

REPORT

—
June 2021

Jan Krämer
Richard Feasey

DEVICE NEUTRALITY

**OPENNESS, NON-DISCRIMINATION AND
TRANSPARENCY ON MOBILE DEVICES FOR
GENERAL INTERNET ACCESS**



The project, within the framework of which this report has been prepared, was supported by the following members of CERRE: ARCEP, BIPT, Bakom, Facebook, Huawei, and Qualcomm. However, they bear no responsibility for the contents of this report. The views expressed in it are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, these views do not necessarily correspond either to those of CERRE, or of any sponsor or of any other member of CERRE. As provided for in CERRE's by-laws and in the procedural rules from its "Transparency & Independence Policy", this report has been prepared in strict academic independence.

© Copyright 2021, Centre on Regulation in Europe (CERRE)

info@cerre.eu

www.cerre.eu

Table of contents

About CERRE	4
About the authors	5
Executive summary	6
1 Introduction	11
2 The internet access value chain	15
2.1 Layers of the internet access value chain	15
2.2 Interfaces and standards connecting the layers	18
3 Possible device neutrality issues along the internet access value chain	21
3.1 Smartphones and the termination monopoly	21
3.1.1 Smartphones as key devices for general internet access	21
3.1.2 Termination monopolies: Ex-post market power in ex-ante competitive markets	22
3.2 The hardware layer	23
3.2.1 Market overview	23
3.2.2 Possible issues.....	24
3.3 Issues at the operating system layer	25
3.3.1 Market overview	25
3.3.2 Possible issues.....	28
3.3.3 Application discovery layer	31
3.3.4 Application layer	37
3.4 Overview of conduct concerns	37
4 Arguments to justify 'non-neutral' conduct	40
4.1 Innovation and investment	40
4.2 Security and privacy	43
4.3 Harmful content	43
5 Policy recommendations.....	46
5.1 Key objective: Ensuring alternative routes to content for consumers	46
5.2 Interventions at the Operating System Layer	49
5.2.1 Enabling side-loading of apps.....	49
5.2.2 De-installation and user consent for pre-installed apps	50
5.2.3 Transparency about APIs and Monitoring of Standards.....	52
5.2.4 Data portability for devices	53
5.3 Interventions at the Application Discovery Layer.....	55
5.3.1 Enabling alternative app stores	55
5.3.2 Unbundling of the dominant app store for compatible operating systems.....	57
5.3.3 No self-preferencing in browsers and app stores.....	58
5.3.4 Transparency and redress mechanisms for dominant app stores.....	60
5.4 Interventions at the Hardware Layer	61
6 Conclusions	62



About CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation in Europe's network and digital industries. CERRE's members are regulatory authorities and operators in those industries as well as universities.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to network industries and the markets for their services.

CERRE's activities include contributions to the development of norms, standards and policy recommendations related to the regulation of service providers, to the specification of market rules and to improvements in the management of infrastructure in a changing political, economic, technological and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments and regulatory authorities, as well as at strengthening the expertise of the latter, since in many Member States, regulators are part of a relatively recent profession.

About the authors



Jan Krämer is a CERRE Academic Co-Director and Professor for Information Systems at the University of Passau, Germany, where he holds the Chair for Internet & Telecommunications Business. He has a diploma degree in Business Engineering and Management, and a Ph.D. in Economics, both from the Karlsruhe Institute of Technology. He has published numerous articles in the leading journals in the areas of Information Systems, Economics and Marketing. His current research interests include the regulation of telecommunications and internet markets, as well as digital ecosystems and data-driven business models.



Richard Feasey is a CERRE Senior Adviser, an Inquiry Chair at the UK's Competition and Markets Authority and Member of the National Infrastructure Commission for Wales. He lectures at University College and Kings College London and the Judge Business School. He has previously been an adviser to the UK Payments Systems Regulator, the House of Lords EU Sub-Committee and to various international legal and economic advisory firms. He was Director of Public Policy for Vodafone plc between 2001 and 2013.



Executive summary

Two decades after the net neutrality debate started, the internet ecosystem has evolved and additional gatekeepers have emerged. In order to access content from content and service providers (CSPs), consumers have to pass through a whole internet access value chain, comprised of broadband providers, device manufacturers and online platforms. Today online platforms, such as search engines, online marketplaces and other online intermediation services also play an important role in the consumer's discovery and choice of CSPs. Likewise, devices (such as smartphones and connected speakers) and the software (such as operating systems and apps) that runs (or does not run) on them can significantly impact the consumer's access to and choice of online services. In this report, we discuss whether, **'openness', 'non-discrimination' and 'transparency'**, which are the key pillars of net neutrality regulation, should be regulatory principles that also apply at other layers of the internet access value chain and specifically to certain types of devices. The issue of device neutrality has been put to the forefront of the policy debate by ARCEP, the French telecoms regulator, who argued that devices through which services and content on the internet are accessed (e.g., smartphones, tablets, connected speakers) and their associated mobile operating systems are a remaining "weak link" to ensure an "open internet".


In the era of the internet of Things (IoT) more and more devices are connected to the internet, and hence there exists a large diversity with respect to what the specific purpose of these devices are and should be. We therefore see a difference between internet-enabled devices (e.g., smart kitchen appliances, smart toys, light bulbs, cars, etc.) and general internet access devices (smartphones, tablets, laptops, etc.), while noting that some grey zones may exist (e.g., smart TVs, smart speakers with screens, smart watches). This report **focuses on smartphones** as the key personal device for internet access. Smartphones are multi-purpose devices that can – in terms of internet access – replace most others. Indeed, most consumers will not solely rely on internet-enabled devices for accessing services on the internet, but they may well rely on a smartphone to do so. Moreover, smartphones are the devices that are closest and personal to the consumers, being with them at all times. This also means that for many applications, smartphones are consumers' first choice for accessing the internet.

Unlike net neutrality, where the gatekeeper control is exercised over the physical connection by the broadband provider, **the exercise of 'gatekeeper control' in devices can apply at many different layers of the value chain.** We distinguish between three main building blocks of the internet access value chain, comprising:

- (1) online content (located on remote servers),
- (2) the network (i.e., the connection between the remote server and the consumer's device),
- (3) the device.

Each building block comprises several layers or links again. The key insight here is that there are many complementary building blocks that establish the link between a consumer and content online. Each layer in isolation is not providing value, unless it is interacting with the other layers. Content has to pass through several (but not necessarily all) of these layers to reach the consumer, and the different layers depend on each other. Net neutrality only regulates a small portion of this value chain, namely the internet service provider's final network connection to the consumer.

Devices constitute a termination monopoly and thus establish market power at the device level, even if the market for devices is competitive. The main competitive bottlenecks are seen at the operating system layer and the application discovery layer, however. The latter is constituted by browsers and app stores, each of which are special applications in the sense that they are themselves the gateway for consumers to access other content or apps. The operating system layer and the application discovery layer are also characterised by strong indirect network effects, which implies a strong market concentration. Hence, for each of mobile operating systems, app stores and browsers, *de facto* only two major players exist in Europe. By contrast the market for hardware (without software or operating system) is not characterised by network effects and remains competitive.



While a number of issues may arise at each of the different access layers, concerns concentrate predominantly at the operating system and application discovery layers. Specific issues relate to the pre-installation of apps, discriminatory access to OS functionality or system resources, admission and self-preferencing in app stores, as well as limiting the functionality of browsers on an operating system, or limitations on content imposed by browsers (e.g., ad blocking). Three main theories of harm emerge in this context. First, that integrated firms with gatekeeper control distort competition in related, normally downstream, markets by preventing those offering rival applications from having equivalent access to key hardware or software functions on the device (e.g. sensors, payment chips or allocation of system resources such as CPU and memory). This may also prevent these rivals from threatening their gatekeeper position in the upstream market. Second, that integrated firms with gatekeeper control exploit their position by levying excessive fees or commissions on any firm wishing to access the users of the devices in question through a convenient means, such as an app store. Related to this, the integrated firm may degrade other ways in which users might access third party applications or services (e.g. by degrading the experience through the browser) in order to force app developers to pay for inclusion in the app store. Third, that integrated firms with gatekeeper control distort competition in related, normally downstream, markets by directing users of devices towards their own services and away from those of rivals, either by pre-installing or requiring the pre-installation of their services on the device before it is sold, or through other means such as preferring their own services when returning search results or when allocating system resources (e.g. memory or CPU). The extent to which this conduct is harmful depends on the extent to which users of a device have alternative means of discovering, downloading and installing third party services and applications onto their devices. Again, distorted competition in the downstream market may also protect the integrated firm's gatekeeper position in the upstream market and reduce the threat of disintermediation.

A number of arguments however can be made to justify individual conducts, particularly relating to innovation and investment, security and privacy and harmful content. Openness and non-discrimination, which are the main guiding principles of a neutrality regulation, are not necessarily the right approach to stimulate innovation and investment. In particular, research on open and closed platforms or ecosystems has shown that there typically exists an inverted U-shaped relationship between the degree of openness of a platform and innovation by or on the platform. Thus, a medium degree of openness is often optimal for innovation and investment, where platforms open up to outside complementors (e.g. by allowing third party application developers on the platform), but yet remain in control over access to the platform. In very open platforms, it is difficult to manage security, quality of the complements and hence quality of user experience and integrity of the platform. This drives down the average value of the platform for the consumers, and the platform becomes too congested on the supply side. Hence this also reduces the incentives of third party complementors to contribute to the platform. That is, a paradox arises where complementors avoid the platform, precisely because it is too open. In reverse, a platform that is too closed will miss out on the opportunity to invite third party complementors and thereby stifles innovation. Consideration of investment and innovation should therefore also consider the incentives of third parties who may themselves invest in new services or applications. Providing privileged access to device hardware or software resources may also enable innovative applications and services which would not otherwise run correctly if resources were to be allocated in a 'neutral' manner. The ability for third parties to obtain differentiated access to the device's resources (or to be pre-installed on the device) will encourage them to develop applications and services which can exploit these opportunities.

These considerations prompt a number of policy recommendations. We suggest that the regulation of the Internet access value chain should not centre on the notion of 'neutrality', especially if the view is broadened to also include devices. Instead regulation of the internet access value chain should focus on maintaining alternative routes for content to the consumer and the related aspect of avoiding a fragmentation of content (i.e., that some content is not reachable for some consumers). Here we also see a fundamental difference between the device layer (especially operating system and application discovery layer) and the network layer. At the device layer, it is often possible to introduce different routes to content (e.g., through side-loading apps, or by use of progressive web apps instead of native apps) that are accessible at the same time (although not necessarily under the same conditions and possibly constrained by the operating system). By contrast, this is not

possible at the network layer, because consumers typically only have one physical connection to the internet.

Accordingly, we **suggest four main areas for regulation at the operating system level:**

- (1) **Enabling side-loading of apps in dominant operating systems**, such that consumers can install any lawful and safe app on their device.
- (2) While we do not object to pre-installation of apps, **users should consent to pre-installed apps** in the same way as they would need to consent to apps that are installed later. Moreover, **a user should be able to truly de-install pre-installed apps**, and **alternative apps should be able to receive the same access privileges** as comparable apps that were pre-installed.
- (3) Dominant operating system providers should make **publicly available the specifications of all APIs and functionalities that can be invoked by apps, alongside the conditions under which those API can be accessed**. Moreover, **OS providers should give a minimum notice period to app developers** when changing APIs. Policymakers should also consider monitoring the implementation status of standards that have been adopted by standardisation bodies such as the W3C.
- (4) **The right to data portability should also apply to devices**, so that consumers can switch from one device (operating system) to another, as smoothly as possible. To this end, operating system providers should develop **codes of conduct and common interfaces** that would enable hassle free data portability between devices.

Moreover, we consider **the application discovery layer, and specifically app stores, as a crucial gateway for consumers to access content, and make policy recommendations in four areas:**

- (1) **Enabling alternative app stores**, which have the ability to host apps under different terms and conditions as well as with different prices and by using a different payment system. We also suggest that **dominant app stores, if pre-installed, should not be allowed to exclude alternative app stores from being accessible** through the dominant app store but the dominant app store should not be liable for activities that are then facilitated by the alternative app store.
- (2) **Unbundling the dominant app store from other apps**, so that the app store can be licensed to device manufacturers using a compatible OS on a standalone basis (and on FRAND terms). Following the Commission's Android decision, this is already the status quo, but should also be maintained in possible other cases in the future.
- (3) **No self-preferencing in browsers and app stores**. While we emphasise that it is important to make the ban of self-preferencing explicit, as has been done in the Digital Markets Act (DMA) proposal, we are more sceptical about how self-preferencing can be effectively detected and remedied.
- (4) Transparency and redress mechanisms for dominant app stores are already imposed under the Platform-to-Business regulation. Additional transparency and redress mechanisms are also foreseen under the Digital Services Act (DSA) and DMA proposals, and dominant app stores are likely to be subjected to all three pieces of regulation. We suggest that these provisions are sufficient in conjunction with the other recommendations made here, but **policymakers need to consider carefully how the obligations under P2B, DMA and DSA may interact when they are imposed concurrently**.

Most of our recommendations are very much in line with a number of new provisions that were included in the proposed DMA, which was published by the European Commission after we had started this study. The relevant provisions are Articles 5b, 5c, 5f, 6b, 6c, 6d, 6e, 6f, 6k and 6h. Generally, we concur with all of these provisions, but make a number of suggestions on how these may be adapted or specified in the context of devices in order to avoid unintended consequences



and in light of our findings in this report. We also show that almost all of these provisions would need to be specified further, including some of the Article 5 provisions, although these are deemed to be self-executing by the Commission.

01

INTRODUCTION

1 Introduction

Neutrality has become a loaded term in the context of the regulation of the internet ecosystem. Almost twenty years ago, the concept of “neutrality” in the context of the internet ecosystem was popularised by Tim Wu in 2003.¹ The idea originated from the observation that there was little competition between internet Service Providers (ISPs) in the US, which gave those ISPs market power and made them powerful gateways for consumers’ access to the growing number of Content and Service Providers (CSPs) on the internet.

