable digital markets, by

22 See for example: Sebastien Soriano, Big Tech Regulation, Empowering the many by regulation a few, September 2019.

23 Jacques Crémer Yves-Alexandre de Montjoye Heike Schweitzer, Competition Policy for the Digital Era, 2019, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

24 Inge Graef, Rethinking the Essential Facilities Doctrine for the EU Digital Economy, Tilburg University, April 2020

25 See Autorite de la concurrence and Bundeskartellamt, Competition Law and Data, May 2016, http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=B433476372FD2F7A43EF4F482255113D.1_cid387?__blob=publicationFile&v=2

26 https://ec.europa.eu/info/sites/info/files/proposal-regulation-single-market-digital-services-digital-services-act_en.pdf

prohibiting or discouraging conduct which, by intent or effect, prevents entry of a rival, where entry would otherwise be possible".[27] It lists a set of 'do's and don'ts' for gatekeeper companies in its articles 5 and 6, which includes, for instance:

- A duty to silo data, i.e. gatekeeper platforms have to refrain from combining personal data sourced from their core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end-users to other services of the gatekeeper in order to combine personal data
- A duty to provide advertisers and publishers to which it supplies advertising services with information concerning the price paid by the advertiser and publisher, as well as the amount or remuneration paid to the publisher for the publishing of a given ad and for each of the relevant advertising services provided by the gatekeeper.
- A prohibition on using non-public data generated from business users in competition with them
- A requirement to provide effective data portability of data generated through the activity of a business user or end-user, and tools to facilitate the exercise of that data portability.

4.1.2 Reflections

Throughout the workshops that were organized a view emerged that regulating very large online platforms across the board as public utilities would generally result in marginal benefits to the resilience of the Digital Public Sphere, and would not leave enough flexibility to address specific problems related to specific services of specific platforms. As one participant stated: "*utility regulation is the biggest canon you have in your regulatory arsenal, but it doesn't allow you to take into account all the necessary trade-offs that other interventions allow you to make. A medical analogy might work here. If you use too much of a medicine, you can kill the patient by overdosing. But if you use too little, you might not achieve anything*". Or, as another participant put it "*the notion that we can deal with the diversity and heterogeneity of problems in this space by thinking of the platforms as utilities is not operational and does not make any sense to me*".

27 Cristina Caffara, Fiona Scott Morton, The European Commission Digital Markets Act: A translation. Vox, 2020.

One participant mentioned that public utilities have historically been used to deregulate public incumbents in order to prepare them to enter the commercial market, whereas platform regulation starts from exactly the opposite logic: how would you impose more principles-based responsibilities on commercial actors? Public utility regulation also generally comes with a highly detailed list of prescriptive rules, which is less suitable in an ecosystem with rapidly changing business models. A principles-based approach, like the European Digital Markets Act seeks to achieve, was seen as a more suitable option.

But there was agreement among most of the participants that traditional elements that have been associated with a public utilities doctrine such as non-discriminatory access, interoperability, and fairness are suitable safeguards that need to be used more proactively as a safeguard against non-competitive behaviour.

4.2 Impose a structural separation of dominant companies ('break them up')

Similar to the discussion on public utilities, the popular conversation on the need to 'break up' the Big Tech companies is mainly a US discussion. In the US, the US House Judiciary report gave four succinct reasons why such structural separation could be needed[28]:

- Dominant platforms have misappropriated the data of third parties that rely on their platforms, effectively collecting information from their customers only to weaponize this against them as rivals.
- Dominant platforms can exploit their integration by using their dominance in one market as leverage in negotiations in an unrelated line of business.
- Dominant platforms have used their integration to tie products and services in ways that can lock in users and insulate the platform from competition.
- These firms can use supra-competitive profits from the markets they dominate to subsidize their entry into other markets.

