

GOVERNING ONLINE GATEKEEPERS

TAKING POWER SERIOUSLY

by Justin NOGAREDE



GOVERNING ONLINE GATEKEEPERS

TAKING POWER SERIOUSLY

by Justin NOGAREDE

*The author and foundations involved in this project would like to thank Michelle Meagher for substantial input, and the participants to the seminars for their constructive feedback on the topic, in particular the following experts:
Catalina Goanta, José van Dijck, and Orla Lynskey*

Policy report published in January 2021 by

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES



**THE FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES (FEPS)**

Rue Montoyer 40, B-1000 Brussels, Belgium
+32 2 234 69 00
info@feeps-europe.eu
www.feeps-europe.eu
@FEPS_Europe



FRIEDRICH-EBERT-STIFTUNG

Hiroshimastrasse 28, D – 10785 Berlin, Germany
+49 30 26935-7413
www.fes.de
@FES_Brussels



FONDATION JEAN-JAURES

12 Cité Malesherbes, 75009 Paris, France
+33 (0)1 40 23 24 00
www.jean-jaures.org
@j_jaures



FUNDACION PABLO IGLESIAS

Calle Margués de Riscal 6, 28010 Madrid, Spain
www.fpabloiglesias.es
@fpabloiglesias



FONDAZIONE PIETRO NENNI

Via Alberto Caroncini 19, 00197 Rome, Italy
+39 (0) 68077486
www.fondazioneNenni.it
info@fondazioneNenni.it
@FondazioneNenni

With the financial Support of the European Parliament



European Parliament

The present study does not represent the views of the European Parliament

Copyright © 2021 by FEPS
ISBN: 978-2-930769-48-6

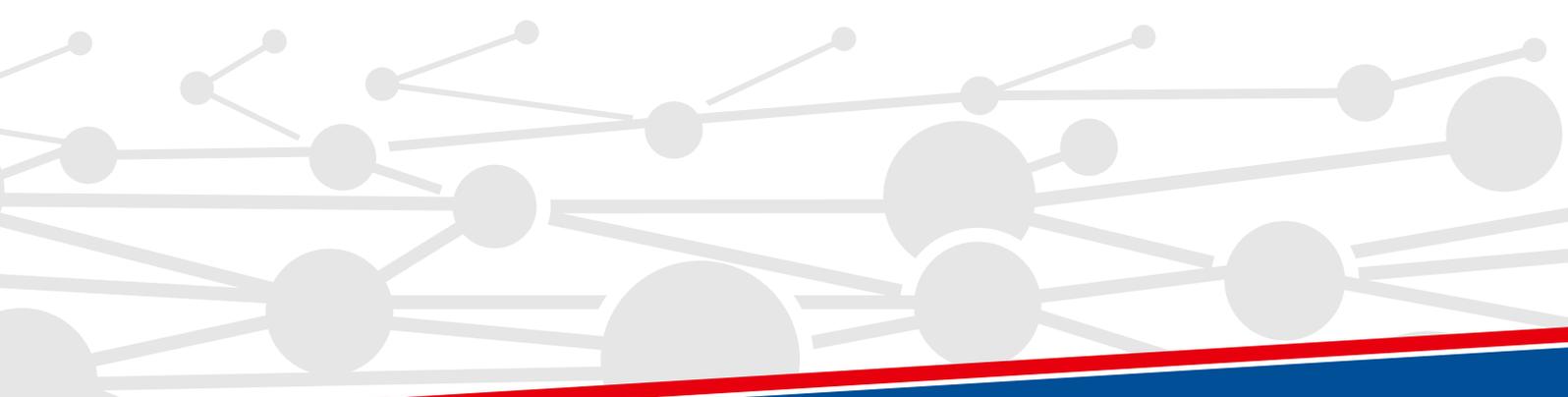
Graphic design : Triptyque.be
Photo cover: Shutterstock

TABLE OF CONTENTS

EXECUTIVE SUMMARY AND RECOMMENDATIONS	6
INTRODUCTION	10
ONLINE PLATFORMS: GATEKEEPERS OF THE DIGITAL AGE	11
- Common infrastructure, corporate control	11
- A hierarchical ecosystem of powerful actors	12
- Democracy and society: negative externalities?	17
THE EXISTING EU POLICY FRAMEWORK	19
- Competition policy: a narrow interpretation, too widely applied	19
- The rules: sector-specific versus horizontal	23
- A note on enforcement: the GDPR	28
GATEKEEPERS: AN AGENDA	31
- The internet as infrastructure	31
- Gatekeepers: simple and asymmetrical rules	32
- Content, information and democracy	33

LIST OF FIGURES

Figure 1: Google’s online consumer-facing services	13
Figure 2: Facebook’s online consumer-facing services	14
Figure 3: Big tech is eating the world?	15
Figure 4: In search of competition: Google Search’s dominance	20
Figure 5: Of platforms, intermediaries, online marketplaces and more: recent laws affecting platforms	27
Figure 6: Budget differences EU Data Protection Authorities	30
Figure 7: Big tech firms’ cash versus Data Protection Authorities’ budgets	30
Figure 8: Facebook already monitors and tags pictures uploaded to its platform	34







EXECUTIVE SUMMARY AND RECOMMENDATIONS

WHY SHOULD THE EU INTERVENE IN THE BUSINESS MODELS OF LARGE ONLINE PLATFORMS?

In the absence of public investment and legislation, the internet has evolved into an online ecosystem of powerful and private gatekeepers that control a wide range of digital services essential for businesses, citizens and society. These gatekeepers regulate social activity via the technical design of their services, but in ways that are increasingly at odds with the public interest, societal well-being, and citizens' rights.

For instance, the organisation of digital services according to what sells the most advertisement has had large, unintended consequences for the quality of public debate and the sustainability of the media. Left unchecked, the power and mode of operation of these gatekeepers will expand into and over public services, such as healthcare and education, and into and over physical infrastructure, such as mobility and the 'smart home'. The EU needs to ensure these infrastructures are designed to foster interoperability, data protection, transparency and ultimately democracy.

WHY IS WHAT THE EU HAS DONE SO FAR NOT ENOUGH?

The EU has long relied on competition policy to regulate big platforms, but as they have grown in power and metastasised across many sectors, this case-by-case approach has become insufficient to address the scale of the problem, and the different public values and fundamental rights that are at stake.

Since 2016, the EU has taken a sector-specific approach towards online platforms, with the aim of aligning their business models with the public interest. But the different self-regulatory and legal initiatives lacked ambition, whilst adding legal complexity. Simply put, the sector approach does not match the converging ecosystem of powerful multi-sided platforms, and self-regulation has meant that platforms, instead of public authorities, now decide how citizens can exercise their fundamental rights online. Instead, the EU should take a horizontal approach by creating new rules for online gatekeepers and updating the E-Commerce Directive of the year 2000. The latter has been inspired by US laws that give one-sided priority to innovation and free speech, over other important rights and values such as fairness, equality, media plurality, health and safety. The harmful effects of that approach are increasingly visible, not least in the US itself.

Furthermore, enforcement authorities have not been sufficiently rigorous in holding big platforms to account for their infringements of existing laws, in particular the General Data Protection Regulation (GDPR). This has allowed illegal business models around the collection of personal data to flourish. Data protection authorities in particular struggle to overcome the information asymmetry with regard to the largest platforms, and to match their resources. In addition, enforcement institutions are scattered across the EU's territory and across different domains, whereas the biggest platforms operate EU-wide and their business models impact on consumer laws, data protection laws and competition laws at the same time. This is a mismatch of weak, decentral and sectoral enforcers and strong, centralised and multi-sectorial platforms.

WHAT SHOULD THE EU DO NEXT?

The EU needs to act now to create a new balance of power, not just in the interest of competition and innovation, but to buttress the economic and political freedoms of citizens, and to protect democracy. This requires public investment, new and simple rules for gatekeepers, and significantly more resources and coordinated capabilities for enforcement.

RECOMMENDATIONS:

Public investment in essential infrastructure

- Many of the services provided by gatekeeper platforms are essential infrastructure – and yet public authorities have made little effort to shape the design of this space, which is now characterised by ubiquitous surveillance. Remedying this situation will require public investment. The debate about how and in what to invest should start swiftly, given the soon to be released 1.8 trillion EUR in public funds linked to the next EU budget and the coronavirus recovery fund. There are strategic choices to be made – for instance, an EU-cloud infrastructure would require very high and sustained public investment, whereas a European digital identity infrastructure could give citizens more practical control over their data in the short or medium term.

Regulation: focus on online gatekeepers' economic AND political power

- Competition policy and sector-specific approaches to regulate online platforms are not sufficient. While they have not managed to constrain the power of the biggest online platforms, they have nevertheless created a complicated environment that is difficult to navigate for smaller businesses and new entrants. The EU should make large platforms more responsible for the power that they already exercise, without unwittingly locking in their current position. The EU should therefore proceed with a public law framework that focuses only on the most powerful online platforms, the so-called gatekeepers. This should include rules to limit or outlaw the widespread anti-competitive practices of gatekeepers favouring their own products (through self-preferencing, tying, bundling, and the strategic use of competitors' data).
- This new legal framework should not, however, be limited to restoring competition in the market alone. The business models of online gatekeepers do not only harm competition, but, through the use of opaque algorithmic systems can also negatively affect consumer rights and the protection of citizens' personal data. And given the scale at which gatekeepers operate, such algorithmic governance affects society and democracy as a whole. Putting in place behavioural rules for gatekeeper platforms is therefore important to protect fundamental rights of individuals and important public values such as democracy and transparency.
- The EU should not limit itself to regulating concentrated power in digital markets. It should also actively deconcentrate digital markets, and allow alternative business models and civil society to flourish. This means more stringent merger control laws, and possibly even reversing a few mergers. The EU should also include an effort to assess the impact of new legislation on power dynamics. The European Commission already analyses the impact on SMEs, but this should be broadened to civil society and the good functioning of democracy. Regulators should ask themselves whether initiatives will strengthen existing power, and if so, how this can be remedied and how countervailing powers can be spurred. This could include, for instance, broad citizen participation in the implementation processes, or through participation, consultation and control rights of civil society.

Ensuring responsibility and media plurality in the 'automated public sphere'

- The EU should update the e-Commerce Directive, which did not provide for the internet as we know it today. The biggest content platforms that already use content-recognition systems for commercial purposes should be required to use these systems in the public interest also – to automatically filter out clearly criminal content, such as child pornography. These systems are not perfect and decisions should therefore be subject to human review, and open to challenge at an independent arbitration body. Removing illegal content is of course only one step, and strict follow up via national criminal law proceedings is its necessary corollary. Therefore, platforms should have the obligation to report criminal content and to identify its source to law enforcement, as is already the case in Germany, via its Network Enforcement Act.
- The EU cannot limit itself merely to accepting the power of big platforms to organise opinion, based on whatever sells the most advertisements. The EU should consider additional measures to safeguard the EU public sphere, going beyond the current rules for audiovisual media. This will require more transparency from gatekeepers' on their algorithms and advertisements. But more importantly, it will require institutional innovation, and the organisation of countervailing powers – for example, in the form of support for a European TV streaming and search platform that brings together political news and documentaries from broadcasters across the EU, with automatic subtitling in all EU languages. Germany's new Interstate Media Treaty provides interesting examples that require social media to be more transparent about their algorithms, and to ensure media plurality.

Enforcement: matching gatekeepers' resources and reach

- The biggest online gatekeepers are highly centralised and operate in a variety of sectors in all EU countries. They can leverage money, data and know-how from one sector to expand in another. In addition, their business practices often pose problems from different fields of law, such as competition policy, data protection and consumer rights. But the authorities that have to enforce these rules are scattered; both across sectors, and across the EU. This is a mismatch that must be addressed by the creation of an EU-level regulator, with broad competence.
- The new rules need new enforcement capabilities. The EU needs to be able to intervene quickly and flexibly to ensure data-sharing, portability and interoperability, and to better prevent mergers in concentrated markets. Interoperability in particular can help break scale effects in social media. It should not be preconditioned on a finding of abuse of dominance, as this has been tried and has led to endlessly drawn-out cases. In addition, preconditioning interoperability on a finding of abuse of dominance unduly narrows the scope of enforcement, which should cover at least competition, data protection and consumer concerns.
- Furthermore, data protection authorities need to be properly staffed, required to carry out their duties, and prioritise enforcement against online gatekeepers. Some claim that previous legislative efforts, even successful ones as the General Data Protection Regulation, have fortified existing power constellations. But it was the lack of enforcement of data protection rules that allowed today's gatekeepers to become as powerful as they are, with largely illegal business models. If the GDPR is enforced with more rigour against gatekeepers, this will reduce their relative power and enable a shift away from surveillance and behavioural ads as the prevailing online business model.

INTRODUCTION

Online platforms are the most powerful actors of today's digital economy. Under the motto of 'move fast and break things', they have indeed disrupted a range of sectors. From the media and communications, to e-commerce and labour markets, they cut out middlemen and provide a more direct channel between consumers and sellers, creators and audiences, and increasingly citizens and public services.

Platforms have thus become powerful intermediaries in their own right. But not all platforms are equal. The platform ecosystem is highly centralised, with a few commercial actors occupying key nodes. Via the control of information flows, goods and services, and ranking and rating systems, these actors are able to bend entire markets and social systems to do their bidding. For instance, when Google decides to change its search algorithm, media across the globe have to adapt their operations instantly.¹ The sheer size and resources of these commercial actors also allows them to routinely skirt the law, and simply accept the occasional fine as a cost of doing business.

The infrastructure platform businesses have built and control is not neutral, but a means to exercise power. Their design facilitates the collection of data, and steers the behaviour of the platform users in ways that further the aims of the platform owners. Although citizens, business and workers are dependent on many of these platforms, they have very little insight into the inner functioning of the platforms, let alone the ability to have a say in it.