The list of alleged distortions of consumer’s choice were large, ranging from active depression of freedom of speech² over outright blocking certain types of traffic for commercial reasons, to requesting CSP to pay additional fees in order to terminate their traffic. While there was significant evidence of blocking P2P and VoIP traffic, other violations of ‘neutrality’ were found to be rather anecdotal and often due to reasonable justifications, such as for security reasons, or reasonable network management in peak times.³ However, the debate revealed that ISPs were important gateways to the backbone of the digital economy and highlighted which practices *could* be undertaken by them, if they were to exercise their market power in such a way. Indeed, the most contentious and hotly debated topic was whether ISPs should be allowed to offer CSPs a preferred access to consumers in return for some additional payment.

Two variants of such preferred access were discussed the most. First, ISPs could offer CSPs a better network service so that their service would not suffer (as much) from the consequences of network congestion. This has become known as pay-for-priority or simply ‘fast lane’ access. Second, ISPs could offer CSP to exempt their traffic from being counted against a consumers’ monthly data allowance, in case such an allowance existed in the consumer’ internet access plan. This has become known as zero rating. Both practices were seen as especially problematic in case the CSP were to be vertically integrated with the ISP, such that the ISP would grant such privileges to its own services without any payment in return, possibly in an effort to leverage its dominant position in the market for internet access into the competitive digital content and service. However, research has also pointed out that pay-for-priority and zero rating can increase consumer surplus and innovation incentives.⁴

What started as a US centric debate quickly spread as an idea to Europe and other parts of the world: Access to the content, services and possibilities provided by the internet should be *neutral*: This means that consumers should be able to reach the services that they want without interference by the ISP that enables consumer’s access to these services. In particular ISP shall not prefer or block any consumer or CSP in any way, and shall be fully transparent about its internet access service. In other words, the ISP should just serve as a conduit, between consumers and the CSPs, but it does not take an active role in managing the relationship between them. This is the idea of net neutrality, which in the EU is enshrined in Regulation 2015/2120 on Open Internet Access and has been in effect since 2016.⁵

On a more abstract level, (net) neutrality regulation is grounded in three principles: (1) openness, (2) non-Discrimination and (3) transparency. Openness refers mainly to the unfettered ability of entry by new players in the internet ecosystem, the possibility that new (types of) services can emerge based on the internet’s modular design and standards, that consumers are free to choose the services and content that they want, and that freedom of speech is preserved.


¹ Wu, T. (2003). "Network Neutrality, Broadband Discrimination". Journal of Telecommunications and High Technology Law. 2: 141–179.

² A famous incident occurred in Canada, where Telus blocked some websites during a labour dispute. See <https://www.nytimes.com/2005/08/01/business/worldbusiness/a-canadian-telecoms-labor-dispute-leads-to-blocked.html>.

³ See https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/45-berec-findings-on-traffic-management-pra_0.pdf.

⁴ For an overview see Easley, R. F., Guo, H., & Krämer, J. (2018). Research commentary—From net neutrality to data neutrality: A techno-economic framework and research agenda. Information Systems Research, 29(2), 253–272.

⁵ Although the debate started in the US, net neutrality regulation has never been in effect in the US for long. Net neutrality regulation is expected to be enacted again under the Biden administration, however.



Non-Discrimination refers predominantly to fair competition in the various internet-enabled markets and non-discrimination of content providers based on origin, content, the identity of senders or receivers, and unfettered consumer choice. Transparency, finally, relates to transparency about choices, actions and restrictions that may have a significant impact on openness and discrimination of content.


Two decades after the net neutrality debate started, the internet ecosystem has evolved and additional gatekeepers have emerged. In order to access content from content and service providers (CSPs), consumers have to pass through a whole internet access value chain, comprised by broadband providers, device manufacturers and online platforms. Today online platforms, such as search engines, online marketplaces and other online intermediation services also play an important role in the consumer's discovery and choice of CSPs. Likewise, devices (such as smartphones and connected speakers) and the software that runs (or does not run) on them can significantly impact the consumer's access to and choice of online services. In this report, we discuss whether, **'openness', 'non-discrimination' and 'transparency', which are the key pillars of net neutrality regulation, should be regulatory principles that also apply at other layers of the internet access value chain and specifically to certain types of devices, as well as to the final network connection, between a consumer's device and the online content or service that the consumer ultimately wants to access.**

In particular, the issue of device neutrality has been put to the forefront of the policy debate by ARCEP, the French telecoms regulator, who argued that devices through which services and content on the internet are accessed (e.g., smartphone, tablets, personal voice assistants) and their associated mobile operating systems are now the remaining "weak link" to ensure an "open internet".⁶ Again, concerns similar to those in the net neutrality debate were raised. In particular, CSPs may be induced to negotiate preferred placement and functionality on devices, or may be disadvantaged in comparison to the apps of vertically integrated providers. For example, apps of vertically integrated providers may be placed more prominently or may be easier to access, may not be as easy to uninstall, or may have privileged access to hardware, such as battery management, or built-in sensors and chips (e.g. NFC, GPS, Bluetooth). If Openness, Non-Discrimination and Transparency are upheld as the guiding policy principles for internet regulation, and applied in a same way as in the context of net neutrality, these principles would need to be maintained at each level of the consumer's access and discovery process, i.e. also including the devices. This is what is meant by device neutrality.

In this report, **we will focus on device neutrality**, but as the preceding discussion highlights the topic has close interlinkages with net neutrality and the regulation of dominant platforms, and at times the boundaries between the concepts also may become blurred. For example, app stores are indeed platforms that run on devices, and devices have the ability to block certain apps from accessing the internet. However, it will soon become evident that the issue of device neutrality is far more complex than that of net neutrality, because it relates to a multitude of different access layers (as opposed to 'just' the network layer in net neutrality), and hence there exists a myriad of possible practices that could violate 'neutrality' principles.

The need to regulate also other parts of the internet access value chain has already been recognised by EU policymakers. In particular, Platform-To-Business (P2B) Regulation (EU 2019/1150) has introduced a transparency obligation – which is a key element of a 'neutrality' regulation – for online platforms. It applies horizontally to all online platforms, irrespective of whether they are dominant or have 'gatekeeping power'. Hence, the obligations under the P2B are relatively mild, and do not contain any non-discrimination or openness provisions.

⁶ Autorité de régulation des communications électroniques et des postes [ARCEP] (2018). Devices, the weak link in achieving an open internet. Available at https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf.



Competition authorities, including the European Commission, have also been investigating cases of discrimination or exploitation by providers of devices, operating systems or app stores⁷, most notably in the Google Android case which the Commission concluded in 2018⁸. These and other cases have then informed the European Commission Proposals for ex ante regulation in a Digital Markets Act (DMA) (COM(2020) 842 final), and which will complement the P2B Regulation. The DMA is targeted at digital gatekeepers, which operate a 'core platform service', and thus does not apply to all platforms. The proposal contains not only stricter transparency obligations than the P2B, but also non-discrimination (e.g., no self-preferencing of own services) and openness obligations (e.g., being able to side-load apps and app stores), so all elements of a 'neutrality' regulation. Even more so, the DMA contains a number of provisions that specifically address 'device neutrality' issues, such as issues relating to the operating system or app stores. However, these provisions are clumped together with other provisions that do not relate to devices. In the following, we will therefore take a step back and address the issue of device neutrality from the bottom up, rather than top down. **In our policy recommendation, we will then link our findings and insights specifically to the P2B and DMA, and comment on whether we think the proposed provisions are comprehensive from a 'device neutrality' perspective.**

The remainder of this report is structured as follows: Next, we introduce the internet access value chain, and highlight how it is comprised by individual layers, each of which is crucial so that online content can reach consumers. We also show which of these layers can be attributed to devices, and which to networks and online content. In Section 3, we then discuss in more detail possible device neutrality issues that can arise along the internet access value chain, and identify the main areas of concern for policymakers. In Section 4, we discuss justifications for 'non-neutral' conduct that should caution policymakers against imposing too strict 'neutrality' rules for devices. We present a number of policy recommendations to address potential concerns, particularly with a view on ensuring alternative routes for content to reach consumers on devices. Our policy recommendations are organised according to the different access layers that we have identified previously. Finally, we conclude by highlighting the relationship of our recommendations to the DMA and the Open Internet Regulation, respectively.

⁷ 'Commission opens investigation into Apple's app store rules', 16 June 2020, at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073; 'Commission opens investigation into Apple practices regarding Apple Pay', 16 June 2020 at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1075; 'ACM launches investigation into abuse of dominance by Apple in its App Store', April 2019 at <https://www.acm.nl/en/publications/acm-launches-investigation-abuse-dominance-apple-its-app-store>; 'CMA investigates Apple over suspected anti-competitive behaviour', 4 March 2021, at <https://www.gov.uk/government/news/cma-investigates-apple-over-suspected-anti-competitive-behaviour>.

⁸ Case AT 40099.

02

THE INTERNET ACCESS VALUE CHAIN

2 The internet access value chain

2.1 Layers of the internet access value chain

In order to access (and provide) content and services online, the interaction and interoperability of numerous technical access layers is necessary, each of which provides a dedicated functionality. The access layers depend on which devices, which network connection, which operating system, and so on, is used.

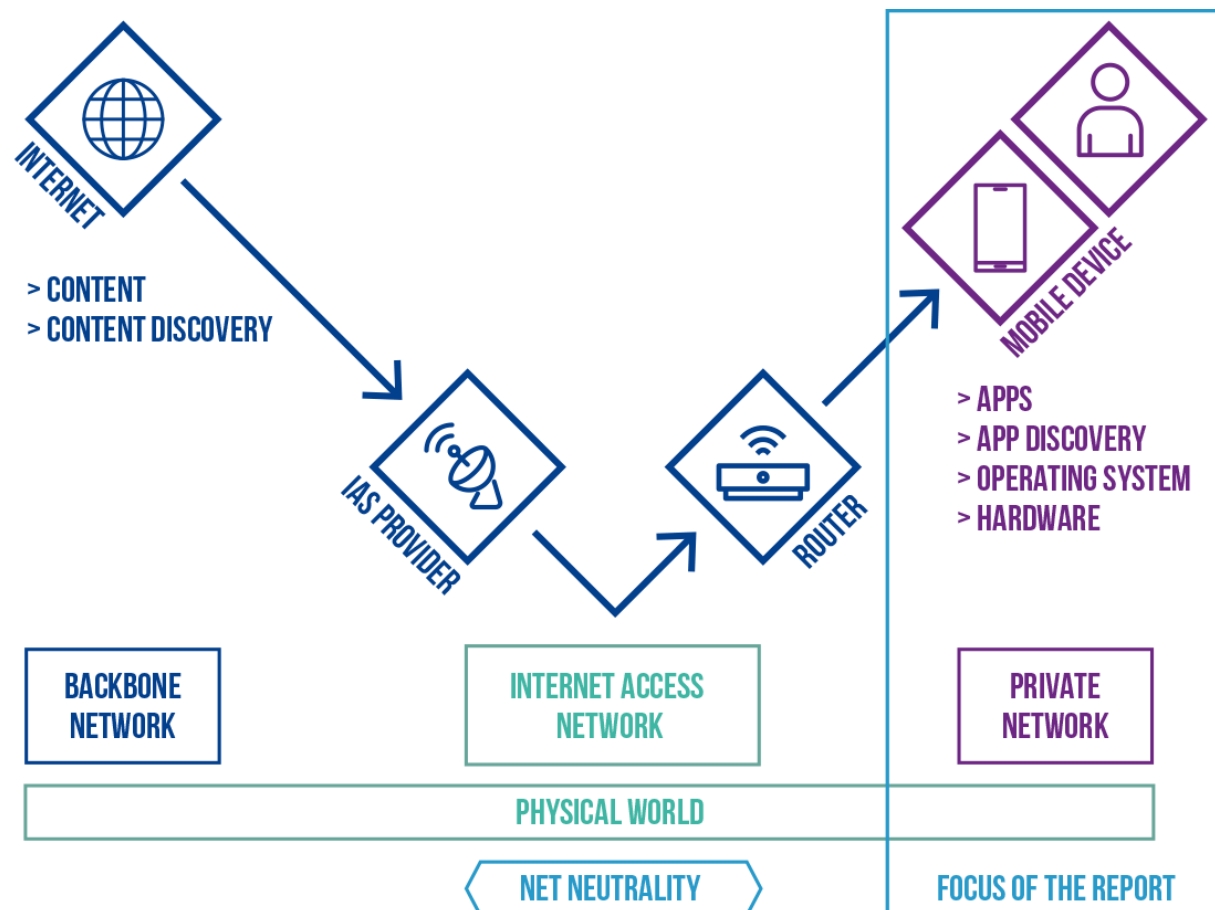



Figure 1: The internet access value chain and the various access layers.

Source: Jan Krämer, Richard Feasey

Figure 1 depicts what we denote as the internet access value chain and highlights the layers that content may have to pass through in order to reach the consumer. For example, the content requires a network to reach the consumers, and device with which the network and the content can be accessed. But the network also requires content and a device to provide value.

The logic is similar to that of a 'protocol stack', which is typically used in computer science to show a hierarchy of networking protocols that depend on each other, such as a TCP running on top of IP. However, we organise and denote the layers in a more unconventional way in order to fit the purpose of this report. **In particular, we may differentiate three main building blocks of the internet access value chain.**

(1) **Online content**, i.e., the digital content, services and online platforms that are provisioned on a remote server on 'the internet': This is located in the top-left corner of Figure 1. The provision of online content as such is independent of a particular device or a particular network connection used by a consumer, and thus outside of the scope of 'device neutrality' or 'net neutrality'. Yet, 'neutrality' issues may nevertheless arise due to the dominance of some platforms that can become gatekeepers to accessing content as they perform – in the jargon of the Digital Markets Act – a 'core platform



service', specifically 'online intermediation services' and 'online search engines'. The very purpose of platforms is to facilitate consumers' discovery of content and services and to intermediate between the providers and the consumers of such services. Typical examples are search engines, online marketplaces or hotel booking sites. We denote this as the 'Content Discovery Layer', because content that is not discoverable by consumers at such platforms (e.g., not listed prominently by a search engine), is often de-facto not visible to the consumer and will therefore yield significantly less demand for the content provider. As the very purpose of platforms is to discriminate between content in an effort to facilitate the content discovery process for consumers, 'neutrality' regulation comparable to that of net neutrality (i.e., that all content shall be treated equally) is meaningless at the content discovery layer.⁹ The P2B Regulation addresses this layer specifically, requiring, among other things, platforms to make transparent how they rank content. Also the DMA proposal contains provisions targeted at the content discovery layer, such as a ban of self-preferencing for vertically integrated platform providers (Article 6(d)).