In the EU, the European Commission has powers, as defined in Article 102 TFEU, to impose a series of remedial measures against firms that have abused their dominant market position, including the mandating of a breakup of a business as a last resort. This requires an assessment that the infringement of competition law is inherent to the structure of the firm and that behavioral remedies focusing on non-discrimination, access or interoperability would be

28 US House Judiciary Report, Investigation of competition in digital markets, 2020 at 378.

insufficient or more burdensome. However, such procedures take years and only can be done on an ex-post basis. The new Digital Markets Act repeats that structural remedies, such as "legal, functional or structural separation, including the divestiture of a business, or parts of it" should only be imposed "either where there is no equally effective behavioral remedy or where any equally effective behavioral remedy would be more burdensome for the undertaking concerned than the structural remedy".[29]

Structural separation remedies can take many forms. Tim Wu has argued in favor of applying a separations regime in information industries, specifically favoring an approach that would create "a salutary distance between each of the major functions or layers in the information economy".[30] Often-used examples in this context refer to the need to separate Amazon's marketplace from its retail activities where it competes with third-party sellers, or the need to separate Google's ad exchange and business on the exchange (Doubleclick) from the rest of its activities.

Khan has argued that structurally separating Google and Facebook's ad businesses in particular would address concerns with conflicts of interest, as both entities are involved in distributing publisher's content as well as competing with publishers in the sale of ad space.[31] Facebook and Google have used their dominant positions (as a communications network in the case of Facebook, and in search and advertising more generally for Google) to extract sensitive business information from publishers, including information on publishers' audiences. But such a separation might also help to safeguard media pluralism. She argues that

> *Insofar as this dual role played by Facebook and Google deprives publishers of digital advertising revenue, structurally separating the communications networks these firms operate from their ad businesses could potentially be justified on the basis of protecting the news media. Rather than separating platforms from commerce, such a separation would target a particular business model in order to promote media diversity and protect journalism.*[32]

29 European Commission, Proposal for a Digital Markets Act, §64.

30 Wu, *The Master Switch*. Vintage, 2010.

31 Khan, *The Separation of Platforms and Commerce*, 119 Columbia Law Review 973 (2019).

32 Idem at 1068.

As an alternative to full ownership separation, structural separation could be achieved via functional separation remedies such as "Chinese Walls" alongside conduct and disclosure rules.[33] Separation remedies can also include less intrusive interventions such as a duty to keep separate accounts for different activities. For example, Google would have to have separate accounts for Adwords, Search, YouTube and Android, so the revenues from one activity can't be used to finance another one. This increased transparency might facilitate the application of other remedies.[34]

4.2.1 Reflections

There was a wider range of opinions on the effects of breaking up platforms which generally reflected the different backgrounds of the participants. On the one hand economists and competition lawyers among our participants stressed the need to assess the trade-offs between providing sufficient incentives for innovation, investment, economic efficiencies and consumer welfare before arriving at such a decision, whereas other stakeholders were keen to include different political and societal considerations to argue in favor of breaking up such companies.

At the same time economists and competition lawyers also invoked other political reasons to illustrate their reluctance to outright call for breaking up tech companies. Several participants argued that competition agencies don't choose their cases in a vacuum, but they select cases they think are winnable in Court.[35] In a European context, such divestiture cases against US platforms were seen by some as politically toxic, whereas in the US this option would be much more feasible. Others argued - again in a European context - that other, less far-reaching, remedies have not even been properly tried. As one participant noted: "*Instead of focusing on breaking them up we should first try to stop them from merging with other companies in the first place*".

33 Srinivasan has argued that conduct rules could be used to manage the incentive and ability of vertically integrated digital advertising intermediaries to self preference in respect of access to data, speed and the auction. She also suggests that fiduciary duties could apply to digital advertising intermediaries to revert ownership interests in ad server data back to publishers and advertisers, empowering them to share user IDs and other market and consumer data as they see fit. Srinivasan, D. (2019), *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, Berkeley Business Law Journal, Vol. 16/1, pp. 39-101.

34 ARCEP, Remèdes aux problèmes posés par les plateformes numériques structurantes. ARCEP, 2020.

35 This same argument has been invoked to account for why certain EU competition agencies are reluctant to take on data exploitation cases that don't have an obvious leveraging angle.