By reorganising social activity in the interest of data and value extraction, platform's business models can have large unintended consequences for society and democracy. For example, treating information as nothing more than a commodity has degraded public debate by amplifying mis- and disinformation. This requires scrutiny, as online platforms are expanding into delivery of public services such as healthcare and education.

Across the globe, authorities, legislatures, academia and civil society are waking up to this fact, and are pondering action to improve the situation. Much of this effort is focused on restoring competition in digital markets, but there are broader public interests at stake. Already back in 2016, the European Commission took a range of actions to align platforms' business models with fairness, transparency and democracy. But four years later, the Commission now has little faith that these rules – the effects of many of which are still to be fully felt – will be sufficient.

Our paper evaluates existing policy from the angle of the power that online platforms possess. It includes a few recommendations for the EU's planned update of the regulatory framework on the liability and responsibility of online platforms, and the new regulatory framework for the so-called 'gatekeepers', as well as an instrument that would enable better enforcement of existing laws.

¹ News & Tech (2020) 'Google: Non-AMP content to appear in mobile top stories feature', 23 November (https://newsandtech.com/datetime/google-non-amp-content-to-appear-in-mobile-top-stories-feature/article_efe3ff0a-2dcb-11eb-ba26-27ddf6581409.html); Carmen Arroyo Nieto and Josep Valor (2019) 'Google News changes its algorithm, and with it, the media industry', Media Matters Blog Network, Business School of Navarra, 28 October (<https://blog.iiese.edu/the-media-industry/2019/10/28/google-news-changes-its-algorithm-and-with-it-the-media-industry/>).

ONLINE PLATFORMS: GATEKEEPERS OF THE DIGITAL AGE

COMMON INFRASTRUCTURE, CORPORATE CONTROL

Many of the inventions and much of the infrastructure that make up today's internet are the fruit of decades of public investment, starting at least as early as the 1950s. As public institutions led the effort to build the network, they enforced a spirit of cooperation, in which research findings were shared without intellectual property rights restrictions. It is this approach that led to the internet as an open "network of networks", in which any computer and network can exchange information, based on a common "technical language".²

However, when the value of the network became clear for citizens and businesses, the US decided to privatise the infrastructure that we know today as the 'internet'.³ In Europe, the telecoms companies that provided part of the physical network were also largely privatised, although not unregulated.⁴ The EU laid down rules to liberalise and standardise telecoms services across the EU, with the aim of creating a single market. This included common rules on interconnection, data protection, consumer protection and the quality of service.

But in general, the European Commission took a similar ideological stance to the US, stating in 1997 that "the expansion of electronic commerce will be market-driven".⁵ Regulators took a hands-off approach towards the novel digital applications that were coming to light, and, until very recently, have favoured industry self- or light-touch

regulation.⁶ This is particularly visible in the e-Commerce Directive of 2000, one of the key laws shaping today's internet. This directive lays down minimum general rules for services delivered on top of the physical internet infrastructure. One of the main provisions shields online intermediaries, such as website hosting providers, from liability for the content they transmit, store or host.⁷ This is the so-called "platform privilege". It was inspired by Article 230 of the US Communications Decency Act, which is now much debated in the US.

BOX 1: NO PLACE FOR PUBLIC SPACE

When the US decided in the 1990s to fully privatise the forerunner of today's internet, Senator Daniel Inouye objected. He argued that, because the US government funded the creation of the network, it should reserve at least 20% of internet capacity for non-commercial use by non-profit-making organisations, local community groups, and other public benefit groups. In addition, he argued for a public fund, paid for by fees from telecoms firms, to help non-profit-making organisations and government users to exploit their reserved internet capacity. His proposals were never accepted.⁸

2 Ben Tarnoff (2016) 'The Internet Should be a Public Good', *Jacobin*, 31 August.

3 Yasha Levine (2018) *Surveillance Valley. The Secret Military History of the Internet*; New York: PublicAffairs; Shane Greenstein (2015) *How the Internet Became Commercial. Innovation, Privatization, and the Birth of a New Network*, Princeton: Princeton University Press.

4 Kjell A. Eliassen and Johan From (eds) (1999) *The Privatisation of European Telecommunications*, Aldershot: Ashgate Publishing, Chapter 1.

5 European Commission, 'A European Initiative in Electronic Commerce', COM(97)157.

6 See for instance European Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe', COM (2016) 0288. This has never held for the 'carrier' side of the 'internet', which the EU has strongly regulated, primarily to ensure market liberalisation and integration.

7 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

8 Yasha Levine, op cit, pp. 126-127.

What the European Commission did not, and perhaps could not, foresee back in 1997 was that the online environment would become much more critical than a mere online shopping centre, and that the core infrastructure would not consist of passive hosting services. In the decades that followed, a new business model arose, one that is uniquely placed to gather, store and process data from the different types of user that the internet connects via an online interface, or platform. Today, online platforms have become central to the functioning of our economy, society and democracy, both on and off-line. Platforms intermediate between communications, they structure the search for information, enable payments, exercise a controlling influence over the media sector, operate e-commerce marketplaces, and are crucial for many workers and freelancers in the ‘gig economy’.

The rise of platforms challenges existing rules, which are based on clear distinctions between public and private power, and commercial and social activity. For instance, by controlling essential infrastructure, some of the biggest online platform operators are taking on roles that are akin to those of public authorities. But without any of the legitimacy and safeguards that we associate with public authority.⁹ For instance, Amazon’s marketplace, or Apple’s Appstore, are not accurately described as market players – instead, they create and control entire markets. They decide which producers and consumers can access their market, on what conditions, and – via algorithms – how the market operates. In addition, new online business models on for instance Facebook and Instagram increasingly merge social and commercial activity, and this trend is accelerating.¹⁰

A HIERARCHICAL ECOSYSTEM OF POWERFUL ACTORS

Some commentators state that online platforms are not useful as an analytical category. They point out that platforms can have a variety of different business models and operate in many different economic sectors. In Europe, for instance, there are an estimated 7,000 active online platforms.¹¹ In addition, different strategies of monetisation, for example selling advertisements as opposed to taking a fee for each transaction, create very different incentives and problems.¹² And yet, this paper argues that just focusing on individual platforms and their idiosyncrasies is to lose sight of the forest by zooming in on the trees.

Economic literature highlights commonalities in the business models of online platforms – notably their capacity to benefit from network effects and (close to) zero marginal costs, which create ‘winner-take-all’ dynamics,¹³ and their ability to extract and leverage data from the commercial and social interactions they facilitate.¹⁴ Although this does not necessarily lead to monopolies or oligopolies in and of itself, it does, however, create them in the current economic and political environment of extensive IP and trade secret protections, of a conservative interpretation of competition policy, and of a venture-finance ecosystem that aggressively prioritises scale.¹⁵ In a variety of online sectors there are now one or a few powerful providers of services such as search, social media, app selection, ride-sharing, smartphone operating systems, online marketplaces, video-sharing, web-browsing, ads exchange, short-term home rental and more.

9 Frank Pasquale (2018) ‘New Economic Analysis of Law: Beyond Technocracy and Market Design’, University of Maryland Francis King Carey School of Law, Legal Studies Research Paper No. 2018-17; Nicolas Suzor (2019) ‘A constitutional moment: How we might reimagine platform governance’, *Computer Law & Security Review* 36.

10 Andreessen Horowitz (2020), ‘Social Strikes Back’, <https://a16z.com/social-strikes-back/>.

11 The European Commission estimates that Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services would apply to 7,000 online platforms operating in Europe (https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1168).

12 Christine Caffarra (2019) ‘Follow the Money’, Concurrences No 91579, August; see also Ben Thompson, who criticises lumping ‘big tech’ together, and who distinguishes between services that aggregate consumer demand such as Facebook, Netflix, and Google Search, and more classic platforms, such as Apple’s control over devices and the App Store, for which it demands a fee. Ben Thompson (2015) ‘Aggregation Theory’, *Stratechery*, 21 July (<https://stratechery.com/2015/aggregation-theory/>).

13 For the general argument on scaling effects linked to intangibles, on which many platforms rely, see Jonathan Haskel and Stian Westlake (2018) *Capitalism without Capital. The rise of the intangible economy*, Princeton: Princeton University Press.

14 Nick Srnicek (2017) *Platform Capitalism*, Cambridge UK: Polity Press, pp. 95-97.

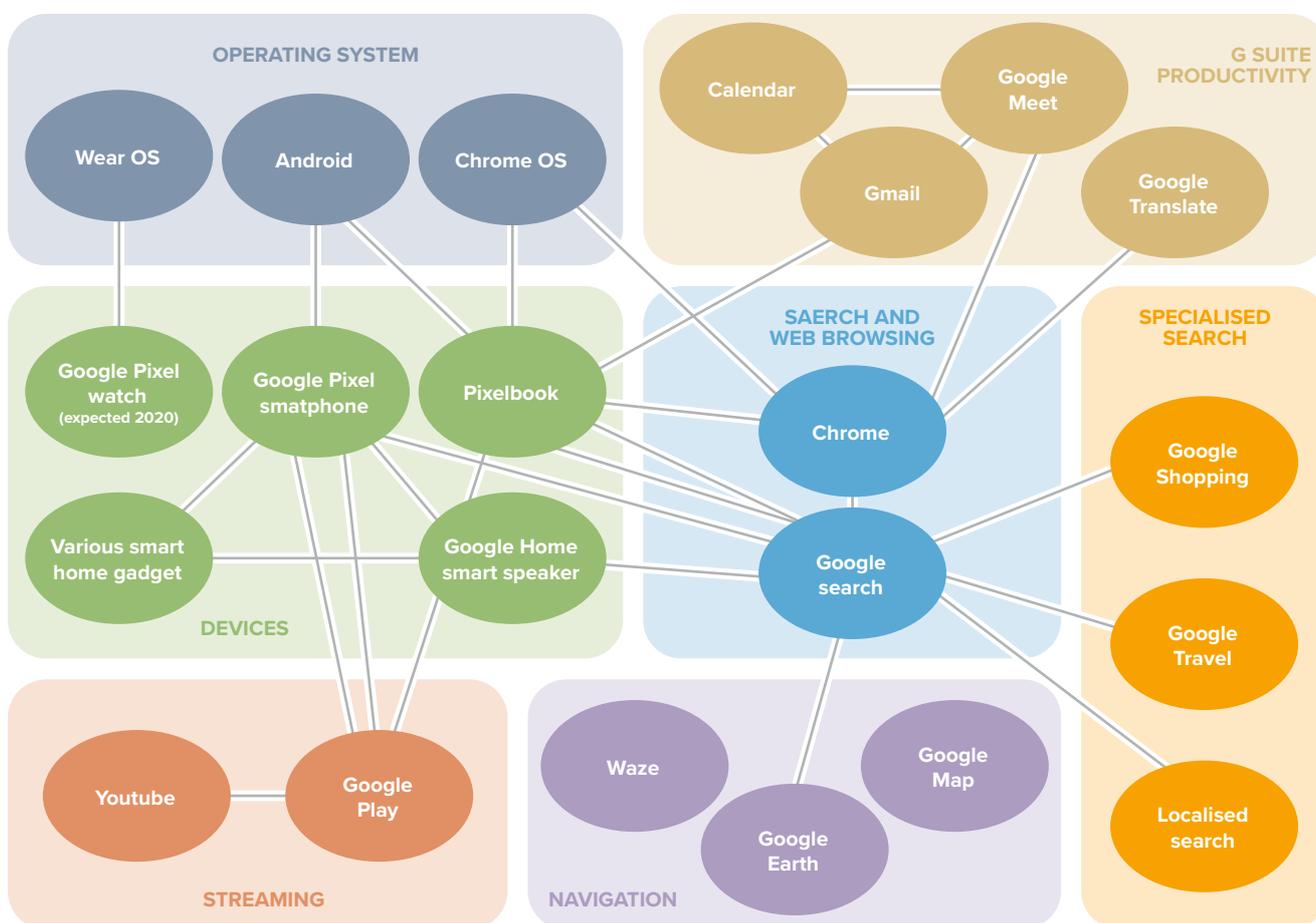
15 See Julie Cohen (2019) *Between Truth and Power*, Oxford: Oxford University Press; Frank Pasquale (2015) *The Black Box Society. The Secret Algorithms That Control Money and Information*, Cambridge MA: Harvard University Press.

ONLINE PLATFORMS: GATEKEEPERS OF THE DIGITAL AGE

In addition, media and communications literature also analyses the emergence of platforms as a form of infrastructure with common characteristics.¹⁶ While there is no definite classification of different types of platforms yet,¹⁷ it is clear that certain ‘super-platforms’ play a crucial role. The last decades have seen the creation of a hierarchy organised platform ecosystem, characterised by a strong centralisation of power. For instance, in August 2020, the market capitalisation of tech firms Apple, Amazon, Microsoft, Facebook and Alphabet reached over US\$9 trillion.¹⁸ Together they own around 70 platforms, which

include much key online infrastructure.¹⁹ The biggest platforms structure the overall ecosystem: any business that wants to operate online needs to adapt to the logic of Google Search’s algorithm, or to the conditions set by Apple’s App Store. While the biggest firms compete with each other in certain areas, they are also strategic partners. For instance, for the past 15 years, Alphabet has been paying Apple to ensure Google Search remains the default search engine on Apple devices. According to the US Justice Department, these annual payments now total between US\$8 billion and US\$12 billion a year.²⁰

Figure 1: Google’s online consumer-facing services (source CMA)



16 Jean-Christophe Plantin (2016) ‘Infrastructure studies meet platform studies in the age of Google and Facebook’, *New Media & Society* 20.

17 But see the distinction between infrastructural, intermediary, and sectoral platforms, in José van Dijck (2010) ‘Seeing the forest for the trees: Visualizing platformization and its governance’, *New Media & Society*.