(2) The **network**, i.e., all links over which the content is transmitted between the remote server and the consumer's device: This contains at least (i) the backbone networks, i.e., the links between the remote server and a consumer's internet access service (IAS) provider; (ii) the internet access network controlled by the IAS provider up until (and sometimes including) the customer's router/modem (i.e., the last mile network); and (iii) the customer's private network (e.g., a Wi-Fi network established by the router). 'Neutrality' violation could occur in each part of these links. For example, backbone providers could send traffic coming from certain servers over less direct or more congested routes through the Internet (e.g., due to the so-called 'hot potato routing'); or content providers could negotiate more direct, and less congested routes with IAS providers (e.g., through paid peering), or install a content delivery network in proximity to the IAS provider in order to expedite the transmission of their data packets.¹⁰ Likewise, the customer's router may discriminate between different types of content, e.g., by giving priority to VoIP or VoD content, or block certain content, e.g. through web filters. These features may also be pre-configured by the router manufacturer. Nevertheless, the customer's private network as well as the backbone network are not part of net neutrality regulation, and hence the types of conduct mentioned above are legal, although they have a similar effect as a violation of net neutrality. Net neutrality regulation only applies to the IAS network.

(3) The **device**, i.e., both the hardware as well as the software, including the operating system and the app store. The device is necessary to receive remote content being sent through the network. Here, we can differentiate between several layers within the device.


(i) The **hardware layer** denotes the physical device as such. This includes both fixed components (e.g., the network card, built-in sensors, and a secure element chip¹¹) as well as ancillary and exchangeable components (e.g., memory cards, SIM card).

(ii) The operating system (OS) layer. The operating system is separate from the hardware layer, because an OS can run on several different physical hardware. Essentially, an operating system is a piece of software that controls the devices functionalities and allows other software to be run on the device. Thereby, it also controls the applications' (running on the operating system) access to hardware functionality of the device over well-defined software interfaces. It is worth mentioning, however, that the operating system also consists of different (software) layers that provide functionalities at different levels of abstraction. On an abstract level, we may, for example distinguish between high level and low level functionalities of an OS. Low level functionalities are 'minimal'

⁹ General non-discrimination obligations for online platforms, including a ban of payment for prominence schemes are also not necessarily desirable. For a discussion see Krämer, J., Schnurr, D., & de Streel, A. (2017). Internet Platforms and Non-Discrimination. CERRE Report. Available at: <https://www.cerre.eu/publications/internet-platforms-non-discrimination>; Krämer, J., & Schnurr, D. (2018). Is there a need for platform neutrality regulation in the EU?. Telecommunications Policy, 42(7), 514-529.

¹⁰ For a discussion of these practices, see Easley, R. F., Guo, H., & Krämer, J. (2018). Research commentary—From net neutrality to data neutrality: A techno-economic framework and research agenda. Information Systems Research, 29(2), 253-272.

¹¹ The secure element can, in fact, also be implemented without fixed hardware through a cloud-based or a software based solution. See <https://developer.android.com/guide/topics/connectivity/nfc/hce>. Moreover, the secure element may, in theory, also reside on exchangeable hardware components.




functionalities that an OS has to provide, such as input-output management, memory management, CPU management and battery management. High level functionalities provide more complex functionalities that require several low level functionalities to work, and often have a direct graphical user interface as well (e.g., built-in/pre-installed apps, e.g., contact book, phone app, voice assistants, maps). It is worth noting that some operating systems are based on so-called microkernels, which essentially only provide such low level functionalities. For example, Huawei has announced that HarmonyOS, which the company seeks to deploy on a range of different devices, would be a microkernel OS. The advantage of such microkernel OS is that it can be more easily adapted to different hardware, because its components can be exchanged more easily. By contrast, Android is not a microkernel OS and uses a so-called 'monolithic' kernel that is based on the Linux kernel. Android (more precisely the Android Open Source Project) and the Linux kernel are open source under the Apache and GNU license, respectively. Apple's operating systems are based on a hybrid kernel (neither monolithic nor micro), called XNU, which again is the foundation of the Darwin core operating system, on top of which all of Apple's OS are built (MacOS, iOS, WatchOS, etc.). XNU and Darwin are licensed and free and open source under the Apple Public Source License (APSL), which is less permissive than the Apache license, however.

(iii) Similar as the content discovery layer, the **app discovery layer** includes those applications that are crucial for consumers to access other apps or web content. The layer is comprised by app stores (such as Google's PlayStore and Apple's App Store) as well as browsers. As mentioned above, app stores are platforms that run on a device and as such they fulfil a similar purpose as search engines for apps. Especially in mobile operating systems, app stores are usually the only practical way for ordinary users to install additional applications on the device. App stores are explicitly mentioned as an online intermediation service in the P2B regulation and thus fall under the scope of that regulation as well. Browsers are special apps that enable access to the content of the World Wide Web (WWW). As such, browsers are similar in functionality to app stores, because they allow to access content of third parties. Indeed, in modern operating systems a similar functionality and user experience as in native apps can be achieved by so-called progressive web apps (PWA) that run inside a browser and do not need to be installed via the app store. Like app stores, browsers also have the ability to make some content more prominent than others, for example by highlighting content on the starting page, or by setting a default search engine, or by blocking access to certain websites. Thus, it is useful to consider them also at the 'application discovery layer'. However, browsers are not explicitly mentioned as online intermediation service in the P2B regulation, and thus, this regulation does not apply here. We note that browsers are also not included as a 'core platform service' in the DMA proposal (but may be added later according to Article 17).

(iv) Finally, the app layer denotes all the apps (including web apps and websites) that can be used on a device. Content and content discovery may occur inside an app (e.g. a browser), so that it is logically located below the 'online content' layers discussed above. Moreover, we note that the distinction between the application layer and the application discovery layer will often depend on context. For example, some apps can act as app stores themselves, or be themselves a platform for other content, such as certain messenger apps (e.g., WeChat) or social networks. Thus, depending on the level of analysis, a third-party app store could be seen as an app that is "discoverable" within an app store pre-installed on a device; or after the third-party app store has been downloaded and installed, this app store can then be considered to be part of the discovery layer itself. This nesting of layers is typical for the layering concept.

Not all layers may exist in all scenarios (e.g., some apps may not need to make a network connection, content and application discovery layer may be skipped). Depending on how closely one may want to examine the problem, one could also define more layers. Especially within what we call the operating system layer and the hardware layer, there exists a hierarchy of possible other layers that could be differentiated (e.g., Level 1, Level 2 and Level 3 cache). But likewise the network layer is indeed comprised of several logical layers ('the protocol stack'). Those differences, however, are not really important for the purpose of this report. Nevertheless, it is important to point out that the boundaries between some of the layers depend on the perspective. For example, we already noted that the app discovery layer is also comprised by apps. For example, a browser is located both at



the app layer (e.g. can be downloaded from an app store or from a website), as well as the application discovery layer (e.g., is used to download an app or to run a web app) and this is not a contradiction.

Likewise, an app can be part of the high level functionality of the operating system when it is pre-installed (e.g., browser, contacts), but also be installed later, thus blurring the boundaries between the operating system layer and the app layer. Nevertheless, it is useful to differentiate these layers.


2.2 Interfaces and standards connecting the layers

Interaction between layers usually runs over well-defined interfaces (APIs, hardware- and software standards), which enables modularity, e.g. browsers can run on different OS, device can communicate with different networks, and so on. The purpose of the interfaces is to define the set of functionalities provided by a (component of a) lower layer, how they must be invoked, and what they would return. For example, Apple's Core Location Framework is an interface provided by the operating system layer, whereby applications (running in the application layer) can poll the OS for the geographic location, altitude and orientation of the device. It is important to see that the Core Location Framework does not provide direct access to sensors and to the (physical) data that they may generate – and this is often also not important (or convenient) for the application. That is, the application may, for example, only care whether the device is currently in a horizontal or a vertical position in order to adjust the layout of the screen. It does, usually, not care about how that information was precisely derived from the build-in sensors. A similar interface then exists between the OS layer and the hardware layer, where the actual sensor is located. This is where the OS typically receives raw sensor readings (e.g., from a gyroscope) from which it then derives the orientation of the device. Finally, one may also say that there exists an interface between the hardware layer and the physical layer (i.e. the actual physical environment), whereby the gyroscope 'polls' the physical environment for changes in momentum and gravitation.

Such layering is a very useful concept, because it offers more security, reduces the complexity and enables a very modular design. For example, if Apple were to change the gyroscope in its device, then it would probably not have to make any changes to the OS, and all applications that would use the Core Location Framework would just continue to work in the same fashion. One would only have to make sure that the new gyroscope implements the same interface (and thereby delivers the same type of readings) to the OS as the previous version. Likewise, if the OS is updated, it can – in principle – still operate with the same hardware and does not require that every app is re-programmed, as long as the interfaces are the same. In other words, each layer is only concerned with how it interacts with the layer exactly below it, and the layer exactly above it, and this allows for great modularity and reduction in complexity. Admittedly, this illustration and claim is a little oversimplified, but we believe that it is yet a very useful approximation, especially for our purposes here in the context of device neutrality.

What is important to understand is that to achieve such layering and modularity it is absolutely vital to define standards for the interfaces. This does not preclude the possibility that unilateral (ex-) changes and upgrades can be made within each component of a given layer. As long as it implements the standardized interfaces, it would continue to work without disrupting the whole system. In reverse, this means that changes to the interfaces can have a quite disruptive effect on every party that depends on it.

Standards can be of four generic types: Open vs. proprietary standards, and common vs. individual standards. By open standards we mean all those standards that are free to use and do not need to be licensed by a third party. Standards that require such authorization and licenses are proprietary standards. By common standards we mean standards that are set by common standardization organizations and groups, such as IEEE, ISO, W3C; whereas by individual or modified standards we mean such standards that have not been (fully) implemented in the way in which they were standardized, modified from the original standard or designed and adopted without the auspices of a standards body. Standards may also be adopted only very slowly, or older devices and software may not be updated to the newest available common standards.



Despite the benefits of layering and interfaces, there may be technical or commercial reasons not to open up functionalities of lower layers. For example, an OS may restrict (third-party) apps access to certain hardware functions due to security concerns, and/or reserve that functionality only for built-in high level apps of the operating system. This is “neutral” in the narrow sense only when it applies to all apps at the application layer, and all apps (including the OS provider’s apps) have the same restrictions. Similar issues can arise also at higher layers, for example, when due to privacy considerations apps cannot access user (tracking) information provided by the OS.

Likewise, at all levels, manufacturers or developers may choose for technical or commercial reasons to modify a common standard. However, as mentioned above, such changes must be communicated in a transparent and open way, and the actors at the different levels must be given due time to adapt their hardware or software to the new interface. Yet, this may also mean that some hardware or even some software may become unusable (or requires additional effort or costs that consumers may not want to bear) – yielding stranded investments on the side of the consumers.

Not implementing certain standards, or not opening certain interfaces, or even requiring to use a certain interface could also be used to impact the functionality of certain groups of apps. For example, Apple requires all browsers on iOS to use the implementation of its WebKit browser engine, which does not fully adopt the W3C standards.¹² In this way, it can control, among other things, the functionality of progressive web apps. This may likely affect the user’s choice between PWA and native apps.

¹² Blink, the competing web rendering engine developed by Google as part of the Chromium project, was originally based on WebKit, which was developed by Apple. See <https://www.wired.com/2013/04/blink/>.

03

**POSSIBLE DEVICE
NEUTRALITY ISSUES
ALONG THE INTERNET
ACCESS VALUE CHAIN**

3 Possible device neutrality issues along the internet access value chain

Concerns about device neutrality arise because those controlling the devices or ancillary features may perform a 'gatekeeper function' in the same way that a provider of an internet access connection controls a 'gateway' to the internet. Users typically rely on a single connection to their home or business to access the internet. In the same way, a user capacity to access and use different services, and the capacity of third party service providers to access users, will depend upon the way in which the device they are using functions and the way in which users and providers can interact with it.

3.1 Smartphones and the termination monopoly

3.1.1 Smartphones as key devices for general internet access

In the era of the internet of Things (IoT) more and more devices are connected to the internet, and hence there exists a large diversity with respect to what the specific purposes of these devices are and should be. We therefore see a difference between **internet-enabled devices** (e.g., smart kitchen appliances, smart toys, light bulbs, cars, etc.) and **general internet access devices** (smartphones, tablets, laptops, etc.), while noting that some grey zones may exist (e.g., smart TVs, smart speakers with screens, smart watches). In this report, our primary focus is on general internet access devices, and specifically **we focus on smartphones as the key personal device for internet access**. This is because smartphones are multi-purpose devices that can – in terms of internet access – replace most others. Indeed most consumers will not solely rely on internet-enabled devices for accessing services on the internet, but they may well rely on a smartphone to do so.¹³ Moreover, smartphones are the devices that are closest and personal to the consumers, being with them at all times. This also means that for many applications, smartphones are consumers' first choice for accessing the internet. Across all applications, it is estimated that globally users spent roughly 53% of the time online using a smartphone vs. a laptop or desktop device.¹⁴ As smartphones are becoming more and more powerful, and with an industry trend to converge the operating systems being used on mobile and stationary devices, it is expected that smartphones will become even more important general internet access devices in the future.