Yet there was agreement that when behavioral remedies do not achieve their intended effect, structural separation is a viable last option. One participant referred to the work of Ezrachi and Stucke[36] to argue that such separation is the only way to curb the dominant position of a few of the very large online platforms ('Gamemakers') which from the outset seemingly create a competitive environment, such as the online advertising market, but which control that environment entirely and use it to exploit the participants, while primarily benefiting the creator. The harms in such a monopoly ecosystem are not just price and supply-related, but also largely related to broader conceptions of the public interest, including concerns about content distribution.

4.3 Prohibit excessive data collection via third party trackers[37]

A 'third party' tracker is an entity that collects data about users from first-party websites and / or apps, in order to link such data together to build a profile about the user. This data collection is a result of dominant platforms' technology being integrated by a 'first-party' entity into its website or mobile application. A metric for measuring the concentration of power within the tracking ecosystem proposed by Binns[38] demonstrates that a handful of companies are engaged in the great majority of third-party tracking that occurs on the web or through apps.

Third party tracking can be seen as playing a decisive role in attaining market power in the digital environment, since companies derive market power from their ability to gather up-to-date personal information on users across platforms and devices, which allows them to analyze and subsequently monetize this data through targeted advertisements and other means. These data gathering practices of dominant players might also be driving out smaller competitors that do not have the ability to impose such far-reaching privacy terms on their users.

36 Ezrachi, Stucke, *Virtual Competition*. Harvard University Press, 2016.

37 This argument is a simplified summary of Viktoria Robertson, *Excessive Data Collection: Privacy considerations and abuse of dominance in the era of big data (*2020) 57 Common Market Law Review, pages 161–189

38 Reuben Binns et al, *Measuring third party tracker power across web and mobile* https://arxiv.org/pdf/1802.02507.pdf

Data acquired through authorized third-party tracking may be seen as a user's non-price counter-performance for the provision of a 'free' digital service.[39] In many instances, users are not aware to what extent third-party trackers are able to collect personal data related to them and are therefore not informed about the extent of the counter-performance that a certain privacy policy would require from them. This is sometimes the result of misleading or deceitful descriptions in the ToS that describe the extent of third-party tracking[40].

Data collection through third-party tracking in such a way could be regarded as an abuse of dominance within the meaning of EU competition law, where a dominant undertaking degrades the quality of its product by reducing its users' privacy protection, or where it collects amounts of data that appear excessive compared to the users' reasonable expectations[41]. As such this data collection practice could be considered to be 'excessive' in the European Union, under the meaning of Article 102(a) TFEU.

However, excessive data collection does not necessarily need to be modelled on the abuse of excessive prices; it may just as well be possible to regard it as a stand-alone abuse under the heading of unfair trading conditions based on a decrease in quality or the mere excessiveness of the personal data gathered. The abuse of unfair trading conditions may better capture the essence of excessive data collection. It allows for a number of parameters to be taken into account when assessing whether a dominant undertaking is committing an abuse, such as the principle of proportionality, the principle of equity, the indispensability of a trading condition, and the parties' bargaining power. These criteria, which were developed in the case law of the Court of Justice of the European Union, could be applied in the context of the collection and processing of personal user data through third-party tracking.

4.3.1 Reflections

Participants were supportive of this option but pointed out some of its limits, especially if this would be limited to a competition law analysis such as using Article 102 of the Treaty on the Functioning of the European Union as the main point of reference as it wouldn't cover most of the ad tech 'middlemen'.

39 See by analogy the EU's new Electronic communications code, recital 16, which mentions both data and exposure to advertisements as a consumer's counter-performance.

40 See Norwegian Consumer Council, GDPR complaints against Grindr and five third-party companies, available at https://www.forbrukerradet.no/side/complaints-against-grindr-and-five-third-party-companies/

41 See Ariel Ezrachi and Viktoria HSE Robertson, *Competition, Market Power and Third-Party Tracking* (2019) 42 World Competition at 19.