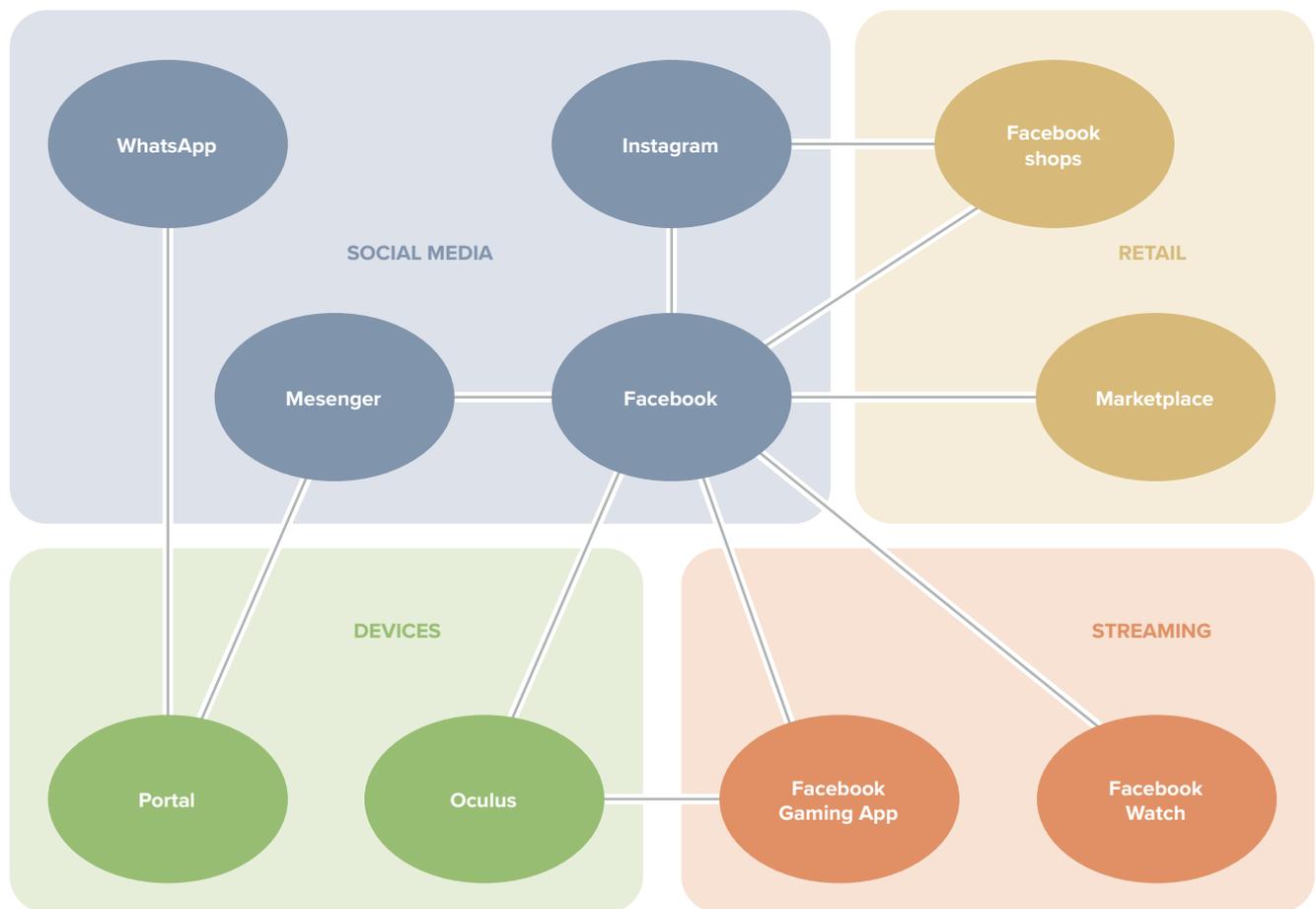
18 Sergei Klebnikov (2020) ‘U.S. Tech Stocks Are Now Worth More Than \$9 Trillion, Eclipsing The Entire European Stock Market’, *Forbes*, 28 August (<https://www.forbes.com/sites/sergeiklebnikov/2020/08/28/us-tech-stocks-are-now-worth-more-than-9-trillion-eclipsing-the-entire-european-stock-market/#4418936f3e61>).

19 José Van Dijck (2018) *The Platform Society. Public Values in a Connective World*, Oxford: Oxford University Press.

20 NPR (2020) ‘Google Paid Apple Billions To Dominate Search on iPhones, Justice Department Says’, 22 October (<https://www.npr.org/2020/10/22/926290942/google-paid-apple-billions-to-dominate-search-on-iphones-justice-department-says?t=1606347425954>).

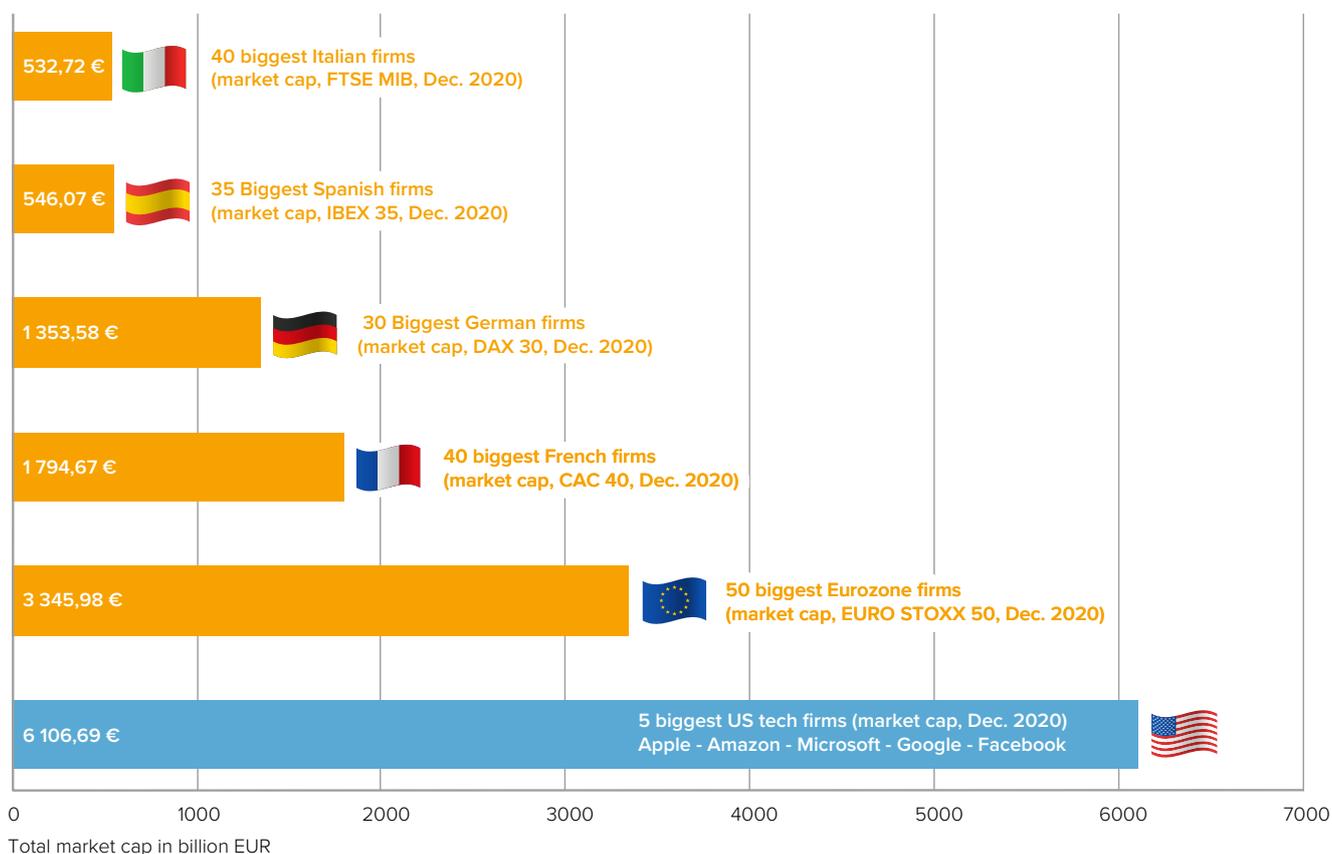


Figure 2: Facebook's online consumer-facing services (source: CMA)



ONLINE PLATFORMS: GATEKEEPERS OF THE DIGITAL AGE

Figure 3: Big tech is eating the world?



The biggest online platforms pursue strategies of vertical integration, meaning that they aim to control multiple aspects of a particular value chain. They can also leverage their power in one market to gain a foothold in adjacent markets, increase control over customers and suppliers, and make it impossible for potential competitors to enter markets. For example:

- To protect its position in search, Google established a dominant position in web browsing via its Google Chrome browser, and in mobile operating systems via Android, both of which come with Google Search as the default;
- Apple is swiftly moving beyond producing hardware devices, by expanding downstream into the manufacturing of chips, and by leveraging its control over the iOS operating system and AppStore upstream for the selling of services such as Apple Music, News, TV, Arcade, and in the future possibly even search;

- Amazon, while owning a huge online marketplace, also provides global distribution services, selling a wide range of its own products via its own platform, offering cloud services and hardware devices such as the Kindle e-reader and Alexa virtual assistant, and increasingly selling online advertisements, traditionally the strong suit of Google and Facebook. The founder of Amazon also owns the Washington Post, a key national newspaper in the US;
- Microsoft expanded beyond its Windows and Office software platforms, and now offers a comprehensive cloud offering to businesses and authorities worldwide. It is also active in the online gaming market, has its own search engine, Bing, and took over the professional networking site LinkedIn.

The control over essential digital infrastructure enables companies to engage in endemic rent-seeking: Apple takes a 30% cut for transactions in its App Store; Google receives a cut when people search for news or products

online, via control over digital advertising; and Amazon receives a cut for each sale made by a third-party firm via the Amazon platform. In addition, companies use their platforms to sell and favour their own products, shut out competing businesses, and collect data about competitors and adjacent markets to expand their own market share.

With the resulting revenue, these big digital platform companies can stave off and neutralise any competitive threats. Only between 2008 and 2018, and based on public information, Google took over 168 businesses, Facebook 71, and Amazon 60.²¹ In addition, firms also buy stakes in other digital platforms – for example, Alphabet owns stakes in ride-sharing platforms Uber and Lyft, which both rely on a variety of services provided by Google.

The power of large online platforms is not just confined to ‘cyberspace’. They are increasingly connected to the physical environment and everyday activity. Recent academic literature highlights the infrastructural power of big tech firms as they move into the physical realm and overlay existing infrastructure in mobility, public services (such as education, health and electricity), supermarkets, robotics, and the home.²² This development is variously and loosely referred to as the Internet of Things²³ or the Next Generation Internet.²⁴

Microsoft, Amazon and Alphabet now offer cloud infrastructure for public administrations and universities, and together with a few industrial giants like General Electric and Huawei, they dominate ‘smart city’ markets that are “rapidly evolving to integrate technology into infrastructure, mobility, surveillance and security, lighting and access control, and other community-oriented areas.”²⁵ This leaves the field of ‘artificial intelligence’ (AI) unmentioned. However, huge sums are invested in this, as AI is widely expected to become significant in a variety of domains. Alphabet, Facebook, Microsoft and Amazon are playing an influential role, which is likely to increase.²⁶

In addition, big online platforms also aim to gain a foothold in traditional sectors that are rapidly digitising. For example, Alphabet has partnered with Swiss Re to offer health insurance, while it is also in the process of buying Fitbit, a company that produces wearables for a healthy lifestyle. Google has also become the biggest collector of health and patient data in the world. Meanwhile it has also branched out into education, with nearly 70% of schools in the Netherlands, for example, already using Google software solutions.²⁷ If the media sector is any indication, the expansion of tech firms into these sectors with very strong societal and public interests bodes ill for the future.

BOX 2: EXPANSION FROM DIGITAL TO COMMON INFRASTRUCTURE

- Alphabet has moved into autonomous driving, via its subsidiary, Waymo
- Amazon acquired Wholefoods to enter the supermarket business
- Facebook is investing heavily in robotics systems and aims to create a digital currency



21 Elena Argentesi (2019) ‘Merger Policy in Digital Markets: An Ex-Post Assessment’, DP14166, Centre for Economic Policy Research, December.

22 Ganaele Langlois and Greg Elmer (2018) ‘Impersonal subjectivation from platforms to infrastructures’, *Media, Culture & Society* 41.

23 Arielle Pardes (2020) ‘The WIRED Guide to the Internet of Things’, *WIRED*, 9 November (<https://www.wired.com/story/wired-guide-internet-of-things/>).

24 Vincent Mosco (2017) *Becoming Digital. Towards a Post-Internet Society*, Bingley: Emerald Publishing.

25 SmartCitiesWorld (2018) ‘Top smart companies named in new index’, 8 March (<https://www.smartcitiesworld.net/news/news/top-smart-companies-named-in-new-index-2683>).

26 CSET (2020) ‘Identifying AI-Related Companies. A Conceptual Outline and Proof of Concept’, July ([see here](#)).

27 Kaya Bouma and Liselot van der Klift (2019) ‘Google wordt steeds grotere speler op scholen, tot zorg van privacyorganisaties’, *de Volkskrant*, 1 November (<https://www.volkskrant.nl/nieuws-achtergrond/google-wordt-steeds-grotere-speler-op-scholen-tot-zorg-van-privacyorganisaties~bae18dcd/>).

ONLINE PLATFORMS: GATEKEEPERS OF THE DIGITAL AGE

DEMOCRACY AND SOCIETY: NEGATIVE EXTERNALITIES?