Nevertheless, it is also important to maintain an 'ecosystem view' on devices. Generally, users will own or use several internet-enabled devices¹⁵, and may have strong incentives to purchase devices from the same provider if, by doing so, it is easier to transfer services or share or back up data between them, or they present the same user interface or services across all devices. Most notably, there is an ongoing trend to have unified operating systems for different kinds of devices, which will bolster the relevance of ecosystems. For example, Apple's latest move to use ARM-based chips in laptops, which are already used in smartphones, will enable them to provide a more seamless user experience across devices. Similarly, many internet-enabled devices run a variant of Android.¹⁶ Suppliers may also offer financial inducements to purchase devices from the same provider (such as then allowing device owners to share paid-for services) and to remain within the same 'ecosystem'. Thus, market power that is generated by controlling (a specific layer in) one particular device, most notably a smartphone, may also be leveraged to other devices within the same ecosystem, such as wearables, smart speakers or laptops. This can be achieved, for example, by providing users the ability to seamlessly transition between devices belonging to the same ecosystem (e.g., to continue to write an email on the desktop device that was started on the mobile device), but not for other devices.

¹³ Nevertheless, for specific applications, consumers may preferably use a specific internet-enabled device, e.g. an ebook reader, VoIP phone or weather station.

¹⁴ See Datareportal (2021). Digital 2021: Global Overview Report. Available at <https://datareportal.com/reports/digital-2021-global-overview-report>.

¹⁵ According to the Digital 2021: Global Overview Report (id.) "9 in 10 internet users say they go online via a smartphone, but two-thirds also say that they use a laptop or desktop computer to access the internet."

¹⁶ In fact, Android was initially devised for digital cameras and not smartphones.

3.1.2 Termination monopolies: Ex-post market power in ex-ante competitive markets

Although users may switch from one device supplier to another, the costs of purchasing new devices (whether reflected in the upfront prices paid by users or in the multi-year contractual commitments required by telecoms operators to repay those costs) can represent a barrier for some users. Competition between device providers may mean that users select a particular device after having considered the kinds of applications services which it supports (alongside other considerations relating to the appearance or performance of the device itself) but, once that choice is made, users may be unlikely to switch devices if access to a particular service were subsequently to be denied or restricted. In addition, it may be difficult to assess for consumers at the time of purchase, which applications they would need in the future. This means that a third party provider of services or applications may find it very difficult, if not impossible, to induce users to switch from one device to another (e.g. by withholding its services or applications from one device in order to persuade users to switch away from them). It is much more likely that, in the majority of cases, the user would simply substitute another service or application for that of the third party on the same device, rather than switch device. The implication for app developers is that they need to provide their applications for several (incompatible) ecosystems. While large and established app developers already do this, the costs of developing performant apps for several platforms and promoting apps on multiple platforms are especially high for small and emerging app developers, who are much more constrained in their resources.¹⁷ Small developers may therefore well choose just to be available on one ecosystem first.

Furthermore, users may be unable to detect whether access is being restricted or may be unaware that it was when deciding which device to purchase. Once a user has purchased a number of synchronised devices that operate within the same interoperable 'ecosystem', the costs of persuading a user to switch to another device provider may become very significant or insurmountable.¹⁸ Surveys have suggested that around 85% of owners of Apple devices remain 'loyal' to the Apple ecosystem (i.e. replace the device with another Apple device) and over 90% of Android users remain loyal to the Android ecosystem¹⁹. Other surveys suggest that fewer than 5% of those who switch between ecosystems do so in the expectation that they will obtain better access to third party applications or services. Device features, performance and cost were much more significant considerations, confirming how difficult it would be for third party application and service providers to bypass particular device gatekeepers by persuading users to switch to another.²⁰

In consequence, devices, especially if they are expensive (as is generally the case for smartphones) and if they are incorporated in an ecosystem of devices (which also makes switching more expensive, as multiple devices have to be replaced) may perform a 'gatekeeper function' despite the fact that many users own multiple devices and that markets for the supply of devices may themselves be competitive. This is commonly referred to as a termination monopoly and has indeed also been the main reason why all internet access providers – as opposed to only the dominant internet access providers – were subjected to net neutrality regulation.


However, unlike net neutrality, where the gatekeeper control is exercised over the physical connection by the broadband provider, the exercise of 'gatekeeper control' in devices can apply at many different layers of the value chain (see above). As van Gorp and de Bijl explain, vertically integrated digital platform providers, including those engaged in the provision of devices or related software, seek to intermediate between different groups of users. If they are able to do so in a way which means users have no alternative route to the services of the other users (i.e. the platform cannot be 'disintermediated') then they may acquire what we refer to in this paper as 'gatekeeper control'.

¹⁷ See Bresnahan, T., Orsini, J. and Pai-Ling, Y. (2014). Platform choice by mobile app developers. Available at https://www.law.northwestern.edu/research-faculty/clbe/events/internet/documents/Yin_multihoming%20v12py.pdf.

¹⁸ Such switching costs also arise for single devices, without consideration of an ecosystem of devices. However, switching costs are likely to be higher if switching entails to change several devices simultaneously.

¹⁹ <https://www.forbes.com/sites/chuckjones/2018/03/10/apples-ios-loyalty-rate-is-lower-than-googles-android-but-apple-may-steal-more-users-each-year/?sh=43e7834e68a8>.

²⁰ <https://9to5mac.com/2018/08/23/iphone-android-switching-survey/>.



Users may, however, be able to bypass the intermediary if there are other connections available, either within the same value chain or via a completely different route. Thus, they write:

“In digital markets, competing platforms intermediate and disintermediate each other, aiming at control of and access to essential content, data or user groups. Intermediation may lead to gatekeeper positions, that is, control over nodes that cannot be avoided by users that want to interact with each other. However, these gatekeeper positions may be contested by rivals from parallel markets through disintermediation. That is, competition is not so much characterised by rivalry to offer similar services, but by introducing alternative routes of access to essential content, data or user groups. For example, internet browsers may disintermediate operating systems by offering end-users alternative options to run software and view content. It follows that competition between digital platforms sometimes exceeds market boundaries and allows monopolists in parallel markets to challenge each other ('mologopolistic' competition).”²¹

The previous section has highlighted the different access layers at which device neutrality issues could arise, namely at the (1) hardware layer, (2) operating system layer, (3) app discover layer (browsers or app stores) and (4) the app layer. We now consider each of these layers in turn and discuss possible device neutrality issues, or more generally market power issues that may arise or have arisen at each layer.²² Our main goal is to highlight some (but not all) issues at each layer, but that some layers may be seen as more problematic than others.

3.2 The hardware layer

3.2.1 Market overview

The hardware layers is characterised by the devices as such without the operating system that runs on them. The smartphone hardware market, comprised by Original Equipment Manufacturers (OEMs) generally is competitive in Europe, with the largest OEMs being Samsung (37% market share in Q3, 2020) and Apple (18% market share), closely followed by Chinese manufacturers Xiaomi (17% market share) and Huawei (12% market share).²³ Market shares have also remained relatively stable in the past five years, especially for the market leaders Samsung and Apple, and there is no trend that any vendor may monopolise the hardware market in the near future. However, there is some indication of some market consolidation in the long tail of the smartphone market, especially following the entry of Xiaomi and Huawei, which together now supply 29% of the market, with no significant market shares five years ago.²⁴ In addition, Huawei's recent decline in market share is probably due to US export restrictions, which prohibit Huawei (but not Xiaomi) to obtain a license for Google Android and Google Mobile Services on their devices. This reveals that the supply of hardware alone is not sufficient to compete in the market for devices. We will return to this point later Section 5.3.2.

²¹ <https://www.government.nl/binaries/government/documents/reports/2019/10/07/digital-gatekeepers/Digital+Gatekeepers.pdf>.

²² For a more detailed description of specific neutrality issues, although not grouped according to the layer in which they occur, we refer to the report by ARCEP, ibid.

²³ <https://www.statista.com/statistics/632599/smartphone-market-share-by-vendor-in-europe/>.

²⁴ Following this market concentration, LG announced in April 2021 that it would discontinue its mobile phone business worldwide. See <http://www.lgnewsroom.com/2021/04/lg-to-close-mobile-phone-business-worldwide/>.

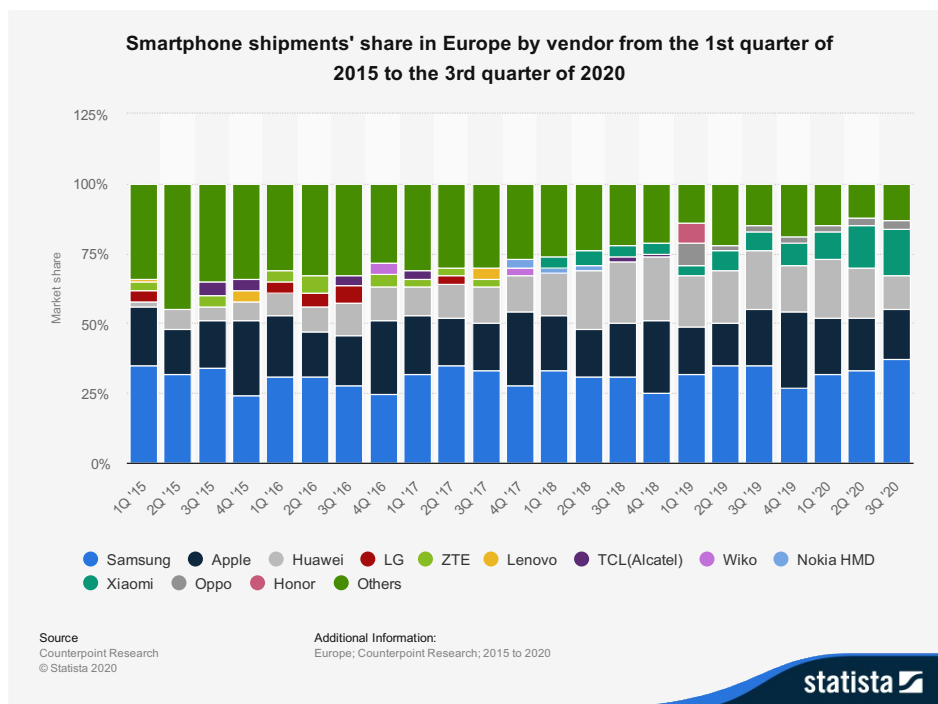


Figure 2: Smartphone market share by vendor in Europe, Source: Statista

With respect to the technical features of devices (e.g., quality of the camera, resolution and size of the screen, storage, CPU, etc.), the device landscape seems to be competitive. Taken together, we can conclude that smartphone hardware as such (without the operating system and other software) is not a competitive bottleneck. There are also no significant network effects at the hardware layer that would make further market concentration more likely in the future. However, the hardware layer alone is dysfunctional without the OS and application (discovery) layers. We consider these other layers in turn.


3.2.2 Possible issues

The hardware of the device will necessarily influence the performance of services that run on the device, or whether services can run at all. An integrated firm such as Apple or Amazon (or Google in relation to its Pixel phone) will design and configure the hardware of a device to support the requirements of its own services and the needs of its customers. To date, concerns have arisen not from limitations in the features or capabilities of digital devices - which continue to evolve at a rapid rate in response to competition between device manufacturers - but from concerns about how control over the device hardware may distort competition in related software markets²⁵.

For example, an integrated firm may allow its own services to exploit hardware assets, such as NFC chips, processors or sensors that are unavailable to third party applications services. This would mean that third parties are unable to replicate the services being offered by the integrated firm. The blocking of access to a particular hardware asset may be easy to detect, but firms may discriminate in more subtle ways when a hardware resource, such as battery or processor capacity, is shared by a number of services and access to them is managed by the OS (see below). Such concerns have arisen in relation to Android software which disables the background activity of certain apps, partly to preserve battery power and partly for security reasons (to inhibit spyware), but allows other, more popular, apps to continue to run²⁶. Also devices that are locked to a certain mobile network (NET-locked or SIM-locked phones) can be considered to violate the openness principle inherent to device

²⁵ It is conceivable that producers of one type of device might also take measures to distort competition in a market for other types of devices – for example, by limiting access to Bluetooth chips to prevent the transfer of data to devices of other suppliers, or adopting proprietary technologies which only interoperate on devices supplied by the same producer.

²⁶ https://en.arcep.fr/uploads/tx_gspublication/report-state-internet-2019-eng-270619.pdf, p.63.



neutrality. The list of possible device neutrality violations can thus become quite long. Theoretically, a firm controlling the *hardware level* could

- privilege, restrict or prohibit access to certain networks (mobile, ad-hoc or infrastructure networks);
- prohibit or inhibit the installation of certain operating systems;
- reserve or privilege system resources (e.g., battery, memory, computing power, storage, dedicated interfaces) for specific apps;
- prohibit, inhibit or restrict software at higher layers to access hardware components (e.g., sensors, chips, camera, microphone);
- prohibit, inhibit or restrict compatibility with ancillary hardware components and devices.

3.3 Issues at the operating system layer

3.3.1 Market overview

In Europe, and indeed across the world, there are in fact just two mobile operating systems: Android and iOS. By now market shares are relatively stable, with Android-based operating systems having a share of about 70% and iOS 30%. While the market share of iOS has remained around 30% for the past five years, the market share of Android has increased in the same period thanks to the decline of Blackberry and Windows Mobile. In contrast to the hardware layer, there are significant network effects at the operating system layer. These are mainly rooted in indirect network effects, especially because developers are more inclined to produce software for an operating system with a large user base, and consumers are more likely to adopt such an operating system. However, also other indirect network effects exist, such as the larger availability of community support (e.g., video tutorials). Such network effects are not specific to mobile operating systems, of course, and hence it also explains the similar structure in desktop operating systems. Taken together, this already leads to the conclusion that more than two (incompatible) OS are probably not sustainable in the market. A larger number of incompatible OS is also not necessarily desirable from a welfare perspective. By the same token, more incompatible OS would reduce the network effects of each of them. This would increase the development costs for apps, and, as developers could choose only subset of the available OS, resulting in more fragmentation of content, where each OS would only provide a subset of the available content. Competition between OS would probably further drive fragmentation, because OS would also compete on exclusive content, in similar fashion as competing gaming consoles compete on exclusive content. Thus, competition does not ensure 'neutrality' of content.