While banning excessive data collection by third party trackers in general would lead to significant privacy improvements and increased safeguards against behavioral discrimination, it would not necessarily affect the dominant position of the largest players in the online ad ecosystem, since much of their power derives from direct, first party tracking across devices and services in the first place. Even more, some participants pointed to the paradox that such a ban could be seen as undermining competition in the online digital advertising market because it would prevent both ad tech vendors and publishers from generating revenue. Others pointed out that having a really competitive online advertising market could lead to many different side effects, "*including the entry of new companies with very little experience of managing data, making ads even cheaper and potentially leading to less revenue for publishers*", according to one participant. However, as one participant noted, the tension between 3rd party tracking and personalisation through infrastructural control "*becomes a bit of a false one when you take a more normative side-step and decide which practices you actually might want to see in the Digital Public Sphere, and what the definition of a vibrant market for that might look like*".

Some participants argued that a better long-term solution would be to consider how to address the actual practice we are worried about (behavioral advertising) rather than the means by which it is facilitated (tracking by first and third parties).

While some participants were sympathetic to this argument most argued that an outright ban could go too far. They argued that targeting of ads based on a person's use of a specific website or app they are intentionally interacting with is fundamentally different compared to behaviorally tracking someone across multiple unrelated websites. This type of first party targeting should be allowed, for instance for newspaper or publishers, as it actually might enable a switch to more contextual advertising. This also might shift a lot of revenue towards the companies that the public is choosing to interact with or the service providers that are servicing that interaction as opposed to various middlemen, including dominant companies, taking up most of that monetary value. Others pointed out that the main goal of banning both first- and third-party tracking wasn't aimed at shifting any revenue between different parties but was mainly aimed at stopping the exploitation of users in the first place.

Others added that even a focus on first party tracking - nor the option to 'ban targeted ads' or data leveraging - isn't future proof since it would not remove the power from platforms to manipulate the public with targeted content. Where up until now the ability to collect data through microtargeting or device fingerprinting has been a determining factor to grow and reach a dominant

position, this isn't necessarily the case in the future. The Google Fitbit merger was highlighted as a first important example of this trend. Google can rightfully claim that they won't process any personal data or use Fitbit data to serve a user ads on Google products, and that is precisely because Google is mainly interested in obtaining Fitbit's data analysis and optimization infrastructure. As one participant stated *"In the long run, optimization comes from whoever controls the ability to coordinate a protocol and run code in a coordinated way*".

4.4 Prohibiting 'dark patterns'

'Dark patterns' is a design term that refers to design choices and characteristics that trick users into making decisions they normally wouldn't make, often by exploiting our cognitive biases. They benefit a dominant company by "coercing, steering, or deceiving users into making unintended and potentially harmful decisions".[42] As the Norwegian Consumer Council points out, "a commonly used dark pattern involves making certain choices prominent and simple, while the choice the user originally wanted to make is obscured or made into an arduous process"[43].

Jamie Luguri and Lior Strahilevitz observe that dark patterns "are harming consumers by convincing them to surrender cash or personal data in deals that do not reflect consumers' actual preferences and may not serve their interests. There appears to be a substantial market failure where dark patterns are concerned—what is good for ecommerce profits is bad for consumers".[44] Dark patterns are often used to direct users toward outcomes that involve greater data collection and processing activities[45]. For example, as the Stigler Committee points out, "a firm might employ ambiguous language that confuses consumers into sharing more personal information than they intended, or it might require consumers who want to select popular settings

42 CNIL, Shaping choices in the digital world, 2019.

43 Norwegian Consumer Council, You can log out, but you can never leave. January 2021, available at https://fil.forbrukerradet.no/wp-content/uploads/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf

44 Jamie Luguri & Lior Strahilevitz, Shining a Light on Dark Patterns 29 (Univ. of Chicago Public Law Working Paper No. 719, 2019).

45 Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, Damian Clifford, 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective' https://arxiv.org/abs/2009.10194, 2020.

that protect their privacy but decrease firm profitability to jump through a large number of hoops in order to do so".[46]

As a result, the use of dark patterns might also lead to competition concerns, as it enables dominant companies to collect more data than a competitive market would allow, further entrenching their market power while diminishing privacy in the process. Dominant platforms routinely design not only user interfaces but also their core services to optimize their service offerings, often using advanced behavioral profiling and testing techniques, such as A/B testing, or finely targeted personalization of their service offering. Some of these design choices:

- are intended to confuse users about their possible choices
- make unrealistic assumptions about what consumers are likely to prefer
- make it difficult for users to express their actual preferences, or
- manipulate/nudge users into taking certain actions.