Big tech firms are undeniably innovative. They invest vast sums in research and development and expand the frontier of technological possibility. But the digital transition is now increasingly synonymous with the vision of technology and society pushed by a handful of firms, and within those firms, a few people, such as Mark Zuckerberg for Facebook, or Jeff Bezos for Amazon.²⁸

It is disconcerting that one man can decide what almost 1.82 billion people view on a daily basis. Such control over information flows gives content platforms the power to directly steer public perception in their favour, and if that fails, they can and do use their cash reserves to influence policymaking.²⁹ As a result, they operate effectively beyond the remit of the law, and are rarely held to account for the routine infringement of existing legislation and fundamental rights. However, the problem is not just with the concentration of power, but also with how that power is used. To quote US Law Professor Tim Wu, “Silicon Valley has the engineer’s mindset of solving one problem and let the chips fall where they may. Which is cool when you’re a start-up with a hundred guys, but when you get a little bigger, not so cool.”³⁰

The term platform has an ambiguous meaning and conjures up notions of architectural concreteness, neutrality and even equal opportunity.³¹ But this misrepresents the reliance of digital services on user profiling, data flows and algorithms.³² Platforms are not simply a fixed infrastructure that allows users to communicate, buy goods, sell their labour or rent their house. Instead, platforms shape and

influence their users’ activities by constantly optimising their algorithms, and hence operations, in reaction to data gathered about user behaviour. The exact way in which this works is often opaque and protected by intellectual property rights and trade secrecy laws; but engineering social activity to obtain the maximum data, attention, and ultimately money, has large consequences.

For instance, much of the social media and search environment has been optimised to track citizens and gather their data in order to predict and influence their behaviour, and to show them the content that is most likely to capture their attention for the sake of maximising profits.³³ By engineering the information landscape to promote whatever most captivates people’s attention, tech firms have degraded the quality of available information, amplified dis- and misinformation, undermined people’s capacity to focus and form social relationships, and negatively affected children’s cognitive development and mental well-being.³⁴ Furthermore, Alphabet’s and Facebook’s commodification of information, and their control over and capture of the bulk of digital advertising spend, has undermined the work of journalists and starved independent media of revenue.³⁵

This prevailing business model, of pouring billions into the development of ‘artificial intelligence’ and data infrastructure to optimise the viewing and sale of online advertisements, has been described as a gigantic bubble – but a bubble on which many have become dependent, and which has large negative consequences.³⁶ Although there is debate about how effective this manipulation is, the surveillance alone already has important chilling effects on citizens’ speech and autonomy.³⁷

-
- 28 Alan Dignam (2019) ‘Artificial Intelligence. The Very Human Dangers of Dysfunctional Design and Autocratic Corporate Governance’, Queen Mary School of Law Legal Studies, Research Paper No. 314.
 - 29 Ingo Dachwitz and Alexander Fanta, ‘Medienmäzen Google. Wie der Datenkonzern den Journalismus umgarnt’, Otto Brenner Foundation in cooperation with the German Trade Union Federation (DGB); Corporate Europe Observatory, ‘Big Tech Lobbying. Google, Amazon & friends and their hidden influence’, 23 September 2020, <https://corporateeurope.org/en/2020/09/big-tech-lobbying>; Kenneth P. Vogel (2017) ‘New America, a Google-Funded Think Tank, Faces Backlash for Firing a Google Critic’, *New York Times*, 1 September.
 - 30 Tim Wu (2018) “A Decade of Cravenness”: Tim Wu on How Enforcing Competition Law Could Have Stopped Big Tech’, *New York Magazine*, 14 November (<https://nymag.com/intelligencer/2018/11/tim-wu-on-how-competition-law-could-have-stopped-big-tech.html>).
 - 31 The Internet Governance Forum is creating a glossary on platform law and policy terms, to provide a common language: <https://www.intgovforum.org/multilingual/content/glossary-on-platform-law-and-policy-terms>.
 - 32 Seda Gürses and Joris van Hoboken (2018) ‘Privacy After the Agile Turn’, in Jules Polonetsky, Omer Tene and Evan Selinger (eds) (2018), *Cambridge Handbook of Consumer Privacy*, Cambridge UK: Cambridge University Press, pp. 579-601; Tarleton Gillespie (2010) ‘The Politics of Platforms’, *New Media & Society* 12, pp. 347-364.
 - 33 Shoshana Zuboff (2019) *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, London: Profile Books.
 - 34 For a comprehensive list of harms, see the ‘Ledger of Harms’ maintained by the Center for Humane Technology (<https://ledger.humanetech.com>).
 - 35 Jonathan Taplin (2017) *Move fast and break things. How Facebook, Google and Amazon cornered culture and undermined democracy*, London: Macmillan.
 - 36 Tim Hwang (2020) *Subprime Attention Crisis. Advertising and the Time Bomb at the Heart of the Internet*, New York: Farrar, Straus and Giroux.
 - 37 For a more sceptical view of the effectiveness of behavioural advertising, see Natasha Lomas (2019) ‘The case against behavioral advertising is stacking up’, *TechCrunch*, 20 January (<https://techcrunch.com/2019/01/20/dont-be-creepy/>); Moritz Büchi (2020) ‘The chilling effects of algorithmic profiling: Mapping the issues’, *Computer Law and Security Review* 36, pp. 1-15.

The capacity for surveillance also leaves consumers, workers and businesses vulnerable to manipulation and coercion by platforms.³⁸

In box 3, Professor of Computer Science Stuart Russell explains the effects of unleashing algorithms that manipulate human behaviour for profit in the area of social media.

Beyond that, big tech firms have pushed a particular form of innovation, one that foregrounds short-term convenience and narrow technological solutions to complex social problems;³⁹ and one that favours disruption over maintenance, leading to an increasingly fragile and opaque ecosystem.⁴⁰ What does it mean, for instance, if Google's Android operating system breaks down, or if Microsoft decides to discontinue its cloud and software operations? Finally, the online ecosystem is one perceived as being largely designed by young, privileged, white males, which limit "innovation" to what they recognise as promising. The perspectives of children, women and people of colour are often not seen and therefore left out. For instance, what does it mean that Instagram's algorithm subtly steers users to include nudity in their posts?⁴¹ Should children be conditioned like that?

The key question is that posed by Dutch Professor of Media and Digital Society José van Dijck. Looking at the platformisation of societies, she asks "how can European citizens and governments guard certain social and cultural values while being dependent on a platform ecosystem whose architecture is based on commercial values and is rooted in a neo-libertarian world view?"⁴² The next section analyses why existing legislation at EU level has been unable to answer that question effectively.

BOX 3: MANIPULATING HUMAN BEHAVIOUR TO OPTIMISE CLICK-THROUGH

"Content selection algorithms on social media are designed to maximize click-through (...). The solution is simply to present items that the user likes to click on, right? Wrong. The solution is to change user's preferences so that they become more predictable. A more predictable user can be fed items that they are likely to click on (...). People with more extreme political views tend to be more predictable. Like any rational entity, the algorithm learns how to modify the state of its environment – in this case the user's mind – in order to maximise its own reward."⁴³

38 Shoshana Zuboff, op cit.

39 See Evgeny Morozov (2013) *To save everything click here*, New York: Public Affairs; and Ben Green (2020) *The Smart Enough City*, Cambridge MA: MIT Press.

40 Lee Vinsel and Andrew L. Russell (2020) *The Innovation Delusion. How Our Obsession with the New Has Disrupted the Work That Matters Most*, New York: Currency.

41 Judith Duportail a.o. (2020) 'Undress or fail: Instagram's algorithm strong-arms users into showing skin', *AlgorithmWatch*, 15 June (<https://algorithmwatch.org/en/story/instagram-algorithm-nudity/>).

42 José van Dijck (2020) 'Governing digital societies: Private platforms, public values', *Computer Law & Security Review* 36. For a discussion on the values propagated by Silicon Valley: Richard Barbrook and Andy Cameron (1996) 'The Californian Ideology', *Science as Culture* 6, pp. 44-72; Langdon Winner (1997) 'Cyberlibertarian Myths and the Prospects for Community', *Acm Sigcas Computers and Society* 27, pp. 14-19;.

43 Stuart Russell (2019) *Human Compatible. Artificial Intelligence and the problem of control*, New York: Viking Press.

THE EXISTING EU POLICY FRAMEWORK

COMPETITION POLICY: A NARROW INTERPRETATION, TOO WIDELY APPLIED

As late as 2015, the European Commission framed its comprehensive digital strategy under the umbrella of the ‘digital single market’,⁴⁴ and it has relied mainly on the competition rules to regulate digital services. However, current competition policy has focused on a narrow concept of economic efficiency, instead of serving a variety of public goals that are being undermined by large online platforms. Even with that more restrictive understanding of what competition policy should achieve, the toolkit of case-by-case assessments of competition in clearly defined markets has been unable to preserve an open, competitive digital environment.

A focus on economic efficiency

Originally, EU competition policy aimed to restrain market power, not just in order to preserve competition, but also because such power has negative repercussions on society and poses a threat to a free and democratic society.⁴⁵ However, although EU competition policy could serve a number of public policy principles that go beyond short-term consumer interest – such as freedom, fairness, sustainability and even solidarity – this is not how EU competition law has typically been applied.⁴⁶

Instead, under the banner of ‘the more economic approach’, the European Commission has essentially narrowed competition policy to the consumer welfare paradigm, in which

low consumer prices and market integration are the primary policy concerns. In the words of one commentator, in competition policy the European “Commission has essentially disclaimed any role for broader public interest consideration.”⁴⁷ This means that for the most part, public interest considerations, such as the preservation of cultural diversity, have not been addressed under the EU competition law framework.⁴⁸

This is unfortunate, because in the platform economy the distinction between economic and non-economic concerns is difficult to make, and the business models of online platforms have broad public interest implications. For instance, the decision who can or cannot access a gatekeeping platform is important for traders, but also for users as citizens in a democratic society. Platforms’ usage of algorithms to personalise offers to their users may restrict consumer choice but can also impinge on users’ autonomy in their capacity as citizens, by using personal data to discriminate against them.⁴⁹

In the literature, the need for more coherence between competition policy, consumer law and data protection has been noted, and there are some signs of incremental change.⁵⁰ Notably, there is the decision from the German competition authority to fine Facebook for breaching data protection rules,⁵¹ claiming Facebook’s actions constituted an infringement of competition law as well as a breach of data protection. But this effort is incremental and contested in both academia and legal institutions. Right now, competition policy does not seem able to protect the wider concerns that stem from the power of large platforms.

44 For an extended critique of this narrow framing, and a more holistic alternative, see Centrum Cyfrowe, Commons Network and Publicspace.online (2019) ‘Vision for a Shared Digital Europe’, April ([see here](#)).

45 Anna Gerbrandy (2019), ‘Rethinking Competition Law within the European Economic Constitution’, *Journal of Common Market Studies* 57, p. 129-130, 133.

46 Anna Gerbrandy (2018) ‘Conceptualizing Big Tech as “Modern Bigness” and its implications for European Competition Law’, Submission in reaction to the Call for Contributions – Shaping competition policy in the era of digitalization’, December (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3275235).

47 Niamh Dunne (2020) ‘Public Interest and EU Competition Law’, *The Antitrust Bulletin*, 26 March.

48 See for instance Katharina Hoelck’s analysis of the competition law case against Apple and international book publishers, in ‘EU Platform Regulation and its Impact on the Media and Communication Industry’ (2016), Paper presented at the 66th annual conference of the International Communication Association (ICA), Fukuoka, Japan.

49 Anna Gerbrandy (2018) ‘Modern Bigness’, p. 3.

50 Inge Graef, Damian Clifford and Peggy Valcke (2018) ‘Fairness and enforcement: Bridging competition, data protection, and consumer law’, *International Data Privacy Law* 8.

51 Bundeskartellamt (2019), Facebook B6-22/16, 6 February.

Fines as the cost of doing business

Under competition law, the European Commission has extensive powers to fine companies for anti-competitive conduct and order them to change their behaviour (remedies). In addition, the Commission can scrutinise proposed mergers, and block them if they would result in significant threats to competition.