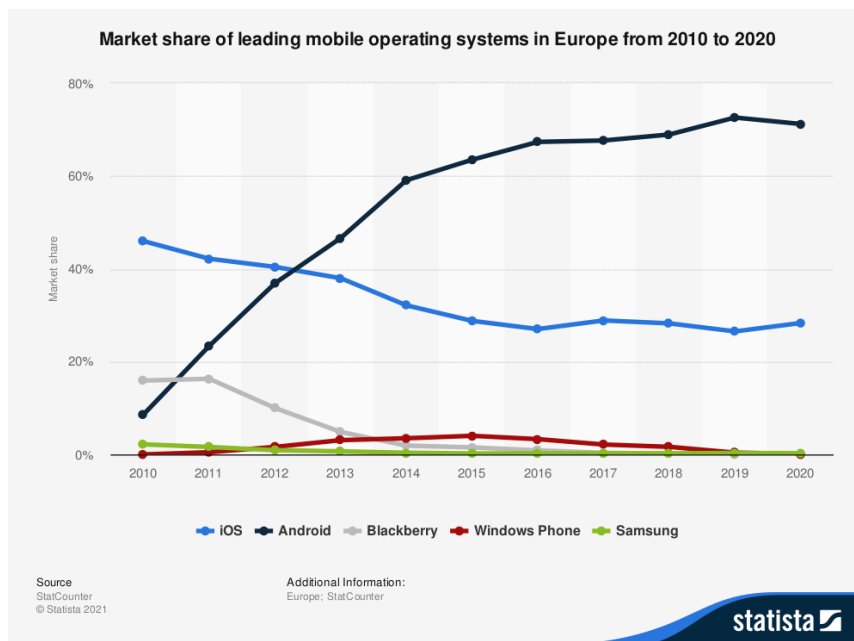



Figure 3: Market share of mobile operating systems in Europe, Source: Statista

In the case of Apple, the hardware layer is not unbundled from the operating system layer, because iOS is only provided together with Apple hardware.²⁷ In the case of Android this is different, as Android runs on hardware from different device manufacturers (whether under a licence from Google or not), and the operating system layer for mobile devices exists independently in the market. However, for what follows it is important to understand the details of the Android OS and how it is controlled by Google. Android originated as an operating system for digital cameras and was compiled by making use of existing open-source components, such as the Linux kernel, java and libraries of the programming language C. After Google bought Android in 2005, it initiated the Open Handset Alliance (OHA) in 2007, which is the main contributor to the Android Open Source Project (AOSP). The OHA is comprised by device manufacturers, application developers, mobile carriers and chip makers. However, although in theory anyone can contribute to AOSP, Google remains very much in control and through a hierarchical organizational structure, code changes to AOSP eventually need to be approved by Google (employees). Google also remains the main contributor to AOSP. AOSP is licensed under the Apache license, which in principle means that it can be freely used, modified and distributed. This open-source character of AOSP makes it very popular among non-Apple device manufactures, many of which are members of the OHA. Members of the OHA mainly modify AOSP code to customize it to their devices and business models. Google sponsored AOSP, because it was concerned that Apple could become too dominant in the mobile market otherwise, which could then also endanger Google's dominance in search. In view of being a later-comer, the open source strategy was a clever move to quickly gain market share of AOSP. However, the open source strategy comes at the price that it can be modified and distributed by anyone. Such modifications of the main AOSP are known as 'forks'. In this context, it is important to distinguish between forks that are approved by Google, and those forks that are not. Moreover, it is important to distinguish between Android (which is a trademark of Google) and the AOSP, which is the open source code-based that can be used and modified without prior consent from Google. Only Google-approved forks of AOSP (mainly coming from members of the OHA) can be called and marketed under 'Android' and participate from the benefits of the Android ecosystem, such as software development kits (SDKs) provided by Google. Other forks must be labelled differently. One of the most prominent non-Google approved AOSP forks are Amazon's fireOS and the non-commercial lineageOS.

The main difference between Google-approved forks (passing certain compatibility tests and requirements set forth by Google and non-Google approved forks is that the latter do not qualify for licensing of Google's proprietary apps, which are known as Google Mobile Services (GMS). Over time,

²⁷ This is not inevitable from a technical perspective, however. In theory, iOS could also be run on non-Apple hardware.



Google has developed more and more apps under a non-open-source, proprietary license that updated and extended existing functionality of the AOSP – and at the same time, stopped developing the same functionality further as part of the AOSP. For example, there is an AOSP version of Google search, which is free to use but deprecated, and a Google proprietary version of search, which is being developed further. The same is true for other key apps, such as calendar, keyboard, camera, maps and photos.²⁸ Most importantly, the Google PlayStore (the mobile application store) and Google Play Services are proprietary to Google and need to be licensed. Especially without these latter apps, consumers would lack immediate access to the millions of apps that are available in the Google Play Store, or some apps that integrated some of Google’s services (e.g., advertising, cloud messaging, maps) would not function properly and cannot be readily used on their device. Taken together, the AOSP operating system has become more and more dysfunctional without the GMS license, which however is controlled by Google.

In order to obtain a GMS license, also called Mobile Application Distribution Agreement (MADA) OEMs have to agree to further contractual terms and undergo further certification by Google. The MADA agreement was also at the centre of the EC Antitrust Case against Google, mainly (1) because Google required that OEMs with a GMS license were not allowed to produce any devices with non-Google-approved Android forks, even if those were to be shipped without proprietary Google apps (anti-fragmentation provision), and (2) because Google bundled its search app and browser app Chrome together with the Play Store and required to pre-install these apps prominently on the home screen. Accordingly, following the EC’s Android case in 2018, Google had to offer the GMS license also without Google search and Chrome, and could not forbid OEMs to manufacture also other devices with AOSP forks that were not approved by Google.


Nevertheless, Android forks, even if they are not approved by Google, are generally compatible with each other, as they use the same underlying software architecture, most importantly the Linux kernel. As detailed in Section 2, Android is based a monolithic kernel and hence there is less flexibility in adapting the OS. On the positive side, this means that Android-based OS (forks) are less different from each other and it is usually technically possible to install the same apps on all Android forks (including non-Google approved forks) without access to the Google Play Store. Android application packages (so called APK) can be downloaded, for example, from repositories like APKMirror or APKPure. It is technically also possible (albeit not necessarily legal) to install most of the services included in the GMS bundle on a non-Google approved fork, although GMS will never be pre-installed on non-approved forks.²⁹ We mention all of this to highlight that Android forks are generally compatible with each other from a technical perspective. Indeed, OEMs probably also have strong incentives to maintain such general compatibility due to the inherent network effects. Incompatibilities and restrictions on the use of Android apps across AOSP forks are therefore mostly of a contractual nature and could be overcome from a technical perspective.

However, this is not to say that all OS that have some ties to AOSP, or significant own developments based on AOSP will maintain a basic compatibility. For example, in recent years Huawei has developed an own OS, called HarmonyOS. Supposedly, this has some origins in AOSP, but has been developed further significantly and is also based on different software architecture, known as a microkernel. Although the details are not publicly known yet, HarmonyOS is most probably not compatible with AOSP or Android due to the different architectural principles (microkernel OS vs. mono). HarmonyOS is also designed to run not only on smartphones but also on laptops and other devices. It will be interesting to see how this new operating system develops, since Huawei is the largest OEM in the Chinese market, and also a significant player in Europe (see above).

Suppliers of OS may also supply the hardware device, as Apple does for all iOS devices, Huawei plans to do with harmonyOS, and as Google does for some Android devices; or they may license their OS to third party hardware suppliers, as Google licences Android (on a royalty-free basis) and as Microsoft (Mobile OS) and Mozilla (Firefox) did until they were discontinued. As with hardware, the

²⁸ For a comparison, see <https://arstechnica.com/gadgets/2018/07/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/>.

²⁹ For example, lineageOS provides a tutorial for installing various apps from GMS: <https://wiki.lineageos.org/gapps.html>.



OS will be designed and configured to meet the needs of the supplier's customers, although Google has also made an open-source royalty-free version of the Android OS available to third parties to 'fork' by modifying the code and adding their software if they wish. Other hardware suppliers can then implement the new OS on their devices, but only after Google has done so on its leading device.

Thus, in conclusion, the hardware layer together with the operating system layer (based on Android forks) can be supplied competitively. However, this consideration excludes the application discovery and the application layer. Such devices may ship without easy access to a large variety of applications, including key applications such as the dominant app store. The competitive landscape in China is characterized by such an environment, where Android-based smartphones generally ship without GMS installed. The fact that Google was able to convince OEMs to sign a MADA which included a prohibition on distributing Android forks, also highlights that (1) Google regarded it as likely that non-Google-approved forks could compete with Google Android, and (2) that Google's control of the dominant app store for Android, the Play Store (which is located at the application discovery layer), was a key input that allowed it to exercise control over the operating system layer.³⁰

Our conclusion that the hardware and operating system layer can be supplied competitively currently hinges on the existence of the further development of AOSP, which is led by Google, and the ability to derive forks thereof.³¹ Because Google is the lead developer of AOSP, it also controls the timing of the release of new versions of the Android OS, and will release a new Google device which incorporates the latest OS when an upgrade is announced, so it has a first mover advantage³². Nevertheless, Google's Pixel devices have not reached a significant market share in Europe, as shown above. Generally, the ability to develop devices based on AOSP forks provides opportunities for OEMs to compete based on functional devices. A functioning device competition based on Android will probably also create some competitive pressure on iOS-based devices (as Android-based and iOS-based devices are substitutes to some degree), although to a lesser extent than between Android-based devices (as these are likely to be closer substitutes). Moreover, our qualifications regarding the existence of a termination monopoly and the relevance of device ecosystems still apply, which means that even if the hardware-OS-bundle can be supplied competitively, OEMs will retain some market power, which can result in potential 'device neutrality' issues.

3.3.2 Possible issues


The OS is, of course, tightly intertwined with the device itself, and thus, similar issues as those at the hardware layer may arise. That is, theoretically, a firm controlling the *operating system level* could

- privilege, restrict or prohibit access to certain networks (mobile, ad-hoc or infrastructure networks);
- prohibit or inhibit the installation of the operating system on certain hardware;
- reserve or privilege system resources (e.g., battery, memory, computing power, (data) storage) for specific apps;
- privilege, prohibit, inhibit or restrict software at higher layers to access hardware components (e.g., sensors, chips, camera, microphone, screen);
- prohibit, inhibit or restrict compatibility with certain applications and devices;
- pre-install certain applications and restrict removal of some or all of these applications;
- integrate certain applications more tightly in the operating system and user workflow (e.g., voice and zero-click activation, background performance, notifications).

³⁰ The potential withdrawal of other core services provided by Google at the application layer (which are or were part of GMS), particularly Search (as found by the EC in its Android decision) also contributed to the ability to exercise control of the OS, although, arguably, access to the Play Store is the most important of these in the present context.

³¹ It is yet too early to say whether HarmonyOS, which is also developed open-source, may become a serious competitor of Android/AOSP. In any event, it is likely that also then the market will not support more than two mobile operating systems in the long run.

³² https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf, p. 128.



In the following, we particularly focus on two issues that have been subject to some debate. (1) the pre-installation of apps, and (2) API access restrictions to OS functions.

3.3.2.1 Pre-installing apps

Almost all digital devices will be supplied with software that is pre-installed on the device before the user purchases it. All devices require an operating system (OS) to run applications and services and, although it is possible to download an OS (and very common to update pre-installed OS via downloads), users expect a new device to be supplied with an OS already installed. In addition, users will generally expect a device to be supplied with a significant number of applications pre-installed.

Decisions about the pre-installation of software and applications (as opposed to the OS) have important implications for competition given the power of 'defaults' in digital services markets. Although, as discussed below, devices may allow users to download applications which could substitute for those that are already pre-installed on the device, a user will have to be sufficiently motivated to take the time and effort to do so. Some users may find it difficult (and some devices may make it difficult) or they may assume that pre-installed applications and services are more likely to run reliably on the device (or that they are otherwise 'approved' by the device supplier). The competitive value of pre-installation for providers of applications and services can be illustrated in various ways³³. For example, some surveys suggest that despite vast array of apps that are available for download from both the Apple (over 4 million) and Google (around 3 million) app stores, the majority of users have only downloaded a relatively small number of apps (around 10) to their device³⁴. There is also evidence that users are downloading fewer apps today than in the past, perhaps because they have now found the (relatively small number of) apps they like to use on a regular basis and perceive limited value in downloading a 'long tail' of apps which may consume memory and battery power on their devices.

Evidence of the commercial value of pre-installation is also provided by the value of the payments which third parties are prepared to make to device vendors to be pre-installed on devices. The European Commission found that Google had agreed to share search advertising revenues with device vendors in return for a commitment that they did not pre-install a search service on any of the devices within a defined portfolio. The UK Competition and Markets Authority found that Google paid Apple €1.35 billion in 2019 to be pre-installed on devices sold in the UK³⁵.

This also illustrates the potential value of exclusivity for OEMs. Purchasers of new devices expect to find the applications they commonly use pre-installed and easy to locate. But users may also be wary of 'bloatware' in the form of other pre-installed applications to which they attach little or no value (or which duplicate functions undertaken by other applications) but which will consume memory and power on the device (as well as potentially extracting personal data about the user, about which users may not themselves be aware³⁶). A consequence of this is that devices will typically come pre-installed with applications to support the most popular functions for which the device is, with less popular 'long tail' applications being left for the user to download for themselves. Constraints on the number of applications that can be pre-installed - as well as the importance of the location of applications on the home or other screens - enable device manufacturers to monetise these arrangements and to use prices to allocate resources on the device.


Google's control over pre-installation was enforced by means of a set of contractual arrangements with device manufacturers and mobile operators which, as discussed above, the European Commission concluded were intended to exclude (and had the effect of excluding) the pre-installation of rival services on Android devices as well as discouraging device manufacturers from developing their own 'forked' versions of the Android OS. The Commission also found that the Google Chrome and Google search apps could not be uninstalled from Android devices. The Commission was therefore concerned that an integrated firm with gatekeeper control would use contractual and

³³ The issue is discussed at length in the Google Android decision, para 786-.