European consumer organization BEUC has suggested that some dominant platforms could be subject to specific obligations, which can be inspired by the requirements of the Unfair Commercial Practices Directive, to ensure that they make it as easy as possible for consumers to make genuine choices.[47]

4.4.1 Reflections

Participants noted that there are a number of challenges in using this term. Firstly, it suggests that dark patterns are predominantly problematic in user interfaces, whereas dark patterns can also be embedded in a system's architecture. Secondly, while it is a well-established term coming from designers, its definition makes it sometimes hard to fit into existing legal frameworks such as consumer law and data protection law. Hence, some participants preferred talking about 'manipulative design' instead of 'dark patterns'.

Participants stressed how dark patterns illustrated the limitations of data protection legislation. As one participant noted: "*A platform can fulfill all GDPR-requirements related to transparency, privacy by design, consent and so on. But design choices can be used to overcome all these, which allows the platform to then come back to the regulator and say what else do you want us to do*?" Experts noted that most dark patterns could actually be addressed as unfair commercial practices and argued that more litigation in this field might

46 Stigler Committee on Digital Platforms: Final Report, September 2019 at 238

47 BEUC, The Digital Services Act and the New Competition Tool (2020)

be worth exploring. Yet, others argued that banning an additional specific set of practices by dominant platforms could be useful[48].

The discussion also focused on how dark patterns are currently influencing procedures for flagging illegal or harmful content online. Facebook for instance was fined $2.3 million in Germany for violating Germany's NetzDG, partly for making it so hard for users to find and report content on the basis of the law. As one participant pointed out: *"Similar problems could occur in the future if governments seek to compel online operators to make algorithms more transparent for users, label online advertisements or include data portability options"*[49].

4.5 Impose interoperability requirements on dominant companies

Interoperability in its most basic sense refers to a technical mechanism for computing systems to work together - even if they are from competing firms.[50] In general, imposing interoperability requirements on dominant companies as an ex-post remedy or as an ex-ante measure has been put forward as one key counter measure to overcome network effects and high switching costs, which cements their dominant position. This could allow competitors of dominant platforms to connect new services to an existing user base. It could also lower switching costs for users by ensuring that they do not lose access to the network they built on the service of the dominant platform as a result of switching.[51] Finally, it could stimulate the production of alternative tools for citizens to connect to these dominant services, via third party client apps or content moderation plug-ins. The advantages of interoperability requirements over simply 'breaking up' certain platforms, is that they get rid of the '*starfish problem'.* Breaking up a dominant tech company is likely to result in new forms of concentration - just like when you cut a starfish it will just grow back. As one interviewee pointed out: "*With interoperability mandates, you can actually have multiple competitors competing dynamically at the same time, instead of one big monopoly.*"

48 The work done by the Dutch Authority for Consumers and Markets was used a source of inspiration in this context, see ACM Guidelines on the protection of the online consumer. February 2020, https://www.acm.nl/sites/default/files/documents/2020-02/acm-guidelines-on-the-protection-of-the-online-consumer.pdf

49 See also Sebastian Rieger, Caroline Sinders, Dark Patterns: Regulating Digital Design. SNV, 13 May 2020, available at https://www.stiftung-nv.de/en/publication/dark-patterns-regulating-digital-design#collapse-newsletter_banner_bottom

50 Ian Brown, Interoperability as a tool for competition regulation, OSF 2020, at 4

51 US House Judiciary Report, Investigation of competition in digital markets (2020), available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf at 385

Brown has developed a sliding scale of interoperability obligations that could be imposed by competition regulators on dominant platforms. The greater the obligations the more freedom users get in terms of services and software they can use to interact with platforms and other users, but also the greater the requirements for regulatory action/market intervention and technical complexity[52]. He summarizes five different levels of interoperability obligations.