However, the use of competition tools has not had the effects desired. To take one instructive example, over the past decade the Commission has issued three fines

for Alphabet, amounting to over €8 billion in total. The cases concerned Alphabet's use of its search algorithm to favour its own Google Shopping service and to block advertising from rival search engines, as well as the use of its Android operating system to push Google Search.⁵²

The Commission's antitrust actions against Alphabet have nevertheless failed to change the market structure and have not helped competitors suffering from Alphabet's anticompetitive behaviour.⁵³ Indeed, fines have not even worked as a deterrent, as Alphabet's market value has only increased.⁵⁴

Figure 4: In search of competition: Google Search's dominance

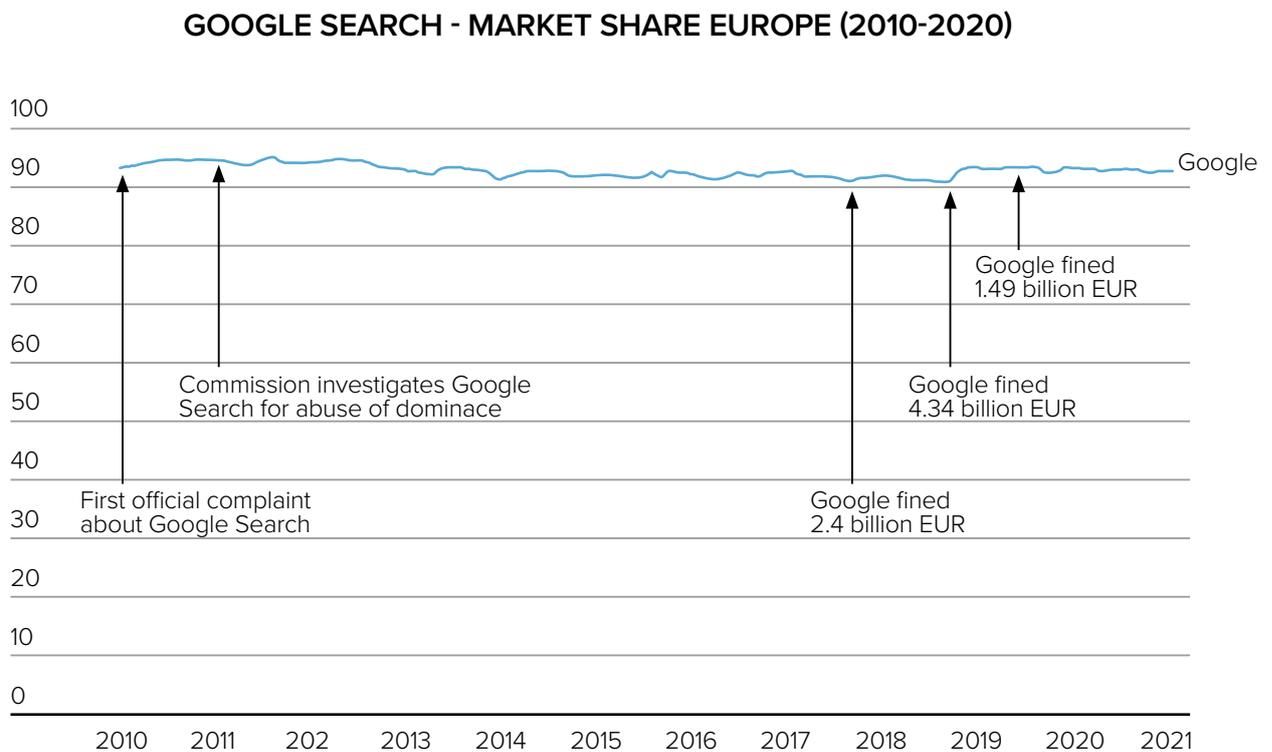


Chart: Author elaboration - Source: Statcounter GlobalStats - Created with Datawrapper

52 COMP/AT.39740 *Google Search (Shopping)*; COMP/AT.40099 *Google Android*; COMP/AT.40411 *Google Search (AdSense)*.

53 See the October 2020 figures (<https://gs.statcounter.com/search-engine-market-share/all/europe>). In Europe, the share of Google in online search is, and has consistently been, well over 90% over the past decade.

54 Nitasha Tiku (2019) 'The EU Hits Google With a Third Billion-Dollar Fine. So What?', *Wired*, 20 March (<https://www.wired.com/story/eu-hits-google-third-billion-dollar-fine-so-what/>).

THE EXISTING EU POLICY FRAMEWORK

A game of whack-a-mole

Competition policy proceeds via case-by-case investigations. Whereas the biggest platforms have very large resources, competition authorities have to decide carefully which cases to pursue, knowing that the current procedures and standards of legality make competition policy slow, resource-intensive and cumbersome. For instance, while the European Commission is still litigating the 2017 Google Shopping decision in court, one wonders how much time and how many resources it can dedicate to the many problems to which Google's dominance in online advertisement give rise,⁵⁵ or how much time and how many resources it can dedicate to scrutinising the complicated commitments linked to the merger between Google and Fitbit over the next 10 years.⁵⁶

Similarly, following the result of an inquiry into e-commerce markets in 2015, the European Commission has only just made a preliminary finding that Amazon is abusing its dominant position by using the business data of third-party traders on its platform, to favour its own retail business. At the same time, the European Commission opened a second investigation into Amazon for the company's suspected preferential treatment of its own retail offers.⁵⁷ Whilst digital platforms are rapidly expanding in variety of different markets and increase their market power, the European Commission is still heavily invested into investigating potential abuse that was flagged years ago.

In addition, when decisions are taken, and companies are ordered to change their conduct, the European Commission often lacks the resources or the expertise to ensure effective and timely compliance with its decisions and to ensure meaningful changes by the infringing party.⁵⁸

For instance:

- Microsoft took years before complying with a Commission decision from 2004 to provide interoperability information to competitors in the work group server market. This resulted in a fine in 2008, ten years after Sun Microsystems filed the official complaint. In addition, Microsoft dragged its feet for years before it stopped tying its Media Player to its Windows operating system, and it was finally fined in 2013 for failing to comply with commitments to stop tying its Internet Explorer web browser to Windows.⁵⁹ It is now under investigation again, this time for allegations that it is tying its Microsoft Teams software to its Office productivity software suite.⁶⁰ Many of the remedies have been of dubious effectiveness.⁶¹
- Google was allowed to design its own remedy as a follow up to the 2018 decision from the European Commission on Google's abuse of its Android operating system. However, two years later Google's implementation of the decision is still decried as ineffective.⁶² Furthermore, in the latest case against Google, for illegally strengthening its dominance in online advertising, even European Commission Vice-President Margrethe Vestager herself admitted that the decision had failed to restore competition.⁶³

In large part, authorities are dependent on the information possessed by the tech firm under investigation, and this leads to significant information asymmetries. For instance, in a comprehensive analysis of the ineffectiveness of the remedies provided by Google in the 'Shopping' case, it is noted that "despite ten years under investigation and

55 Competition and Markets Authority (2020) 'Online platforms and digital advertising', Market study final report, 1 July (https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf).

56 COMP/M.9660 *Google/Fitbit*.

57 European Commission (2020) 'Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices', Press release, 10 November.

58 European Court of Auditors (2020) 'The Commission's EU merger control and antitrust proceedings: A need to scale up market oversight', Special Report No 24/2020.

59 Euractiv (2013) 'EU fines Microsoft for breaking browser pledge', 6 March (<https://www.euractiv.com/section/digital/news/eu-fines-microsoft-for-breaking-browser-pledge/>).

60 Euronews (2020) 'Slack files competition complaint against Microsoft with European Commission', 22 July (www.euronews.com/2020/07/22/slack-files-competition-complaint-against-microsoft-with-european-commission).

61 See for instance Nicholas Economides and Ioannis Lianos, 'The quest for appropriate remedies in the EC Microsoft cases: a comparative appraisal', in Luca Rubini (ed.) (2010), *Microsoft on Trial. Legal and Economic Analysis of a Transatlantic Antitrust Case*, Cheltenham: Edward Elgar.

62 Natasha Lomas (2020) 'Google's "no choice" screen on Android isn't working, says Ecosia – querying the EU's approach to antitrust enforcement', *TechCrunch* 30 July (<https://techcrunch.com/2020/07/30/googles-no-choice-screen-on-android-isnt-working-says-ecasia-querying-the-eus-approach-to-antitrust-enforcement/>).

63 Natasha Lomas (2019) 'Europe's recharged antitrust chief makes her five-year pitch to be digital EVP', *TechCrunch* 8 October (<https://techcrunch.com/2019/10/08/europes-recharged-antitrust-chief-makes-her-five-year-pitch-to-be-digital-evp/>).

three prohibition decisions, it (Google) continues to prefer adhering to a three-pronged strategy of maintaining maximum non-transparency, maximum misrepresentation of both the facts and the law and an outright denial of any wrongdoing whatsoever.⁶⁴ The study concludes that in the three years since the compliance mechanism has been in operation, it has failed to improve market conditions for competing comparison shopping services” (...), “has further strengthened Google’s position on the national markets for CSSs (Comparison Shopping Services), and has entrenched its dominance in general search.”⁶⁵

Taking a broad view of the digital economy, one can only observe that the Commission’s efforts to preserve interoperability and prevent tying of different products have failed, as those practices have become the industry standard. For instance, Google is tying Chrome to its devices, Apple is tying its Safari web browser, and Samsung pre-installing its Samsung internet on its phones.⁶⁶ In other words, the anti-competitive conduct that the European Commission has been combatting since the early cases against Microsoft 20 years ago is becoming endemic as the power of online platforms grows.

Finally, although competition authorities are bogged down in ex post investigations of anti-competitive conduct, the current rules and enforcement priorities are not sufficiently attuned to preventing market concentration in the first place. According to the Furman review, “over the last 10 years the 5 largest firms have made over 400 acquisitions globally. None have been blocked and very few have had conditions attached to approval, in the UK or elsewhere, or even been scrutinised by competition authorities.”⁶⁷

BOX 4: MERGER CONTROL, ANYONE?

A few mergers, with large ramifications that competition authorities did not prevent:

- Facebook’s takeover of Instagram and WhatsApp, which cemented its dominance in social media and messaging;
- Alphabet’s acquisition of the video-sharing platform YouTube, the Google Maps competitor Waze, and the online ads platform DoubleClick.

Traditional tools in a digital economy

Apart from the difficulty of pursuing case-by-case assessments, there is also the question of whether existing competition policy’s analytical tools are still appropriate for the digital age. In response to the expanding concentration of power in the digital economy, competition authorities across the world have investigated their competition policy arsenals. Although there is no single feature that distinguishes digital from traditional markets, many reports highlight that digital markets feature a number of phenomena that together pose difficulties for the current competition paradigm.

Powerful digital platforms notably benefit from “strong network effects, economies of scale, economies of scope connected to the role of data as an input, extremely low marginal costs, and global scope.”⁶⁸ This does not necessarily lead to ‘natural monopolies’ – if it did, Alphabet would not feel compelled to pay Apple billions each year for preferential treatment of the Google Search engine. But it is the case that many digital markets have tipped in favour of one or two leading market players, which are subsequently difficult to displace. This is visible in online search, social networking, mobile operating systems, and online advertising.

64 Thomas Hoppner (2020) ‘Google’s (Non-) Compliance with the EU Shopping Decision’, *Competition Law in Practice*, pp. 33-34.

65 Ibid, p. 15.

66 Dirk Auer (2020) ‘On the Origin of Platforms. An Evolutionary Perspective’, *Truth on the Market*, 7 July.

67 ‘Unlocking digital competition’ (2019), Report of the Digital Competition Expert Panel, March, p. 12.

68 Filippo Lancieri and Patricia Morita Sakowski (2020), ‘Competition in Digital Markets: A Review of Expert Reports’, Stigler Center for the Study of the Economy and the State, Working Paper Series No. 3030, October, pp. 9-10.

THE EXISTING EU POLICY FRAMEWORK

In order to establish that a firm has abused its dominant position, competition authorities have to establish the alleged dominant market power in a well-defined market, which is no easy task - especially for online platforms, where multiple groups of users interact, often not with money but by submitting data, which complicates matters. In the words of Julie Cohen, “because platforms can define terms for each user group separately, pricing is not a reliable sign of market power (...).”⁶⁹

In addition, in the digital economy, vertical integration – the effort to control different aspects of a value chain - is endemic, but this has not historically been a priority for competition authorities. For instance, Amazon is vertically integrated and owns the eponymous e-commerce platform, but also sells its own products and handles the logistics. This gives Amazon clear incentives to favour its own services, to the detriment of competitors relying on Amazon’s platform. Furthermore, it has also been pointed out that market power does not reflect how online platforms are experienced by users, for whom there are often few alternatives to big social media platforms, for instance.⁷⁰

Evgeny Morozov may have had a point when he observed that competition policy could be summarised as “let’s have big tech firms swallow as much data as they can and apply competition law to how they design their websites”.⁷¹ There is evidence to suggest that data can be a crucial strategic resource in the digital economy, and the reluctance of Google and Facebook, for example, to share or give insight into the data that they have amassed, would confirm such a hypothesis.⁷² It has also been said that the competitiveness of firms will increasingly depend on timely access to relevant data.⁷³ And yet this is not well captured by the concept of market power. Indeed, the mainstream view within the competition law community is still to question the special nature of personal data, and to argue against the need for a fundamental rethink of competition policy.⁷⁴

While competition law could play an increased role in addressing concentrated power in the digital economy,

its emphasis on narrow economic interests over wider public policy concerns, case-by-case enforcement, and doctrinaire focus on concepts that are not always well-suited to the digital economy complicate this. Swift change is unlikely, as highlighted once again by the European Commission’s recent approval of the Google-Fitbit merger, which allows Google to extend its dominance into wearables and digital healthcare.⁷⁵

THE RULES: SECTOR-SPECIFIC VERSUS HORIZONTAL

Next to competition law, the EU has mainly relied on the rules of the e-Commerce Directive (ECD) of 2000 to regulate digital services. However, as online platforms’ power over social activity, public opinion and fundamental rights became more obvious, and problematic, the European Commission did review its policy in 2015. But it refrained from reforming the horizontal rules for digital services in the e-Commerce Directive (ECD). Instead, the Commission adopted a ‘problem-driven’ approach, which meant it looked at specific harms in a variety of sectors. This resulted in a variety of soft-law initiatives, and some legislation, for different types of online content. It is too early to evaluate these initiatives empirically – many just entered into force, or will do so shortly. And yet, it is clear that the approach lacks coherence and has resulted in a fragmented and complex set of rules that hinders enforcement. This benefits large platforms at the expense of smaller competitors, new entrants and citizens.

The e-Commerce Directive: a free pass for irresponsibility

Most of the digital services that are delivered on top of the physical infrastructure of the internet are covered by a horizontal set of basic rules in the Electronic Commerce Directive (e-Commerce Directive, or ECD) of

69 Julie Cohen, op cit, p. 174.

70 Orla Lynskey (2019) ‘Grappling with “Data Power”: Normative Nudges from Data Protection and Privacy’, *Theoretical Inquiries in Law* 20, pp. 193-194.

71 Evgeny Morozov (2017), ‘To tackle Google’s power, regulators have to go after its ownership of data’, *The Guardian* 2 July 2017 (<https://www.theguardian.com/technology/2017/jul/01/google-european-commission-fine-search-engines>).