³⁴ <https://mindsea.com/app-stats/>.

³⁵ https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, para 33.

³⁶ https://haystack.mobi/papers/preinstalledAndroidSW_preprint.pdf.



technical restrictions to ensure that OEMs discriminated in favour of Google applications and services, and against rivals, when deciding what software to pre-install on the devices which used the Android OS.

Google has subsequently announced that it has removed the restrictions from its agreements with device manufacturers, allowing them to develop their own forked versions of the Android OS without foregoing access to other Google apps and services, and will allow manufacturers to pre-install the GMS suite without them also having to pre-install Chrome or Google search. Instead, Google now requires the payment of a licensing fee for the Google services in question, but with Google Chrome and search being licensed separately for no fee³⁷. Google will also allow device OEMs to pre-install third party apps alongside Google's. These changes are intended to allow OEMs that use the Android OS to 'mix and match' pre-installed services and apps, both Google and non-Google, on their devices if they wish to. This does not, however, address the question of how OEMs might be compensated for agreeing to pre-install some applications and services and not others. Google will license Chrome and Search on a no fee basis, but it is conceivable that other application and service providers would be willing to pay to be pre-installed, or that OEMs might require payment to do so. These OEMs may therefore discriminate between different third party app providers, even if they do not themselves participate in the market for apps or other software.

Pre-installed software therefore raises a number of issues. The Google Android case highlighted the ability of a supplier of a pre-installed OS to require an OEM to pre-install other services and applications that are supplied by the same firm. There are also questions such as how an OEM should then determine which applications or services are to be pre-installed on the device. Is it reasonable for them to allocate space or positions on the device by reference to commercial considerations like the size of the financial payment which a particular applications or service provider is prepared to offer for pre-installation? In different context, Google has adopted an auction format to allocate slots for search engines that wish to appear in the set up screen for Android devices, allowing users to choose which search services they wish to have as their default in the browser³⁸. Critics of this remedy have argued both that it still discriminates in favour of Google's own Search service and that software providers ought not to be obliged to pay to access a service over which Google enjoys gatekeeper control. They argue instead that some other 'more neutral' means of selecting participants should be employed, although views differ about what this should be. This echoes the debate about the role of 'pay for priority' as a market-based mechanism employed by IAS providers to allocate capacity between different services on their networks³⁹. In the event, 'pay for priority' was prohibited in the United States, leaving IAS providers to rely upon 'best efforts' for the delivery of services to users. 'Best efforts' is a core element of the architecture of the internet, but there is no equivalent rule for determining how apps might be selected for pre-installation on a device.

Finally, some applications that are pre-installed may be 'hard wired' into the phone and incapable of being fully uninstalled (sometimes they can be removed from the screen without being deinstalled). For example, Apple allows to deinstall most of the pre-installed apps, but those apps will still consumer storage space on the device after they were de-installed.⁴⁰ In some cases this could be justified as the application is an integral part of the OS, without which the device would not function properly. However, there may other cases where the intention is to discourage users from switching away from the integrated firm's services or applications. Third party applications which are subsequently downloaded by the user themselves can always be uninstalled and a significant proportion of these apps are indeed uninstalled within a relatively short period of time⁴¹.

3.3.2.2 Access to OS functionality

In addition to concerns about how decisions are made about which applications and services to pre-install on devices, there may also be concerns about the way in which applications can run on a


³⁷ <https://www.blog.google/around-the-globe/google-europe/complying-ecs-android-decision/>.

³⁸ <https://www.blog.google/around-the-globe/google-europe/update-android-search-providers-europe/>.

³⁹ See Stocker and Knieps p.135 at <https://www.degruyter.com/downloadpdf/journals/rne/17/3/article-p115.xml>.

⁴⁰ <https://support.apple.com/en-in/HT211833>.

⁴¹ <https://www.businessofapps.com/news/mobile-app-uninstall-rate-after-30-days-is-28-according-to-appsflyer/>.



device. We explained earlier how this can be influenced by control over access to the hardware components on the device, but it can also be influenced by the extent to which features and functionality within the OS are revealed to third parties to enable them to develop applications and services which run upon it, or the way in which permissions are managed when apps request access to certain functions or data on the device (e.g. whether user consent is required or not)⁴².

Concerns might arise, for example, if an integrated firm that controls an OS platform were to restrict access to functionality in the operating system which would be required if third party software providers were to compete effectively with the software or services produced by the integrated firm. In such a case, the integrated firm would be granting itself preferential access to functions in the OS. The ACM reports that Spotify has complained that its app cannot interoperate with Siri, Apple's voice activated interface, whilst Apple's own Music service does⁴³. But such discriminatory access may not be restricted to vertically integrated apps. For example, Apple granted Uber access to a hidden APO, which enabled Uber to record the screen of the smartphone, without the consumer knowing about it. Such access was not granted to other firms.⁴⁴

As already explained, OS providers will wish to promote complementary innovation and provide access to functions which they think will support new services which will contribute towards the growth and expansion of the OS platform and the wider eco system. It is important to make a distinction here between complementary innovation (which enhances the device with functionality or services that would otherwise not be present) and substitutive innovation (which seeks to replace or marginally improve upon existing functionalities or services). Incentive issues of the OS provider will generally only arise from substitutive innovation, rather than complementary innovation. Specifically, complaints may arise from third party application developers not because they cannot access functionality on the OS, but because the purposes to which that functionality can be put may be circumscribed by the gatekeeper controller in light of the purposes to which it is put. Thus, albeit in a different context, the FTC alleges that Facebook has imposed restrictions on the purposes for which its APIs can be used in order to restrict competition and withdrawn access to APIs from third party developers who have used them to develop services which may threaten those of Facebook itself⁴⁵. The latter conduct suggests that OS controllers may sometimes expose APIs in order to promote complementary innovation by third parties on their platform, but then subsequently withdraw access and copy the functionality developed by those third parties into its own OS. In this way the boundaries between functions which are incorporated within the OS and those that are provided via APIs can prove to be quite fluid over time.

OS providers will also control whether and how other information which can be used by third party advertisers and others to identify the device or the user of the device. This includes access to mobile advertising IDs (MAID), which are accessible to apps (and to advertisers who embed code in those apps) so as to enable the serving of personalised adverts to users of apps (MAIDs identify the user by reference to the identity of the device). It also includes IMEI and IMSI data which may identify the unique device and the SIM card which is required to authorise the connection of the device to a mobile network. This data may be disclosed to some apps with user permission, but the OS controller may again do so in a manner which favours some applications over others.

3.3.3 *Application discovery layer*


The application discover layer is comprised of apps that facilitate consumer's access to other apps or content and have therefore, in principle, the ability to prohibit, inhibit or otherwise influence the

⁴² See CMA para 80- for a discussion of the permissions models for iOS and Android.

⁴³ ACM, p. 82, See also ARCEP p.42: 'Google was able to take advantage of its privileged access to certain Android functions to obtain the list of the relay towers in smartphones' vicinity. These data could help improve location-based services, but third-party apps do not have access to them.'

⁴⁴ See <https://gizmodo.com/researchers-uber-s-ios-app-had-secret-permissions-that-1819177235>.

⁴⁵ 'For many years— and continuously until a recent suspension under the glare of international antitrust and regulatory scrutiny — Facebook has made key APIs available to third-party apps only on the condition that they refrain from providing the same core functions that Facebook offers, including through Facebook Blue and Facebook Messenger, and from connecting with or promoting other social networks', para 23 at <https://www.ftc.gov/system/files/documents/cases/1910134fbcomplaint.pdf>.



consumption of specific content. There are two main types of applications that are of relevance in this context: (1) app stores and (2) browsers.

3.3.3.1 App stores

App stores perform several important functions that are similar to physical stores and to other digital platforms. They allow users to search for, pay for and download a huge variety of applications produced by third parties which the user may themselves have never heard of. App stores are a classic example of a two-sided platform: More users of an app store attract more developers, and vice versa, such that there are strong indirect network effects at play. As is well known, markets with two-sided platforms tend to tip towards the largest platform, even if there is competition between such platforms in the beginning. Under iOS competition between app stores has been ruled out from the start, whereas under Android it is possible to install several app stores in parallel (also before the EC's Android decision). While this may not be frequently exercised in Europe, due to the dominance of the Google Play Store, it is common practice in China, where the Google Play Store is not dominant.⁴⁶

The admission policies and other rules that are used by app stores to screen apps provide the user with assurances that the application they download will work on the device as envisaged and will comply with the rules of the app store controller. Additional assurances may be provided by the rating systems and user feedback which app stores offer. In this sense, the app store provider is a platform that acts as a "regulator" and ensures interactions with high (network) benefits. As with other e-commerce platforms, app stores will rank apps in response to search requests and will make personalised recommendations based on previous purchases and other user data. For app developers (many of whom are small firms), app stores provide a distribution channel to every device on which the app store application has been pre-installed. All Apple devices have the Apple Store pre-installed and the vast majority of Google Android devices will have the Google Play Store pre-installed⁴⁷. However, some Android device manufacturers may also pre-install their own app store on the device (alongside the Google Playstore). Samsung, Huawei and Xiaomi all do this. In addition, there are number of providers of third party apps stores which are independent of either the device manufacturer or the controller of the OS. These include Aptoide, GetJar and specialist services for gamers or other groups such as Itch.io.

As noted earlier, admission to the app store can be thought of as the primary means by which integrated firms like Google and Apple perform their gatekeeper role in relation to apps. Technical access to the same set of APIs and SDKs is generally available to all developers, but admission to the Google or Apple app stores are governed by a complex and extensive set of rules. Thus, for example, the Google Play Store developer agreement prohibits to admission of third party app stores such as Aptoide or those offered by device manufacturers into the Play Store⁴⁸. This means that Android device users who wish to access apps via third party apps stores must either 'side load' the app onto their device or it must be pre-installed by the device manufacturer. Apple prohibits side loading of apps on its devices, although more sophisticated Apple users may 'jail break' the iOS and then sideload unauthorized third party applications (albeit with the risk that their Apple device is then out of warranty and both the device and data on it may be exposed to significant security risks). A small number of apps are so popular that they can bypass the app stores of Google and Apple – the popular game Fortnite is an example, being an app which is downloaded directly from the Fortnite website rather than being listed in the Play Store⁴⁹.

⁴⁶ For an analysis of the Chinese app market, see Wang et al (2019). Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets. IMC 18 Proceedings of the Internet Measurement Conference, pp 293-307. <https://doi.org/10.1145/3278532.3278558>.

⁴⁷ As noted earlier, since 2018 Google has allowed device manufacturers supplying products in Europe to licence the Android OS without also licensing the Play Store and Google Play Services. Amazon devices using its forked Android OS, Fire, have the Amazon app store pre-installed upon them.

⁴⁸ <https://play.google.com/about/developer-distribution-agreement.html>, para 4.5.

⁴⁹ Fortnite was listed in the Apple store, since users cannot sideload apps on iPhones, but has recently been removed following its dispute with Apple about commission fees.

Application developers submitting apps for admission to the Google or Apple apps stores have made many allegations over the years, generally on the basis that the integrated firms have commercial incentives to restrict access to their app stores which they may misrepresent as being for technical, security, privacy or other reasons. Developers have claimed that they have no independent rights of appeal if access is denied, and that it is often unclear what steps they should take in order to overcome the objections which Apple or Google raise.⁵⁰

More recently, concerns have arisen not in relation to whether third party applications are admitted to the app store, but to the conditions, particularly the management of payments made by users of apps, which are imposed as a condition of entry. The European Commission is currently investigating the terms which Apple apply in requiring third party apps to use Apple's payments platform to process all in-app payments in return for a significant (30%) commission fee and which restrict the ability of app providers to provide users with alternative payment methods, following complaints by Spotify and others⁵¹. Epic, the company responsible for Fortnite, has been or is litigating against Apple in the UK⁵², US, Australia and most recently also filed an antitrust complaint in the EU.⁵³ Google imposes similar conditions on third party app providers and charges the same level of commission⁵⁴. In these cases, the complaint is not that firms are preventing third party applications from accessing their app stores or constraining the way in which third parties develop apps in order to favour their own services but that the app store controllers are exploiting their gatekeeper position by imposing unfair commercial terms⁵⁵. On this view, Apple and Google may have incentives to encourage the development of complementary applications which generate significant revenues, but they are also able to extract an unfair share of those revenues for themselves. Some services providers, including Spotify and Netflix, encourage users to bypass the app store controller by subscribing to their streaming service via their website instead, in order to avoid the in-app purchase commission fee⁵⁶.

Currently, the large app stores tend to apply a standard commission fee for payments made on all third party apps (exceptions apply for small developers)⁵⁷. Concerns might arise, however, if the app store controller were to require very different levels of commission from different types of apps, or from different apps of a similar type⁵⁸.

Again, we can only highlight a number of the possible 'device neutrality' issues here. Theoretically, a firm controlling the *app store* could ...

- deny, unduly delay or discriminate access to the app store based on (legal) app content, app functionality or identity of the app developer;
- discriminate commission rates based on app content, app functionality or identity of the app developer;
- bias, distort or restrict "findability" of certain apps based on (legal) app content, app functionality or identity of the app developer.
- require or prohibit apps to use ancillary services and functionalities (e.g., payment services, push notifications, reporting services)
- require apps to share data or deny access to data in discriminatory way;

⁵⁰ <https://www.acm.nl/sites/default/files/documents/market-study-into-mobile-app-stores.pdf>.

⁵¹ https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073.

⁵² 1377/5/7/20 Epic Games, Inc. and Others v Apple Inc. and Another - Summary of claim | 14 Jan 2021 (catribunal.org.uk)

⁵³ <https://www.epicgames.com/site/en-US/news/epic-games-files-eu-antitrust-complaint-against-apple>.

⁵⁴ <https://support.google.com/googleplay/android-developer/answer/9992660>.