Five Levels of Interoperability

1. **Platform-permissioned vertical interoperability**: users can connect their own account on complementary services from a third party to a platform, with its express permission. Users can use major platform IDs to log in to other services. Competition regulators might still impose transparency and stability requirements, and limit self-preferencing.
2. **Open vertical interoperability:** users can connect their own accounts and open IDs on complementary services, or apps, from a third party to a platform, without the platform's permission. This would enable real-time data portability.
3. **Public horizontal interaction** (no external user authorization needed), for publication and messaging with competing services.
4. **Private horizontal interaction** (external user authorization needed at this and higher levels):
    a. Sharing – Platform users can share resources (such as a feed) with a limited number of readers (who should not need an account on that platform).
    b. Messaging – an account owner can authorize any other user to send them (or groups they administer) messages or other types of content.
    c. Social graph: a platform user can authorise a third-party service to access enough details of their contact list to identify contacts present on both.
5. **Seamless horizontal interoperability:** users have the ability to use directly competing services to a platform's own for:
    a. Componentisation – to replace components on a platform.
    b. Seamless interaction with its users.

52 Ian Brown, The Technical components of interoperability as a tool for competition regulation, 26 october 2020, available at https://www.ianbrown.tech/2020/10/26/the-technical-components-of-interoperability-as-a-tool-for-competition-regulation/

The Stigler report concluded that interoperability "may contribute to reducing the gatekeeping power of [dominant] platforms and positively impact the type of information that users consume".[53] Brown suggests that interoperability "enables a parallel route" by which content moderation problems can be solved as it could give users "greater choice of different content moderation regimes, even on the same platform (separately from the issue of statutory requirements for platforms to remove illegal content)". [54] Aviv on the other hand has warned about the "'magical decentralization fallacy' - which he calls "the mistaken belief that decentralization on its own can address governance problems".[55] Ovadya argues that in cases of misinformation and harassment, decentralization can "lead to a far worse world", which in democracies "just turns a hard centralized problem into a harder coordination problem"."

One way to implement some of these mandatory interoperability requirements is to mandate social media platforms to open up access to their platforms to third-party providers through an API. Third-party providers use the API to create competing or complementary services, and users then select the version of the service they want from a competitive marketplace with many providers.

There are different variants of this proposal[56] which have been dubbed 'Magic API proposals' by Daphne Keller. According to Keller, the magic APIs model is broadly analogous to telecommunications "unbundling" requirements, which aim to insert competition into markets subject to network effects by requiring incumbents to license hard-to-duplicate resources to newcomers.

> *In the platform context, this would mean that Google or Facebook opens up access to the "uncurated" version of its service, including all legal user-generated content, as the foundation for competing user-facing services. Competitors would then offer users some or all of the same content, via a*

53 Stigler Committee on Digital Platforms: Final Report, September 2019 available at https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report at 144

54 Ian Brown, Interoperability as a tool for competition regulation, OSF 2020, at 26.

55 Aviv Ovadya, The "Magical Decentralization Fallacy," November 2018, available at https://medium.com/@aviv/the-magical-decentralization-fallacy-69b426d16bdc

56 See further https://writings.stephenwolfram.com/2019/06/testifying-at-the-senate-about-a-i-selected-content-on-the-internet/, https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech, https://www.techdirt.com/articles/20200901/13524045226/if-lawmakers-dont-like-platforms-speech-rules-heres-what-they-can-do-about-it-spoiler-options-arent-great.shtml

> *new user interface with their own new content ranking and removal policies.*[57]

One particular version of this idea was floated by Twitter CEO Jack Dorsey when he imagined "an app store-like view of ranking algorithms that give people ultimate flexibility in terms of what posts are put in front of them".[58]

Article 19 proposes what appears to be a more limited version of the 'Magic APIs' proposal, which is specific to unbundling hosting and content moderation services. Unbundling would allow users to change characteristics of the service without leaving a platform, and could encourage competition on qualities that are net-positive for the public sphere (e.g. privacy safeguards and a variety in content moderation standards). The social media platform would be one of many content moderation providers; it would allow third-party content moderation providers access to its platform through the API, and these third-party providers would then provide users with alternative content moderation services.