72 Frank Pasquale (2013) ‘Privacy, Antitrust and Power’, *George Mason Law Review* 20, p. 1023.

73 Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer (2019) ‘Competition policy for the digital era’, European Commission, Directorate-General for Competition, p. 73.

74 Pablo Ibáñez Colomo and Gianni de Stefano (2019) ‘The Challenge of Digital Markets: First, Let Us Not Forget the Lessons Learnt Over the Year’, *Journal of European Competition Law & Practice* 9, pp. 485-486.

75 Francesca Bria (2020) ‘Europe must not rush Google-Fitbit deal’, *Politico*, 22 July. (<https://www.politico.eu/article/europe-must-not-rush-google-fitbit-deal-data-privacy/>).

2000. Originally, the ECD was developed with internet service providers in mind – providers that allowed access to the internet, and enabled people to publish websites, thus passive providers of hosting services.⁷⁶ At the time the ECD was developed, the business model of online services was still undecided, and the infrastructure for behavioural advertising was not in place. This also meant that providers had a mostly passive role, as they lacked the incentives to use traffic data and actively influence what and how people viewed content, to maximise advertising revenues. In addition, there was no possibility to filter infringing content at scale effectively.

In this context, the EU followed the US and adopted an accommodating set of rules that would encourage experimentation to occur, and that was based on the US's very strong free speech protection under the First Amendment of the Constitution.⁷⁷ For instance, the ECD holds that digital service providers should not be liable for the content that they transmit, store or host, as long as they act in a strictly passive manner.⁷⁸ In addition, the ECD provides that authorities cannot oblige platforms to monitor information they transmit or store, or to seek out signs of illegal activity. They only have to remove illegal activity once they become aware of it, for instance by being alerted by users or authorities.

But much has happened in the last 20 years, including the rise of social media, user-generated content platforms, cloud infrastructure and the powerful set of online platforms that often take an active role in shaping the user experience via algorithmic content selection, recommender systems and enriching third party content with or content or advertisement. In fact, platforms are already generally monitoring the content uploaded on their platforms, and influencing its reach, but for commercial purposes. And yet, they have no incentives – and cannot be required under the ECD – to do so in the public interest, for instance to actively combat child pornography

from being uploaded. As a result, right now, much illegal content, even evidently illegal material, stays online.

In addition, the prediction of US Law Professor Lawrence Lessig proved correct. He observed in 1996 that 'cyberspace' is highly susceptible to regulation, and that in the absence of democratic decisions about the design of this space, others would shape it according to their interests.⁷⁹ And indeed, this has come to pass. Because the ECD fundamentally promoted self-regulation by online platforms, the latter have become the de-facto regulators of online experience. Within their spheres of control, they act as public authorities, and they lay down the law in their terms of service, contractual arrangements.⁸⁰

Beating around the bush: self-regulation

In 2016, the EU decided to have another look at platform regulation, as it became clear the biggest platforms were having an increasingly important influence on public opinion, and were instrumental in a variety of societal harms, from mis- and disinformation, to hate speech, copyright breaches, and more. However, instead of updating the ECD, the legislation that gives platforms a free pass, the European Commission adopted a problem-driven approach, which entailed looking at specific harms, across a wide range of sectors.⁸¹

The European Commission mainly tried to nudge platforms into taking more responsibility for the content circulating on their platforms, via a variety of communications and self-regulatory codes of conduct. These non-binding initiatives have not been very effective, as it simply was not in the interest of large platforms to comply, a known ailment of self-regulation.⁸² In addition, in the absence of transparency, monitoring compliance is difficult for the relevant authorities.⁸³ For instance, a study into the code of practice on disinformation notes

76 Joris van Hoboken, João Pedro Quintais and Joost Poort (2018) 'Hosting intermediary services and illegal content online. An analysis of the scope of article 14 ECD in light of developments in the online service landscape', Report for the European Commission, Directorate-General Communications Networks, Content and Technology.

77 For the US's exceptional approach on free speech, see Frederik Schauer (2005) 'The exceptional first amendment', in Michael Ignatieff (ed) *American Exceptionalism and Human Rights*, Princeton: Princeton University Press.

78 Articles 12, 13 and 14 of Directive 2001/31/EC.

79 Lawrence Lessig (1999) *Code and Other Laws of Cyberspace*, Basic Books.

80 Julia Black and Andrew Murray (2019) 'Regulating AI and Machine Learning: Setting the Regulatory Agenda', *European Journal of Law and Technology* 10.

81 European Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe', COM (2016) 0288.

82 For an overview of weaknesses and risks, see OECD, 'Industry Self-Regulation: Role and Use in Supporting Consumer Interests', DSTI/CP (2014) 4/FINAL, pp. 20-21.

83 Melanie Smith (2020) 'Enforcement and cooperation between Member States. E-Commerce and the future Digital Services Act', Study requested by the IMCO Committee, April.

THE EXISTING EU POLICY FRAMEWORK

uneven implementation due to the lack of enforcement tools, and suggests that co-regulation be considered.⁸⁴ Given this lack of effective action, a number of member states implemented national frameworks with stricter measures in the area of illegal content, such as the Network Enforcement Act (NetzDG) in Germany.⁸⁵ By relying on self-regulation, instead of legislating the conditions and procedural guarantees under which illegal material should be taken down, private online platforms continued to decide on the circumstances in which citizens can exercise their fundamental rights online.⁸⁶

In addition, the approach of pushing platforms to deal proactively with illegal and harmful content is in fundamental tension with the limited liability regime and prohibition on general monitoring contained in the ECD. For instance, in a Communication of 2017, the European Commission demanded that platforms “adopt effective proactive measures to detect and remove illegal online content and not only limit themselves to reacting to notices which they receive.”⁸⁷ In the same document, the Commission also warmly supports the development and use of automatic detection and filtering techniques in the fight against illegal content online. On the face of it, such recommendations squarely contradict the hands-off approach laid down in the e-Commerce Directive.

Beyond soft law instruments, the EU also adopted a number of legal instruments, to ‘level the playing field’ and increase platforms’ responsibility for specific harms, such as copyright infringements or content harmful for minors. For example, it extended obligations from the Audiovisual Media Services Directive to ‘large video-sharing platforms’ such as YouTube, in order to protect minors, and it created new obligations for ‘online content-sharing service providers’, to make sure content on their platform respects copyright rules. In addition, it clarified that the consumer protection rules of the Unfair Commercial Practices Directive applied to platforms.

And yet, also here, the approach taken fundamentally clashes with the limited liability and prohibition on general monitoring contained in the ECD.

For instance, under the new copyright rules, platforms have to obtain prior agreements with copyright holders for copyrighted material shared on their platforms, or, failing that, make ‘best efforts to ensure their unavailability and prevent their future uploads’.⁸⁸ This can only be done via a filtering system, which contradicts the ban on general monitoring obligations of the ECD. Another contradiction can be spotted in the new rules on audiovisual media, which require platforms to take ‘appropriate measures’ to protect minors from harmful content, and everyone from hate speech, child pornography and more.⁸⁹ Finally, the reality of obligations under the Unfair Commercial Practices Directive, would also require platforms to take an active role in ensuring traders using their platform comply with relevant consumer and marketing requirements. It is difficult to see how they could do any of these things and still keep the liability exemption under the ECD.⁹⁰

A problem-driven approach: focusing on the trees, missing the forest

The European Commission’s 2016 problem-driven approach to platforms aimed to establish a ‘level playing field’, as it became clear that online platforms are competitors of many businesses in regulated sectors, without having to comply with similar sector-specific legislation.⁹¹ For instance, it is clear that both Facebook and Google reap the majority of advertisement spend online, whereas the media sector that creates quality content take less and less, whilst having to comply with strict rules and professional codes over how and what they can publish.

Nevertheless, the aim to establish ‘a level playing field’ has put the focus on tweaking laws in a variety of existing

84 Directorate-General for Communications Networks, Content and Technology (2020) ‘Study for the assessment of the implementation of the Code of Practice on Disinformation’, SMART 20190041, 8 May.

85 *Netzwerkdurchsetzungsgesetz* (German Network Enforcement Act), 2017.

86 Teresa Quintel and Carsten Ullrich (2019) ‘Self-Regulation of Fundamental Rights? The EU Code of Conduct on Hate Speech, Related Initiatives and Beyond’ in: Bilyana Petkova and Tuomas Ojanen (eds) *Fundamental Rights Protection Online. The Future Regulation Of Intermediaries*, Cheltenham: Edward Elgar Publishing.

87 European Commission, Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms’, COM (2017) 555, p. 10.

88 Directive (EU) 2019/790, Article 17.

89 Directive (EU) 2018/1808, Articles 28a and 28b.

90 Maria Lillà Montagnani (2019) ‘A New Liability Regime for Illegal Content in the Digital Single Market Strategy’, Bocconi Legal Studies Research Paper, No. 477007, June.

91 For the shift to the ‘level playing field’ as a regulatory principle, see Andrej Savin (2019) ‘Regulating Internet Platforms in the EU. The Emergence of the ‘Level Playing Field’, Copenhagen Business School Law Research Paper Series No. 19-02.

areas, and on symmetric rules that apply equally to all parties. This exactly obscures the dynamic and cross-cutting power of the biggest online platforms. As Professor Harold Feld observes, new communications technologies have often presented specific challenges, requiring specific rules: “armed with the knowledge of how we successfully (...) met these challenges in the age of the telegraph, the telephone, radio and television, we can now consider how to meet these challenges again in the age of broadband and social media.”⁹²

For instance, the revised rules for Audiovisual Media Services aim to ensure better protection of children online, by extending existing rules on media services to large online platforms such as YouTube and Instagram. However, the obligations to shield minors from harmful content and to protect their data are imposed on media service providers (likely to be individual YouTube channels), instead of on the video-sharing platforms themselves, such as YouTube, which have much more control over the data and design of the platform.⁹³ This may significantly undermine the effectiveness of rules to protect minors, while placing potentially onerous burdens on freelance content producers.

In 2016, the European Commission also proposed a new directive in the area of copyright.⁹⁴ While the overall aim of the directive was to create a fairer marketplace for online content, this may not actually be achieved. For example, the directive contains a new right for press publishers, to give them more leverage with regard to the large online services on which content is shared, and to ensure that some of the money from online distribution of content, flows back to those involved in creating it. But the new right has been criticised for favouring large established actors, in an already concentrated market. Adding another property right, and hence more complexity, is likely to make bargaining more costly, which hurts smaller players. Furthermore, similar rights were introduced in Spain and Germany, but have failed to improve the position of press publishers.⁹⁵

Beyond that, online platforms now have to uphold variety of different legal obligations and duties of care, with different authorities responsible for enforcement, and different procedural rules. For instance, there are different standards and requirements for terrorist content, content harmful to minors, child pornography, xenophobic content and copyright. There is a real risk that the plethora of soft law and legislation makes it unduly complex for smaller businesses and new entrants to navigate, and for authorities to enforce the law. The plea for sector specific rules also ignores that citizens and consumers have a legitimate expectation that largely, when dealing with the economy or the state, similar rules apply across sectors and activities. The call for better and more targeted rules, while at the same time criticising the “plethora” of rules, is also a key technique of platforms to undermine the credibility of the democratic process.⁹⁶

Moreover, the proliferation of norms in separate legal domains, runs counter to the integrated nature of the platform ecosystem, and to the long-observed trend of convergence of digital services and markets. As far back as 1997, the European Commission noted that the services covered by different rules on telecoms, audiovisual media and e-commerce were converging.⁹⁷ However, despite calls to simplify the regulatory framework, and to provide a more holistic set of rules for the digital environment⁹⁸, the recently adopted legislative acts do not seem to do much to address it.

BOX 5: CONVERGENCE OF DIGITAL SERVICES

A video can be shown as a television programme, subject to strict rules on audiovisual media services, or it can be streamed, to which only lighter e-commerce rules apply. Similarly, a text message (SMS) is subject to stricter rules than if the same message was sent via an internet service (WhatsApp, Facebook Messenger). The updates to the telecoms and media rules only address this to a limited extent.

92 Harold Feld (2020) ‘From the telegraph to Twitter: The case for the digital platform act’ *Computer Law & Security Review* 36.

93 Catalina Goanta ‘Children on Social Media. A Comparison of COPPA and the Revised AVMSD’, TTLF Working Papers, pp. 17-18 (forthcoming).

94 The European Commission’s proposal from 2016 became Directive (EU) 2019/790.

95 Open Letter, ‘Academics against Press Publishers’ Right: 169 European Academics warn against it’, 24 April 2018 (https://www.ivir.nl/publicaties/download/Academics_Against_Press_Publishers_Right.pdf).

96 Paul Nemitz and Matthias Pfeffer, ‘Prinzip Mensch – Macht, Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz’, 2020;

97 European Commission, ‘Green Paper on the Convergence of the Telecommunications, Media and Information Technology Sectors, and the Implications for Regulation. Towards an Information Society Approach’, COM(97)623.

98 Alexandre De Streel and Pierre Larouche (2016) ‘An Integrated Regulatory Framework for Digital Networks and Services’, CERRE Policy Report, 27 January.