⁵⁵ Although it is argued that any commissions relating to the apps of the integrated firms will be an internal transfer within the firm rather than a cash cost of the kind faced by the third parties, which enables the integrated firm to 'pay' fees which third parties cannot afford.

⁵⁶ https://en.arcep.fr/uploads/tx_gspublication/report-state-internet-2019-eng-270619.pdf, p.63

⁵⁷ <https://support.google.com/paymentscenter/answer/7159343?hl=en-GB#:~:text=The%20transaction%20fee%20for%20all,distribution%20partner%20and%20operating%20fees>.

⁵⁸ For example, Apple requires a revenue share of 30% from subscriptions, paid apps and in-app purchases, except for developers which earn less than 1 million USD, who are required to share 15% of revenue. See <https://www.apple.com/uk/ios/app-store/principles-practices/#:~:text=Apple%20only%20earns%20a%20commission,then%20used%20within%20the%20app>.

- prohibit or inhibit its installation on certain operating systems or devices;

3.3.3.2 Browsers

A browser is a software programme which allows users of a device to navigate between web pages using a graphical interface⁵⁹. It allows users to find and engage with third party content and services that have not been pre-installed on the device itself. Most devices will be supplied with a browser pre-installed on the device, but other browsers may subsequently be downloaded and installed. Users access services and applications through browsers when using PCs, smartphones and other devices, although apps tend to be more commonly used on smartphones⁶⁰.

The market for mobile web browsers has become highly concentrated in recent years. The leading mobile browsers in Europe (and worldwide) are Google's Chrome (about 60% market share), Apple's Safari (about 29% market share), and Samsung's browser (about 8% market share), see Figure 4. These figures are remarkable in number of ways.

First, Safari is only available on iOS, and its market share corresponds to that of iOS⁶¹. Apparently almost every iOS user also uses Safari as the default browser. This is not surprising in so far as under iOS all browsers need to use the same rendering engine (Web Kit) provided by Apple, and thus no real differentiation between browsers in terms of performance is possible.⁶²

Second, these numbers show a clear default bias for the pre-installed browser. Safari is the pre-installed browser under iOS and Chrome is typically pre-installed on Android devices (in part thanks to Google's licensing terms, particularly prior to the EC Android decision), and Samsung's browser is additionally pre-installed on Samsung's smartphones, which have the largest market share among the Android-based devices. The open-source AOSP browser, which was once popular, because it came pre-installed with Android, lost popularity, as Google discontinued to develop it further as part of AOSP, and diverted attention to its proprietary Chrome browser (as it did with other AOSP apps, as discussed above).

Third, there are evidently significant indirect network effects at work in the market for browsers. Websites will optimize their appearance with respect to the dominant browser rendering engines. For iOS this is Apple's WebKit, and for Android this is Google's Blink engine (part of the Chromium project), on which both Chrome itself, but also Samsung's browser are based. Taken together, this means that there is de-facto just one dominant browser (respectively rendering engine) for each OS. Moreover, in each case, the dominant browser is controlled by the firm that also controls the OS, and who also controls the dominant app store for that OS.

⁵⁹ Browsers present visual displays of content but in some devices voice-activated interfaces (Siri or Cortana) may perform the navigation function and provide a verbal description of the content.

⁶⁰ Studies suggest that US smartphone users spend 90% of their time with services accessed via apps rather than browsers, see <https://www.emarketer.com/content/the-majority-of-americans-mobile-time-spent-takes-place-in-apps>.

⁶¹ Note that Figure 3 and Figure 4 use different data sources and do not cover exactly periods, which can explain the slightly higher market share for Safari than for iOS. Worldwide the market share of Safari on iOS devices has been estimated to be around 93%, while Chrome retains only about 4,5% (<https://review42.com/resources/browser-usage-statistics/>).

⁶² Safari is not the only browser available on iOS, however. Alternatives include Chrome, Edge, Firefox and DuckDuckGo, all of which can also be set as the default browser. See <https://www.theverge.com/21444995/ios-14-default-browsers-chrome-edge-firefox-duckduckgo-safari>.

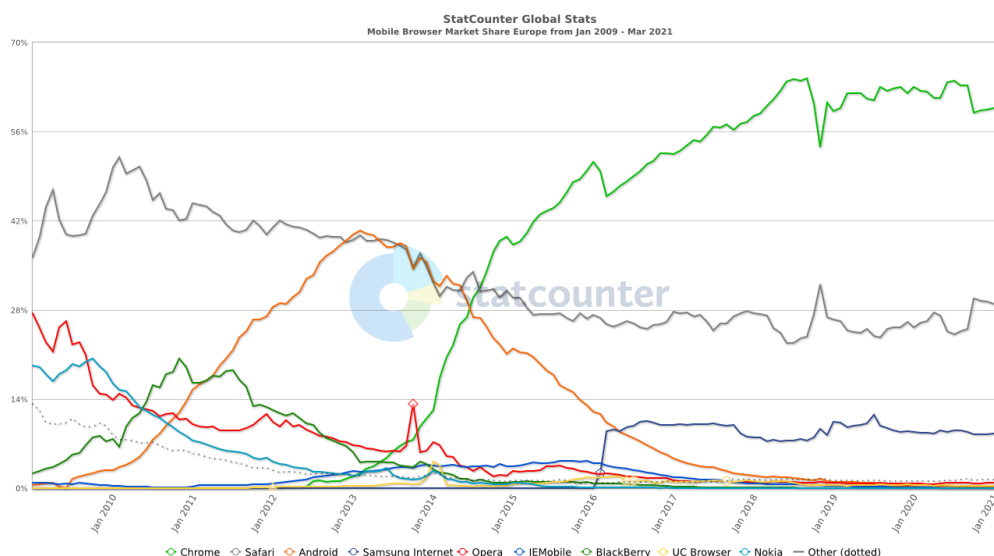



Figure 4: Market share of mobile web browsers in Europe, Source: Statcounter

In this sense, the application discovery layer is really controlled by just one firm for each OS, Google or Apple, respectively, independent of whether content is accessed via native apps or via the browser. Apps are often preferred by users because they are specifically configured to interoperate with and run on the OS on the device in question, ensuring that the application runs properly and exploits all the features and functionality that is available on the OS (apps of this kind are referred to as 'native apps'). However, users can also access 'web apps' via their browser. Unlike native apps, web apps are designed to operate on any OS and run on the server hosting the app rather than being downloaded and run on the device itself. Native apps are generally regarded as having superior performance (since they are specifically designed for the OS on the device and performance may not depend on the quality of an internet connection), but require updates to be downloaded to the device (which web apps do not). 'Progressive web apps' have many of the features of conventional web apps, but perform better than web apps and can be run offline, much in the same way that native apps do. Many commentators nonetheless consider that progressive apps retain significant disadvantages relative to native apps⁶³. The main advantage of web apps is that they do not need to be installed on the device, and hence, also do not require access to the app store. Thus, web apps provide an alternative route for developers to reach consumers, which is not subject to the gatekeeping control of the app store. However, the degree to which web apps can perform similar to a native app, also depends crucially on the browser, and more particular, on the browser rendering engine. In this way, a browser can restrict the functionality of web apps (e.g. the ability to send push notifications) and therefore impact consumer's choice between web apps and native apps (access to which may be largely under the control of an app store). Whether a browser can provide an alternative route to consumers that can alleviate gatekeeper control will therefore depend on both the type of applications and the nature of the browser being used. The standards for progressive web apps, which are set mainly by the W3C, have been implemented differently for different browsers. Google's chrome browser has the most advanced implementation in this regard. While browsers can have their own rendering engine under Android, and therefore are very much in control themselves about the adoption of web browsing standards, a particular issue arises under iOS. Apple requires all browsers under iOS to use its WebKit as the mandatory rendering engine. Thus, browsers under iOS are de facto just different graphical user interfaces, but cannot compete on web rendering or the use of new standards. Moreover, Apple has been quite slow in implementing new web standards, particularly related to progressive web apps, such as the so-called Service Workers.⁶⁴

⁶³ Estimates of progressive web app use are difficult to find. One commentator estimates that there are about one tenth the number of progressive web apps as native apps, <https://medium.com/@firt/progressive-web-apps-in-2020-c15018c9931c>.

⁶⁴ <https://love2dev.com/blog/apple-ships-service-workers/>.



This may be done strategically in an effort to retain control over apps via the app store and to avoid disintermediation.

In addition, the browser may display other content or other services, the nature of which will be determined by the provider of the browser. This may include paid for display advertisements, but also links to other applications and services provided by the browser provider (such as Microsoft or Google apps). Browsers also employ prefetching techniques, which determine preloading of websites that are likely to be clicked on next, such that they load faster. Such preloading can possibly also be biased and prefer certain websites over others.⁶⁵

In addition to leveraging other assets (such as OS) to favour their own browsers, controllers of browsers could engage in discriminatory conduct in relation to third party browser extension providers, or might favour some kinds of content over others for display in the browser. Google has been criticised by third party providers of ad blocking applications for changing the APIs which allow Chrome extensions to determine which ads to block as a webpage is loading⁶⁶. Critics claim that these changes reduce the ability of users of ad blocking software to block adverts or tracking software. Browser extensions can perform a wide variety of functions which will influence the way in which a browser user interacts with a webpage.

In addition to questions about how Google enables third party ad blocking extensions to Chrome, concern has arisen about Google's incorporation of its own ad blocking software into Chrome in 2018. Many ad blocking services filter adverts based on a 'whitelist' which is compiled by the service provider and inclusion in which advertisers may apply or pay for. Questions have arisen as to whether Google's whitelist would favour adverts which were served by Google's own adserving platforms, whilst blocking adverts served by rival platforms⁶⁷.

Some of these concerns go beyond those of 'device neutrality' and relate to the extent to which the controller of a popular browser may have incentives to limit the capability of third party ad blocking software in order to protect advertising revenues. But 'neutrality' concerns might arise if a browser provider were to restrict APIs to third parties so as to prevent them being able to offer browser extensions which were unable to match the capabilities of its own integrated browser, or if it were otherwise to discriminate between the APIs offered to different third parties or to block or otherwise impose discriminatory terms for admittance into the web store. Given that valuable but personal data is obtained from browsing activity, tensions may arise between those seeking third party access to data (e.g. through the insertion of third party cookies in the browser in order to track which websites the user visits) and concerns on the part of browser (and OS) providers to control access in order to safeguard user privacy. Users can block third cookies in their browsers, and some browsers (including Apple's Safari) have begun to by default⁶⁸.

Thus, the ability of third parties, such as adtech companies, to obtain access to user data is likely to be a significant issue in relation to device neutrality. It has arisen in relation to Google's latest initiatives to remove third party cookies from its Chrome browser and to implement a 'privacy sandbox'⁶⁹.


⁶⁵ ARCEP, ibid.

⁶⁶ <https://www.wired.com/story/google-chrome-ad-blockers-extensions-api/>. The changes reduce the number of rules that an extension may apply to a webpage as it is loading to check, for example, whether the page is loading from an advertisers' server.

⁶⁷ <https://theintercept.com/2017/06/05/be-careful-celebrating-googles-new-ad-blocker-heres-whats-really-going-on/>.

⁶⁸ https://assets.publishing.service.gov.uk/media/5fe49554e90e0711ffe07d05/Appendix_G_-_Tracking_and_PETS_v.16_non-confidential_WEB.pdf.

⁶⁹ <https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes>. Concerns have also arisen in relation to whether Chrome pre-loads Google-hosted Accelerated Mobile Pages faster than web pages hosted on rival platforms, thereby driving content owners to host content on the Google platform.



These are just some of the potential ‘neutrality’ issues that relate to browsers. In summary, a firm controlling the *browser* could

- privilege, restrict or prohibit access to selective content (e.g., block advertisements, set default starting page and default search engine);
- privilege, restrict or prohibit access to selective plug-ins / extensions;
- bias, distort or restrict “reachability” of certain websites or plug-ins based on (legal) content, functionality or identity of the website owner (e.g., discriminate with respect to the loading speed of certain websites, warning messages).
- privilege, restrict or prohibit websites’ or extensions access to the browser’s full functionality (e.g., javascript, service worker, stored data);
- prohibit or inhibit its installation on certain operating systems;
- reserve or privilege system resources (e.g., battery, memory, computing power, storage) to specific content;
- unduly delay or omit the adoption of web standards (e.g., in order to retain control over functionality reserved for native apps, especially if the firm controls the app store level as well).

3.3.4 Application layer

The number of apps in the app store is very large and the app market generally is very competitive. We don’t see any device neutrality issues that originate at the application layer as such.⁷⁰ Rather device neutrality issues that may arise at other layers may cause a distortion of competition at the application layer. More specifically, with respect to devices, this is usually due to pre-installation of apps by a firm that controls the OS layer, or preferential treatment of an app (or website) in the app store (or browser). In particular, self-preferencing is a concern if a firm controls either the OS, or the app store, or indeed both (as is currently the case), and also competes at the application layer.


3.4 Overview of conduct concerns

So far, we have explained that concerns about device neutrality and the gatekeeper control exercised by some firms arise despite the fact that many users use multiple digital devices to access digital services. That is because these devices are more often complements that substitutes, particularly when each form part of a common digital ecosystem that is controlled by a single firm. Each individual device provides the gateway through which the user will access digital services in a particular context or at a particular moment in time. Providers of those digital services are unlikely to be able to persuade a user to switch to another device or otherwise to disintermediate the firm holding gatekeeper control.

Gatekeeper power arises particularly at the application discovery layer, where browsers and app stores are located. For example, Google’s control over the dominant app store for Android, allowed it to impose strong contractual restrictions on OEMs. Issues also arise due to vertical integration, especially between the operating system layer and the application discovery layer. For example, this allows Apple to shut off alternative app stores, alternative browser rendering engines, or side loading of apps completely. Moreover, vertical integration between the operation system layer and the application layer, raises issues of self-preferencing from pre-installation or from preferential access to OS functionality. Likewise, vertical integration between the application discovery layer and the application layer raise issues of self-preferencing in the app store or in the browser.