> *This kind of functional separation would not impede large social media companies from offering content moderation to their users; however users would decide whether to opt in if they want to have the same provider offering both hosting and content moderation services. In other words, when creating a profile on Facebook, for example, the user would be asked to select a content moderation provider, and Facebook could remain one of the options to select, but it should not be the default one. Ideally, and to avoid further lock-in, users would remain free to change their choice at any time, through the platform's settings.*[59]

In this sense, the API would side-step the conversation about an individual platform's community standards and allow for a pluralistic ecosystem that preserves freedom of expression. Keller describes the API as 'magic' because of its technical complexity (how would it interact with the technical

57 Daphne Keller. Who Do You Sue? State and Platform Hybrid Power over Online Speech. (pg. 26)

58 Jacob Kastrenakes, Twitter's Jack Dorsey wants to build an app store for social media algorithms. The Verge, 9 February 2021, available at https://www.theverge.com/2021/2/9/22275441/jack-dorsey-decentralized-app-store-algorithms

59 ARTICLE 19's Recommendations for the EU Digital Services Act, see also Article 19. Why decentralization of content moderation might be the best way to protect freedom of expression online

architecture for advertising?) and legal complexity (how would it interact with data protection and privacy laws?), yet others do think that these questions are solvable.[60] Additional questions focus on which appropriate standards definition organization should plan standardization support for interoperability requirements in digital markets.

4.5.1 Reflections

Participants agreed that most interoperability mandates would not address the problem of 'bigness' or monopoly powers, and as such might not be interesting as remedies to address these problems for specific markets such as the online advertising market. However, there was agreement that proactive interoperability mandates would enable a level playing field between different actors to compete with one another on a well-specified pre-defined market segment, which is especially relevant in markets with strong network effects. This also might allow new entrants to actually compete on privacy or data protection as a quality metric.

Interoperability is often portrayed as a 'technical' solution but throughout this project participants agreed that interoperability mandates contain a number of explicit normative assertions which can have a number of positive and negative effects on the resilience of the Digital Public Sphere.

Participants debated how pro-active interoperability mandates at an infrastructural level, which would include building protocols for decentralized social media, would allow people to communicate across networks. Several participants stressed that this could have far-reaching consequences for the ability to moderate or take down content online. By removing even more friction from the content sharing process, the proliferation and amplification of harmful content could exponentially increase. Others wondered how such a proposal would interact with notice and actions procedures: is a platform supposed to take down content that comes from another platform? However, one participant argued that this form of interoperability doesn't necessarily mean that every piece of content can flow to every point of the network. There should always be red lines for what could be shared and not, based on human rights law. Other participants highlighted that this would be difficult to implement and enforce in practice. They also argued that in practice this could result in a further convergence of content moderation standards in order to adhere to content-related laws that require specific interventions when illegal or harmful content is noticed on these separate platforms. This could actually lead to a declining diversity in content moderation standards.

60 Ian Brown, Interoperability as a tool for competition regulation, OSF 2020

But such interoperability mandates shouldn't necessarily lead to one big interoperable singular social media network, as they could be limited to mandating the use of specific APIs that would allow challengers to access specific categories of data that are in the hands of the incumbents. How such access could be done in a privacy compliant way would be crucial to think through in advance. But getting this right, according to one participant, "*could help companies across the economy to build their own machine learning and AI, instead of being dependent on automated systems built by companies who hold training data"*.

More limited interoperability mandates that would unbundle hosting and content moderation services might give back some agency to people, especially if the switching costs to change to another 'content moderation filter' would be low. As one participant said: "*This would only work if it's as easy to switch filters for consumers as it would be to switch channels on a TV channel*." It was argued that obliging dominant platforms to offer a choice in different content moderation service providers would improve the amount of trust people have in their online information environment as they would have a better idea of what they are seeing and why. This lack of agency and trust in the online environment was mentioned by some participants as an important factor that contributes to why some people are vulnerable to disinformation. According to one participant: "*The research today very strongly supports the idea that one reason people appear to be vulnerable to disinformation is they feel disempowered, and they lack a sense of agency. Having disinformation policies foisted on them by a very small number of platforms in an opaque way, perhaps influenced by political movements they don't like, just makes this feeling worse. A market in which there is more choice in terms of choosing the community to which you belong, and more ways to get involved in content moderation decisions, could address some of these broader problems*".