THE EXISTING EU POLICY FRAMEWORK

Figure 5: Of platforms, intermediaries, online marketplaces and more: recent laws affecting platforms

AREA	LAW	DEFINITIONS AFFECTING ONLINE PLATFORMS	APPLICATION DATE
LAWS RECENTLY ADOPTED			
Data protection	General Data Protection Regulation (Regulation 2016/679)	Data processor Data controller	May 2018
Cybersecurity	Directive on Security of Network and Information Systems (Regulation 2016/1148)	Digital service (online marketplace, search engine, cloud computing)	May 2018
Internal market	Geo-blocking Regulation (Regulation 2018/302)	Electronically supplied service	December 2018
Internal market / competition	Platforms-to-Business Regulation (Regulation 2019/1150)	Online intermediary service Online search engine	July 2020
Content	Audiovisual Media Services Directive (Directive 2018/1808)	Video-sharing platform service	September 2020
Telecoms	European Electronic Communications Code (Directive 2018/1972)	Number-based independent interpersonal communications service Number-independent interpersonal communications service	December 2020
Copyright	Copyright in the Digital Single Market Directive (Directive 2019/790)	Online content-sharing service provider Information society service provider	June 2021
Consumer protection	Directive contracts for digital content and services (Directive 2019/770)	Digital service Digital content	January 2022
Consumer protection	Directive on enforcement of consumer protection (Directive 2019/2161)	Online marketplace	May 2022
LAWS STILL BEING NEGOTIATED			
Telecoms/data protection	E-Privacy Regulation (COM(2017)010)	Electronic communications network	
Content	Terrorist Content Regulation (COM(2018)640)	Hosting service provider	
Cybersecurity	Directive on a high common level of cybersecurity (COM(2020)823)	Cloud computing service provider	
		Data centre service provider	
		Online marketplace	
		Social networking services platform	
		Content delivery network provider	
		Public electronic communications network provider	
Content / consumer protection	Digital Services Act (COM(2020)825)	Intermediary service	
		Hosting service provider	
		Online platform	
		Very large online platform	
Internal market / competition	Digital Markets Act (COM(2020)842)	Core platform service	
		Gatekeeper	

If the EU wants to hold platforms more accountable, it should update the horizontal rules of the e-Commerce Directive, in a way that takes the power of large platforms seriously, and which recognises the influence they have over the information environment. This amounts to what some have called digital constitutionalism; that is, making sure that the rule of law applies in the public sphere that large online platforms oversee, instead of private law.⁹⁹

A NOTE ON ENFORCEMENT: THE GENERAL DATA PROTECTION REGULATION

The operations and business models of large online platforms span a variety of sectors, and they are present across the EU. As a result, they fall under the responsibility of a variety of different regulators, from competition authorities and media regulators, to data protection authorities, consumer law agencies and telecoms regulators. What's more, these regulatory domains themselves have a decentral model of enforcement, in which each of the 27 national authorities largely act independently. This is problematic, as national authorities have vastly different resources and capacities to enforce the law, as well as different attitudes. In such a web of overlapping enforcement responsibilities, it is more challenging for authorities to decide when they are competent or best placed to act.¹⁰⁰

In addition, in a decentral enforcement system, firms have an incentive to move their headquarters to the Member State with the most lenient implementing legislation and enforcement model. For digital affairs this is Ireland, which is now home to Apple, Twitter, Google, Facebook, LinkedIn, Airbnb, Uber, Microsoft, and Salesforce, for instance.¹⁰¹ These are all globally operating technology firms with vast resources.

As a result, there are enforcement bottlenecks within the EU. While this is happening in a number of areas, the most glaring lack of enforcement is probably in the field of the General Data Protection Regulation (GDPR). Although the GDPR requires the minimisation of personal data and makes

the processing of personal data illegal unless specific conditions apply, these requirements seem to be routinely infringed without consequences. If the GDPR would be properly enforced, it could play a powerful role in addressing abusive behaviour of the largest online gatekeepers.

Cultural factors, institutional deficiencies, and resources gaps

Concerning the GDPR, there is a widespread culture among enforcement agencies to refrain from using existing capacity to effectively enforce the law. For instance, when evaluating her record in 2017, the UK Information Commissioner stated:

“Issuing fines has always been and will continue to be, a last resort. Last year (2016/2017) we concluded 17,300 cases. I can tell you that 16 of them resulted in fines for the organisation concerned.”¹⁰²

As David Erdos explains,¹⁰³ this translates into a fine in less than one in a thousand cases and leaves many data subjects essentially without recourse when their data protection rights are infringed. This effective lack of recourse is incomprehensible, given the widespread non-compliance that continues to be observed. To give one example from among many, websites regularly share sensitive data about medical diagnoses, drugs and symptoms with firms across the globe. This often clearly violates the GDPR.¹⁰⁴

This is problematic, because the EU opted for a decentral model of enforcement, in which countries with the most lenient enforcement attitudes also tend to have the biggest enforcement responsibilities. The enforcement of the data protection rules is in the hands of the data protection authorities where a firm is established. In the case of big online platforms, that is mainly Ireland and Luxembourg, exactly because they are known to have lenient enforcement regimes. As a result, although the authorities of these two member states have comparatively few resources, they are nevertheless responsible for ensuring that the data of hundreds of millions of European citizens is protected, vis-à-vis global tech firms. That is a glaring mismatch. Data Protection

99 Nicolas Suzor (2018) 'Digital Constitutionalism. Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms', *Social Media & Society* 4.

100 Jonathan Lewallen (2020) 'Emerging technologies and problem definition uncertainty: The case of cybersecurity', *Regulation & Governance*.

101 Melanie Smith, op cit, p. 22.

102 Information Commissioner's Office (2017) 'Blog: GDPR – sorting the fact from the fiction', 9 August (<https://ico.org.uk/about-the-ico/news-and-events/blog-gdpr-sorting-the-fact-from-the-fiction/>).

103 David Erdos (2020) 'A-contextual and Ineffective? Reviewing the GDPR Two Years On – David Erdos', *Inform's Blog*, 5 May (<https://inform.org/2020/05/05/acontextual-and-ineffective-reviewing-the-gdpr-two-years-on-david-erdos/>).

104 Privacy International (2019), 'Your Mental Health on Sale. How Websites about Depression share Data with Advertisers and leak Depression Test Results', 3 September.

THE EXISTING EU POLICY FRAMEWORK

Authorities can take interim and urgent measures, if the competent authorities that are primarily responsible do not act; but so far this possibility has not been used.¹⁰⁵

The GDPR does require a form of coordination among the 27 national supervisory authorities and the European Data Protection Supervisor (EDPS), and created a specific institution for that: The European Data Protection Board (EDPB). The latter can issue guidelines to help interpret provisions of the GDPR, and it is also competent to take binding decisions in disputes about the cross-border processing of personal data, to make sure the rules are applied in a consistent manner across the EU. However, it cannot step in to take over cases from national authorities that do not enforce the rules. This is a significant difference with the EU competition rules for instance, where the European Commission does indeed have such powers over national authorities.

Finally, many data protection authorities lack the resources to carry out all the tasks they have been asked to fulfil. Indeed, it has been reported that half the data protection authorities in the EU operate with a budget of less than €5 million. A report from the European Data Protection Board notes that “although the majority of the 17 replying supervisory authorities stated that they would need an increase in the budget of 30-50%, almost none received the requested amount. There are some extreme examples where this need is close to or even 100%.”¹⁰⁶

These observations are important, because there is a claim that the GDPR has further entrenched the position of large data giants and raised barriers to entry for new firms, restricting the possibilities for data synergies. It has been argued that the disincentives that the GDPR places on collecting and combining data from different sources mean that new entrants may find it difficult to compete with big tech firms that have already amassed large quantities of data.¹⁰⁷ Meanwhile, the role still played by individual consent does not acknowledge the power differentials between large online platforms and individual users.¹⁰⁸

These claims, however, ignore that so far large platforms have benefitted from an underenforcement of data protection rules. They have gained market power largely with business models which under old and now EU data protection rules were illegal. Therefore, stronger enforcement, in the first place against the major collectors and processors of data, would help to reduce the powerful position these operators have gained with illegal business models. If anything, the legislation came too late, effectively regulating a good decade after firms had been collecting personal data, and thus meaning that new entrants are now at a disadvantage. When an entire business model and infrastructure has been created around the collection of personal data, it is very difficult to change track.

BOX 6: UK'S INFORMATION COMMISSIONER'S OFFICE ADTECH INVESTIGATION

“The profiles created about individuals are extremely detailed and are repeatedly shared among hundreds of organisations for any one bid request, all without the individuals’ knowledge”¹⁰⁹ In a 2019 report on online advertisement, the UK data protection authority finds the system revolves around illegal use of personal data. And yet, no enforcement action has been taken as a result.

Finally, enforcement does not sufficiently recognise the importance of scale. Many infringements of citizens’ privacy and autonomy are caused by powerful online platforms, which impose high switching costs by complicating data portability and preventing interoperability with other services, and which have been involved in numerous data leaks and abuses. A multitude of data-driven harms revolve around the influencing of groups, based on aggregated data, and this is easily possible when the data are held by a select few firms.¹¹⁰ In other words, harm often increases with scale, and this should inform an enforcement strategy that prioritises big operators.

105 European Commission (2020) ‘Staff Working Document accompanying the Communication ‘Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition. Two years of application of the General Data Protection Regulation’, SWD/2020/115.

106 European Data Protection Board (2019) ‘First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities’, 26 February (https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf), p. 7.

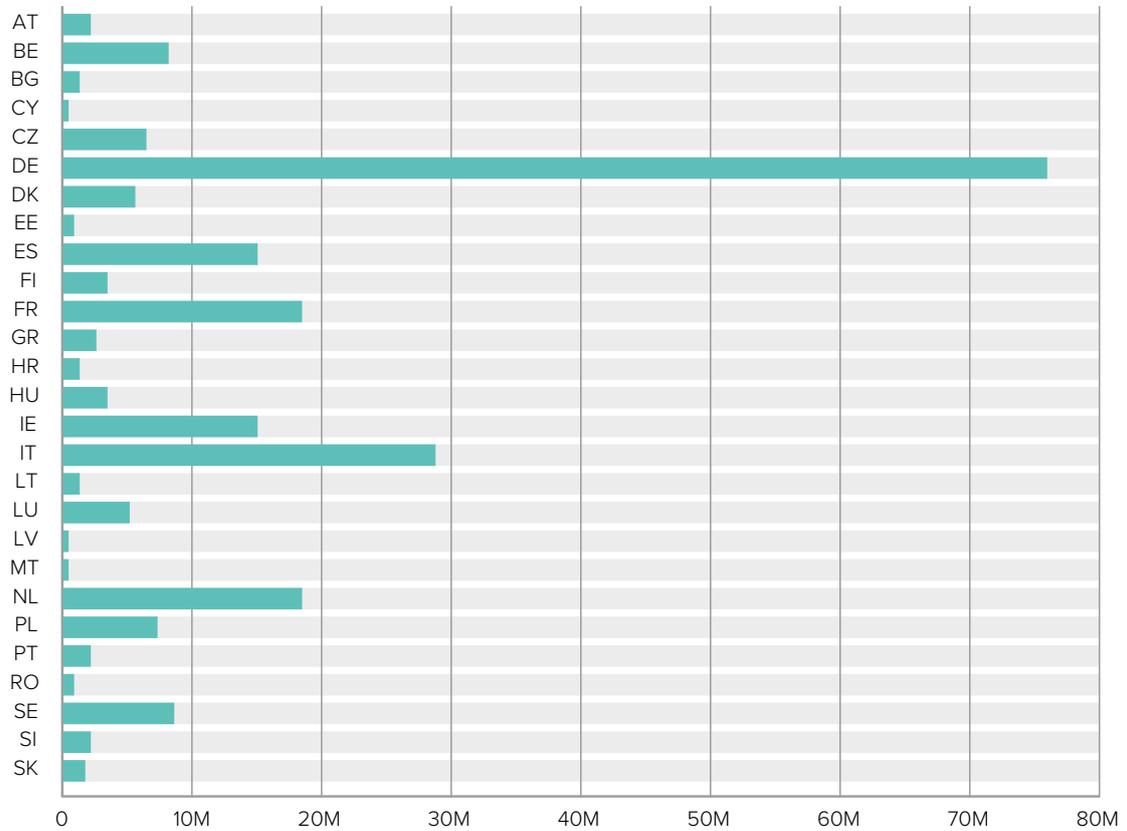
107 Michal S. Gal and Oshrit Aviv, ‘The Competitive Effects of the GDPR’, *Journal of Competition and Economics* (forthcoming).

108 Elettra Bietti, ‘Consent as a Free Pass: Platform Power and the Limits of the Informational Turn’, *Pace Law Review* 40.

109 Information Commissioner’s Office (2019) ‘Update report into adtech and real time bidding’, 20 June (<https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf>), p. 23.

110 Michal S. Gal (2020) ‘Competitive effects of the GDPR’, p. 33; Martin Tisné (2020) ‘The Data Delusion: Protecting Individual Data Isn’t Enough When The Harm is Collective’, Cyber Policy Center Stanford University, July ([see here](#)).

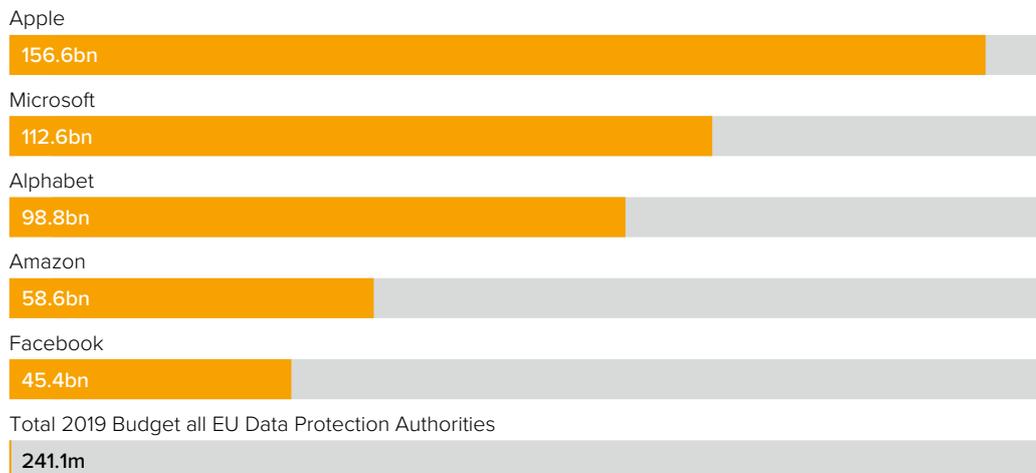
Figure 6: Budget differences EU Data Protection Authorities



European Data Protection Authorities' budgets for 2019

Chart: Elaboration by author - Source: European Commission Staff Working Document SWD/2020/115

Figure 7: Big tech firms' cash on hand versus Data Protection Authorities' resources



Microsoft's figure is based on Q1 2020; Facebook's figure is based on Q3 2020

Chart: author elaboration - Source: The companies' quarterly financial statements

GATEKEEPERS: AN AGENDA

THE INTERNET AS INFRASTRUCTURE

The Covid-19 crisis once again underlined that large platforms function as essential social and economic infrastructure. Online retailers find it difficult to avoid Amazon, citizens find it difficult to avoid Facebook's social media ecosystem, and everyone relies on Google to find and be found online.