Some argued that this option addresses the question of what should be done with legal yet harmful content. "*This model approaches most optimally how societies currently decide which speech should be illegal. Only laws can - and should - set those standards. These can be the red lines in a federated online sphere. Other types of speech can be experienced as harmful to different extents to different communities, which can then choose to join communities which apply different sets of (content moderation) rules*". Others argued that while this option might increase the choice in content moderation options, it could push historically marginalized groups to the fringes of public debate once again, and could also contribute to a further fragmentation of the Digital Public Sphere.

5. Conclusion

This paper starts from the hypothesis that in a resilient Digital Public Sphere (1) data is governed responsibly in line with data protection rules, (2) free expression is upheld while (3) fragmentation and polarization of discourse is reduced and (4) disinformation and hate speech are mitigated in a timely and decisive manner. In this Digital Public Sphere, (5) real possibilities for alternative social media networks can emerge in which citizens would have the ability to connect outside the dominant platforms.

While a range of policy interventions could achieve these goals, the aim of this project was to explore specifically whether a number of market interventions could indirectly contribute to these goals. The first two interventions are options that are often invoked in the US debate but which can cover a variety of interpretations: (1) regulate platforms as public utilities and (2) impose structural separations on dominant platforms ('break them up'). The next three are more detailed options which could be imposed as new obligations or behavioral remedies on dominant platforms, for example in the context of the EU's Digital Markets Proposal: (3) ban excessive data collection by third party trackers, (4) ban dark patterns and (5) impose interoperability requirements on dominant companies.

Throughout a series of three workshops with 40 civil society experts, competition lawyers and academics the following main insights emerged.

- **None of the interventions were seen as having an immediate, direct impact on the amount of disinformation or hate speech that would be available in the Digital Public Sphere. Nor would any of the interventions result in significantly less polarization.** This is partly the result of the framing of the problem, which indirectly creates a priority in the societal harms that need to be fixed. The 1960s concept of a public sphere has always been flawed, as it didn't include the perspectives of historically marginalized groups. Some of the harms of our current online media ecosystem are disproportionately experienced by historically marginalized groups, who are the primary targets of online harassment, abuse, and hate speech. A common US perspective which claims that a 'resilient' digital sphere should be characterized by more choices to exercise one's freedom of speech would not address this particular category of harms, and neither would a traditional European vision of a resilient public sphere, which would predominantly aim to impose limits on how dominant tech companies use data to manipulate our information ecosystem. This reinforces earlier findings that there are a number of speech-related harms for which competition is not a sufficient answer.

- **Most of the interventions were generally seen as contributing to better data governance practices** (with the exception of the 'break them up' scenario), **whereas both the 'break them up scenario' and the 'interoperability scenario' were seen as contributing to a more diverse ecosystem of platforms.**
- Participants noted that these interventions don't live in a vacuum of other solutions and their **impact can vary widely depending on the (regulatory) context in which they are taken.**
- However, while competition tools might not lead directly to a lot of these changes, they might result in opening up a new set of options to address ongoing harms. Imposing more limits on data collection practices might have second-order effects that have an impact on how political actors could target voters, or to exclude categories of people for advertising in a discriminatory way, for instance.
- **Several of the interventions go some way to addressing the economic incentives of a digital public sphere funded (almost) entirely by targeted advertising.** The 'prohibit excessive data collection' scenario does this most explicitly, but this is also explored in the 'public utility' scenario (by including a ban on targeted advertising as an obligation for public utilities), the 'break them up' scenario (by separating platforms' communications networks from their advertising businesses) and the 'dark patterns' scenario (by restricting companies' ability to force/manipulate users into sharing their data). However, none of the options provides for a proven, viable alternative funding model that could support a resilient Digital Public Sphere without some of the negative impacts inherent in existing models. This is a possible area for further exploration.