As previous sections showed, a direct line can be drawn from the late 90s onwards, and the profoundly ambivalent place the Internet has become today. Therefore, the EU should not resign itself to today's situation, in which a handful of firms sets the rules online, but it should invest in creating online public spaces and new institutions, that operate on a logic that differs from data collection, behavioural advertisements, and their corrosive consequences. Technology is unlikely to increase equality, freedom and democracy in the absence of strong institutions and collective action.

For communication and information technologies of the past, such as broadcast TV, postal services and books, public authorities have acted, not just by setting rules, nor by just breaking up firms (although they did that too), but also via investment and the creation of new institutions; such as the BBC, national postal operators, and public libraries, to provide an essential public service. Today, this could for instance take the shape of a European TV streaming platform, with political news and documentaries from broadcasters and other media, in a common search platform and with automatic subtitling in all EU languages.

BOX 7: EU INVESTMENTS IN DIGITAL

In her State of the Union speech, European Commission President Ursula Von Der Leyen announced, and European leaders endorsed, that 20% of the Next Generation EU recovery and resilience fund of €750 billion should be spent on 'digital'. This amounts to roughly €150 billion. In addition, the EU's longer-term budget for 2021-2027 foresees €132,8 billion under the header 'single market, innovation and digital'. The opportunity should not be wasted by spending it all on fragmented local projects across the EU. What is the long-term mission here?

In addition, the EU should facilitate the emergence of alternative online business models that are not dependent on surveillance. Of course, digital infrastructure is material, and it costs time and money to construct and maintain it. The same holds true for the creation of quality content. That said, the current advertisement-based system is not free. Citizens are paying with their privacy, their time and their effort. It is therefore time to discuss and weigh the different trade-offs, and to make room for different business models that have fewer external costs for local communities, citizens, workers and democracy. There are efforts underway to create new ways to monetise content online, without having to rely on intermediaries such as payment platforms.¹¹¹

To make space for alternatives, and for civil society, it is important the EU specifically takes this into account in its digital policy. For instance, the European Commission should assess potential impacts of proposed legislation on existing power structures. Is the legislation more amenable to contesting and reducing the power of these structures, or does it lock this power in? Are new business models, such as those of non-profit-making organisations, taken into account?

¹¹¹ TechCrunch (2019) '\$100M Grant for the Web fund aims to jump-start a new way to pay online', 16 September (<https://techcrunch.com/2019/09/16/100m-grant-for-the-web-fund-aims-to-jump-start-a-new-way-to-pay-online/>).

BOX 8: COST OF SURVEILLANCE

According to Brave, “the average mobile browser user pays as much as 23 USD per month in data charges to download ads and trackers. That’s 276 USD a year.”¹¹² Even if the costs in an EU context were a fraction of that, it would still amount to billions of euros per year.

Having a debate on the values that our digital ecosystem should reflect is important, because the surveillance logic pushed by big platforms is spreading to a variety of sectors, while the resulting toxicity of the public sphere undermines EU democracies’ capacity to come to an informed consensus on the way forward.

BOX 9: ALTERNATIVE WEB ARCHITECTURE

Inventor of the World Wide Web, Tim Berners-Lee, aims to promote a new architecture for the web, Solid, which would allow users to remain in control over their data. He is concerned that powerful technology companies have subverted the open and collaborative nature of the web, and he plans to restore it.¹¹³

GATEKEEPERS: SIMPLE AND ASYMMETRICAL RULES

Given the crucial role played by big platforms in today’s online environment, there is much to applaud in the EU’s plans for a special regulatory regime for online gatekeepers. Regulatory efforts should be directed to their proper target – the firms that control the online experience of citizens and businesses, and whose actions have society-wide effects.

Under EU competition law, dominant companies already have a special responsibility not to distort competition, and recent updates on copyright and audiovisual media rules also acknowledge that scale matters. This principle

of asymmetrical regulation should be embraced and be made the cornerstone of a new ex ante regulatory regime for online gatekeepers. Such a public law framework would also avoid compliance burdens on small firms, which would risk further widening power differentials. Any precise threshold for defining gatekeepers is necessarily arbitrary, therefore the EU could combine multiple criteria, from the number of monthly active users and the ability to lock them in, to financial strength. This should prevent a too mechanistic assessment. In any event, the definition should not be based primarily on a calculation of market share.

Any new law should include rules that limit the widespread anticompetitive practices gatekeepers use to favour their own products and services, such as self-preferencing, tying, bundling, and the strategic use of competitors’ data. Next to regulating gatekeepers’ behaviour, the EU should have the capacity to intervene in markets to address the sources of gatekeepers’ power in existing markets, like social media and digital advertising, and new and emerging markets that risk being monopolised. This would entail the possibility to require gatekeepers to share certain types of data, or to ensure interoperability.

Most importantly, any new regime will only be successful if it provides for a dedicated, strong and central enforcement regime, tailored to the size and dynamics of the biggest online platforms. In 2019, a leaked note from the European Commission stated that there is “no dedicated ‘platform regulator’ in the EU, which could exercise effective oversight and enforcement, in areas such as content moderation and advertisement transparency.” It also noted that “many of the existing regulators lack the digital capacities to interface with online platforms today.” It then concluded that “besides the costly, slow and potentially contradictory oversight exercised by different sectoral regulators, one consequence is that many public interest decisions that should be taken by independent public authorities are now delegated to online platforms, without adequate and necessary oversight.”¹¹⁴ This echoes the assessment made by the UK House of Lords, which called for a new UK body, the ‘Digital Authority’, to co-ordinate regulators in the digital world.¹¹⁵

112 As cited in Maurice E. Stucke and Ariel Ezrachi (2020) *Competition Overdose. How Free Market Mythology Transformed Us from Citizen Kings to Market Servants*, New York: HarperCollins.

113 Financial Times (2020) ‘NHS signs up for Tim Berners-Lee pilot to reinvent web’, 9 November (<https://www.ft.com/content/01480644-3ca3-486e-907d-4abf8aac1719>).

114 European Commission (2019) DG CNECT, note on the regulation of online platforms (<https://cdn.netzpolitik.org/wp-upload/2019/07/Digital-Services-Act-note-DG-Connect-June-2019.pdf>).

115 House of Lords (2019), Select Committee on Communications, ‘Regulating in a digital world’, 9 March ([see here](#)).

GATEKEEPERS: AN AGENDA

When imposing data sharing or interoperability requirements on gatekeepers, there are risks and trade-offs involved, relating to innovation, data protection and cybersecurity.¹¹⁶ It is therefore important that the competent regulator has the broad mandate, the expertise and access to the relevant information, to make informed judgments that take the different values into account. This is also an additional reason why the legal framework should not just have the aim to promote competition, but also reflect wider concerns around fundamental rights, and consumer protection, which are all inevitably at stake.

BOX 10: INTEROPERABILITY BETWEEN SOCIAL MEDIA

The UK Competition and Markets Authority thinks Facebook should be required to offer at least a limited form of interoperability, by allowing users to invite their Facebook friends to join other social media, and by enabling users to share content from other apps on Facebook.¹¹⁷

Alternatively, there have been suggestions to create stronger cooperation between existing regulators across sectors in order to address the increasing overlap of laws that are relevant for online platforms.¹¹⁸ There are indeed signs that national enforcement authorities are looking beyond their sectorial legislation, but coherent enforcement is still lacking.¹¹⁹ Such joined-up enforcement across sectors could take the form of a meta-regulator that could bring together different networks to facilitate coordinated action. This meta-regulator would consist of a pool of experts, and also a set of procedures that would enable not just networking or coordination, but joint decision-taking between different groups of national and regional regulators.¹²⁰

CONTENT, INFORMATION AND DEMOCRACY

Fundamentally, the EU should not accept that a few private firms have such power to shape public opinion. However, right now, the EU should acknowledge that large platforms have created an automated public sphere, and via their terms of service, they determine how citizens exercise their rights online. To make sure platforms at least do so responsibly, the EU should significantly reform the laissez-faire approach it has taken so far in the e-Commerce Directive, and provide coherence in relation to the different laws it has adopted for different types of illegal content. The new rules should provide a simple set of rules to ensure that the largest content intermediaries operate their platforms in accordance with the rule of law and fundamental rights.

It is clear that many large platforms, such as Facebook and YouTube, use content recognition systems to determine what users post and audiences watch, for commercial purposes. When these platforms do so, it is not unreasonable to demand that they also use these systems in the public interest. More specifically, this would mean that for clearly, evidently and on first sight criminal content, such as child pornography and terrorist content, the biggest online platforms – with a gatekeeping function over the public sphere – should take it down proactively and automatically, without first requiring a notice by a third party or a court. Such automated systems are not perfect, and automated removal of this type of content should therefore always be subject to human review.¹²¹

To be clear, this would not involve new upload filters, but requiring firms that already use them for commercial purposes, to use them in the strong public interest of protecting children and not to have the public discourse poisoned by evidently criminal content. The emphasis here is on “evidently”, meaning that in case of doubt, platforms would not be obliged to take down. While in relation to copyright, there is an incentive of

116 See for instance Ian Brown (2020) ‘Interoperability as a tool for competition regulation’, OpenForum Academy (https://openforumeurope.org/wp-content/uploads/2020/11/Ian_Brown_Interoperability_for_competition_regulation.pdf).

117 Competition and Markets Authority (2020) ‘Online platforms and digital advertising’, Market Study final report, 1 July.

118 Catalina Goanta notes the duplications between the Audiovisual Media Services Directive and the Unfair Commercial Practices Directive, in ‘Children on Social Media. A Comparison of COPPA and the Revised AVMSD’, TTLF Working Papers, pp. 13-14 (forthcoming).

119 Inge Graef, Damian Clifford and Peggy Valcke (2018) ‘Fairness and enforcement: bridging competition, data protection, and consumer law’, *International Data Privacy Law* 8, pp. 200-223.

120 Ben Wagner and Carolina Ferro (2020) ‘Governance of Digitalization in Europe. A Contribution to the Exploration Shaping Digital Policy – Towards a Fair Digital Society?’, Bertelsmann Stiftung, May.

121 For an overview of risks, see Robert Gorwa, Reuben Binns and Christian Katzenbach (2020) ‘Algorithmic content moderation: Technical and political challenges in the automation of platform governance’, *Big Data & Society* 7.

platforms to take down too much of allegedly illegal content, given that platforms earn billions from the advertising of content holders in music and film, such incentives are not present for speech that is not clearly

criminal. After all, the business model of platforms thrives on outrage and aggression, and aggressive speech below the level of threats to a person, libel and hate speech, is not illegal.

Figure 8: Facebook already monitors and tags pictures uploaded to its platform



Photo: Shutterstock

To avoid strengthening large platforms' power over how citizens exercise the freedom of speech, the latter should be able to contest any removal decision, at an independent dispute settlement body, financed by the online platforms. The EU should stipulate in a law the key procedural guarantees and procedural aspects of notifications of illegal content and their removal, with a keen eye for the different size of the actors involved. This should preferably be regulated in the form of a regulation, to avoid fragmentation across the EU.

In addition, the EU should require much more transparency in online advertising markets and enable independent research to be carried out. If the sceptics of the effectiveness of behavioural advertisements are right, then the bubble will be exposed for what it is, and burst, forcing a transition to different business models. Alternatively, if research shows that programmatic advertisements are effective, this knowledge could pave the way for stricter measures, such as the outright restriction of behavioural advertising. In any case, it is clear that the personalised

advertisement industry depends on large-scale infringements of the General Data Protection Regulation (GDPR). By strengthening the GDPR's enforcement, authorities can speed up the transition to different online business models.

In previous times of crisis, induced by new media technologies like the radio and broadcast television, legislatures reacted by funding new sources of quality media, and creating media ownership laws to make sure existing media monopolies would not extend their dominance over the new media.¹²² This is an important avenue that the EU should explore. In Germany, the Interstate Media Treaty that was approved in December 2019 contains interesting elements in this direction. For instance, it requires more transparency from the algorithms used by social media platforms, and can put conditions on their operation to ensure that journalistic content is visible. In addition, an advisory report to the European Commission back in 2019 already suggested that online platforms that curate and recommend content based on algorithms should also be obliged to show content in the public interest.¹²³

122 Chris Marsden, Trisha Meyer and Ian Brown (2020) 'Platform values and democratic elections: How can the law regulate digital disinformation?', *Computer Law & Security Review* 36.

123 Guillaume Klossa (2019) 'Towards European Media Sovereignty. An Industrial Media Strategy to leverage Data, Algorithms and Artificial Intelligence', Report by Guillaume Klossa, special adviser to European Commission Vice-President Andrus Ansip, p. 74.

REPORT PUBLISHED IN JANUARY 2021 BY:

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES



FUNDACIÓN
PABLO IGLESIAS



FRIEDRICH
EBERT
STIFTUNG

Copyright © 2021 by FEPS