We also argued that the operating systems layer and the application discovery layer are characterized by significant (indirect) network effects, and thus a market concentration seems inevitable here. This

⁷⁰ Although app stores are also ‘apps’, we considered them at the ‘application discovery layer’. Moreover, ‘neutrality’ issues that might arise from the dominance of some digital platforms, e.g. self-preferencing in search engines, are not considered to be an issue at the ‘application layer’ as such (although they may occur also ‘inside’ an app), but rather at the ‘content discovery layer’ (see Figure 1), which is outside of the scope of devices.



is contrary to the hardware layer that, if looked at in isolation, does not exhibit strong network effects (albeit strong economies of scale and scope) and could be supplied competitively in the long run.

In conclusion, we see that the main issues in the context of device neutrality arise at the operating system level and the application discovery layer, and especially so if both layers are controlled by the same firm. Three main theories of harm emerge in this context.

First, that integrated firms with gatekeeper control distort competition in related, normally downstream, markets by preventing those offering rival applications from having equivalent access to key hardware or software functions on the device. This may also prevent these rivals from threatening their gatekeeper position in the upstream market.

Second, that integrated firms with gatekeeper control exploit their position by levying excessive fees or commissions on any firm wishing to access the users of the devices in question through a convenient means, such as an app store. Related to this, the integrated firm may degrade other ways in which users might access third party applications or services (e.g. by degrading the experience through the browser) in order to force app developers to pay for inclusion in the app store⁷¹.

Third, that integrated firms with gatekeeper control distort competition in related, normally downstream, markets by directing users of devices towards their own services and away from those of rivals, either by pre-installing or requiring the pre-installation of their services on the device before it is sold, or through other means such as preferring their own services when returning search results. The extent to which this conduct is harmful depends on the extent to which users of a device have alternative means of discovering, downloading and installing third party services and applications onto their devices. Again, distorted competition in the downstream market may also protect the integrated firm's gatekeeper position in the upstream market and reduce the threat of disintermediation.

⁷¹ This is known as the 'dirt road' argument, Stocker and Knieps p.138, but is much disputed.

04

ARGUMENTS TO JUSTIFY 'NON-NEUTRAL' CONDUCT

4 Arguments to justify 'non-neutral' conduct

In the previous section we introduced different types of conduct which could be problematic if they distorted competition in related markets, particularly for apps. In this section we consider the arguments that are advanced to justify such conduct, or to suggest that any adverse competitive effects need to be balanced against other benefits. Many of these arguments are similar to those that were employed by controllers of access networks in the 'net neutrality' debate, although some are unique to devices.

4.1 Innovation and investment

A common, but contentious, claim is that firms will only invest significant sums and take significant risks to develop a new piece of device hardware, a new OS or a new software application if they are subsequently able to earn an adequate return on those investments. The integrated firm may only obtain a return by bundling other services with the asset or otherwise using its control of the asset to favour its own services. If the integrated firm were obliged to share the asset with its rivals on a 'neutral' basis then it would have a much reduced incentive to invest. It might prefer to wait until another firm took the risks, and then itself obtain 'neutral' access to their hardware, OS or other software platforms. In consequence, investment in new hardware and software would diminish and the rate of innovation would slow.


A version of this argument arose in the Google Android case referred to earlier, where Google had made significant investments in the Android OS and Google Play software which it sought to recover not from licensing fees to device manufacturers, but from advertising revenues which it expected to generate as a result of the user data and search queries it would obtain as a result of requiring OEMs to pre-install Google applications, including Google Search, on devices which used the Google Android OS. Following an adverse finding by the Commission, Google has decided to license the Google Play software for a fee (although it did not introduce a fee for the Android OS, Chrome, or Search).

In some respects this may be an issue about the business models which integrated firms choose to adopt rather than whether the firms can earn a return on the assets they control. A 'neutrality' obligation may increase competition in related markets and so reduce the returns which an integrated firm may expect to earn in that market, but it does not obviously or fundamentally diminish its gatekeeper control or capacity to charge for access to that asset under a different set of arrangements. Only if regulators were to go one step further and prohibit or otherwise restrict the charges for access to assets would the integrated firm be unable to earn a return on the investments which it has made.

We also need to recognize that competition between vertically integrated firms may mean that some business models are more efficient or competitive than others. Conduct which may distort competition within a particular supply chain might nonetheless be justified if it contributes to greater competition between different ecosystems. Indeed, the economic literature suggests that competition between 'systems' tends to be more intense than competition between independent producers of system components.⁷² One reason for this is that after consumers have opted for an ecosystem, switching is more costly for them (as we have explained above), which makes them loyal and valuable customers. This, in turn increases competition for users that have not yet decided which ecosystem to join. As we explain below, Google argued in the Android case that an important benefit of the restrictions it imposed on device manufacturers was that they enabled Google to supply the Android OS at no fee, which in turn supported the production of low cost Android devices which would then provide a competitive constraint on the (higher cost) Apple devices. Google's argument was that some loss of competition within the Android ecosystem might be justified if a consequence was greater competition between Android and iOS devices⁷³. At least in the Android case, the EC found

⁷² For a seminal paper, see Matutes, C., & Regibeau, P. (1988). "Mix and match": product compatibility without network externalities. *The RAND Journal of Economics*, 221-234.

⁷³ See Bijl and van Gorp, p. 19 and p.26 (discussing a similar argument in relation to the Google Shopping case and a competition with Amazon). This is known as 'moligopolistic' competition – or competition between monopolies (each of whom may otherwise be unchallenged by other potential entrants who lack the network effects and other advantages of these monopolists).



that iOS and Android were competing in different relevant markets and that there would be little competitive pressure between them. We can only speculate on this here, but clearly Android-based and iOS-based devices are substitutable to some degree, and the steady (but asymmetric) market shares do not contradict the notion that there is active competition. Nevertheless, we have also argued that the lock-in into device ecosystems can be a powerful source of switching costs.


Another argument is that some degree of discrimination is inevitable and necessary with devices, as it is with networks, given resource constraints. For example, a non-neutral device which could support all software applications at the same time or allow all apps to be pre-installed would require a battery, processor and screen so large and expensive that the device would be both unusable and unaffordable for users and unprofitable for the producer of the device. Moreover, users would likely be overwhelmed with the amount of apps pre-installed and find it difficult to navigate through and use the device. In a similar way, broadband networks providing internet access have capacity constraints which are difficult and costly for the network operator to overcome, and for which users may in any event be unwilling to pay. On this view, discrimination in the way a device supports services and applications is a necessary way of ensuring that scarce resources on the device are allocated in a way which reflects the willingness of users to pay. Moreover, consumers also have scarce resources in terms of attention, so some pre-selection of 'useful' apps can be valuable to them. This maximises the return on the investment in the production of the device and contributes the efficient consumption of resources. This, in turn, may contribute to higher levels of investment in the development of devices, and to higher levels of innovation as well.

Openness and non-discrimination, which are the main guiding principles of a neutrality regulation, are also not necessarily the right approach to stimulate innovation and investment. In particular, research on open and closed platforms or ecosystems has shown that there typically exists an inverted U-shaped relationship between the degree of openness of a platform and innovation by or on the platform.⁷⁴ Thus, a medium degree of openness is often optimal for innovation and investment, where platforms open up to outside complementors (e.g. by allowing third party application developers on the platform), but yet remain in control over access to the platform. There are two main reasons for this result.

First, in very open platforms, it is difficult to manage security, quality of the complements and hence quality of user experience and integrity of the platform. This drives down the average value of the platform for the consumers, and the platform becomes too congested on the supply side. Hence this also reduces the incentives of third party complementors to contribute to the platform. That is, a paradox arises where complementors avoid the platform, precisely because it is too open. In reverse, a platform that is too closed will miss out on the opportunity to invite third party complementors and thereby stifles innovation.

Second, open platforms require a certain degree of modularity. That is, openness and the integration of third party complementors are achieved through well-defined interfaces (e.g., apps interacting with the OS via APIs). This design is well suited for incremental innovations, because innovation can occur in each module (e.g., apps) independent of changes of the platform or of other modules. Likewise, innovation can occur at the platform (e.g. a new OS) and yet retain functionality of the complements (e.g. the apps), as long as the interfaces (e.g. APIs) remain the same. This is a main reason for choosing a modular design. However, in such a modular, open design, that involves many complementors, it is more difficult to approach radical innovations, e.g., innovations that would also require a fundamentally different modularity, and hence different interfaces. Thus, openness is not a matter of black and white, and more than likely an intermediate degree of openness is optimal for

⁷⁴ See Boudreau, K. J. (2012). Let a thousand flowers bloom? An early look at large numbers of software app developers and patterns of innovation. *Organization Science*, 23(5), 1409-1427. Parker, G., & Van Alstyne, M. (2018). Innovation, openness, and platform control. *Management Science*, 64(7), 3015-3032. Tilson, D., Sorensen, C., & Lyytinen, K. (2012, January). Change and control paradoxes in mobile infrastructure innovation: the Android and iOS mobile operating systems cases. In 2012 45th Hawaii International Conference on System Sciences (pp. 1324-1333). IEEE.



innovation and investment. Moreover, the trade-off between openness and innovation is also dependent on the (technological) and market maturity of the platform.

Taken together, if platform owners were not vertically integrated, they would have a strong incentive to navigate the degree of openness of their platform in a welfare maximizing manner, because they would have an incentive to maintain a high degree of innovation and investment on the platform, which they can then monetise. Such incentives may be distorted in case of vertical integration (which we discuss below) but they will not completely vanish.

Consideration of investment and innovation should also consider the incentives of third parties who may themselves invest in new services or applications. In this case, the incentives are ambiguous. On the one hand, if a gatekeeper is able to favour its own services and applications (or excludes others altogether) then this may force its rivals to replicate the upstream assets themselves. For example, an app developer might develop its own forked version of the Android OS in order to then be able to pre-install its own apps if it were otherwise prevented from doing so⁷⁵. On the other hand, small developers of services or applications - that might otherwise seek to compete with the integrated firm in the downstream market if they had access to the upstream assets - may be discouraged from doing so and may not enter the market at all. Moreover, these competitors might otherwise have been able to expand up the value chain in future, introducing competition not only into the downstream market but directly challenging the gatekeeper position of the firm in the upstream market (e.g. an app developer might subsequently have been able to develop its own OS, exploiting the market position it had already established in the downstream market for apps in doing so, or may disintermediate the OS controller in some other way).

In such cases, investment by third parties might be diminished, even if the investment incentives of the integrated firm itself were preserved. However, if some of the third party services that are deterred are complements rather than substitutes for the services provided by the integrated firm, then consumer demand for the device might also reduce and the investment by the integrated firm might fall as well⁷⁶.

Providing privileged access to device hardware or software resources may also enable innovative applications and services which would not otherwise run correctly if resources were to be allocated in a 'neutral' manner. On this view, the ability for third parties to obtain differentiated access to the device's resources (or to be pre-installed on the device) will encourage them to develop applications and services which can exploit these opportunities. For this reason, it is sometimes argued that neutrality regulation favours large established brands and firms, since consumers will always find their content and services. It is the new entrants and smaller firms, not the large firms, that may stand to benefit most if the rules allow gatekeepers to tilt the playing field in their favour, especially if the gatekeepers do so in return for payment.

Whether consumers will be better or worse off overall will invariably be difficult to determine – as the debates about whether the net neutrality regulations adopted several years ago have or have not inhibited investment in either networks or third party content and services serve to demonstrate. In the United States the FCC first concluded in 2015 that the weight of the economic evidence suggested that 'neutrality' rules would favour innovation and investment but then found, only two years later, that the opposite was the case⁷⁷. In both cases, the FCC's reasoning was based on rather limited evidence (only two empirical studies in the latter case⁷⁸). The most recent and comprehensive multi-country study on the subject found a negative relationship between net neutrality regulation and investment.⁷⁹


⁷⁵ It might be argued that Google has done the same thing by producing its own hardware devices in order to compete more effectively with Apple.

⁷⁶ See Easley et al for a discussion of these trade offs, <http://www.prodecon-cm.com/wp-content/uploads/2017/04/Easley-Hong-Kraemer.pdf>.

⁷⁷ Ford p.176 at <https://www.degruyter.com/downloadpdf/journals/rne/17/3/article-p175.xml>.

⁷⁸ Discussed in Ford, op cit.

⁷⁹ See (Briglauer et al, 2020), Available at https://www.wu.ac.at/fileadmin/wu/d/ri/regulation/wp_net_neutrality_2020_12_30.pdf.



Net neutrality regulation in Europe, as implemented by the Open Internet Regulation, recognised that discrimination may have beneficial effects in some circumstances and may be required in order to run broadband networks efficiently. Lawmakers sought to distinguish between discrimination and prioritisation in the conveyance of some services over others (e.g. to prefer the services of an integrated firm over those of third parties) and conduct which was 'not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic'⁸⁰. By analogy an OS might allocate battery, processor or other resources to run applications based upon the type of application being run, but not by reference to the identity of the firm providing that application.

4.2 Security and privacy

'Quality of service' in relation to the running of applications and services on devices may be affected by issues such as malware or other forms of software which may compromise the operation of the device itself or the performance of other applications and services, or software which may extract personal data from the user or the device without the appropriate permissions. All apps run in a 'sandbox' on the device, and permissions are granted in which ways the app can interact and receive information from the OS. Nonetheless, there have been many instances of users downloading malware with harmful consequences. Users may prefer to use pre-installed applications or those which they access via the pre-installed app store in the expectation that applications provided by the integrated firm will not compromise the performance of the device or the OS which they also supply. Integrated firms argue⁸¹ that they are entitled to control services which they brand or co-brand, including app stores from which third party applications can then be downloaded by the user. The app store policies of Google and Apple contain terms which appear intended to ensure that apps which are admitted to the store will not degrade the performance of the device, the OS, or other applications or services. For example, the Apple guidelines state:

'Design your app to use power efficiently and be used in a way that does not risk damage to the device. Apps should not rapidly drain battery, generate excessive heat, or put unnecessary strain on device resources. For example, apps should not encourage placing the device under a mattress or pillow while charging or perform excessive write cycles to the solid state drive. Apps, including any third-party advertisements displayed within them, may not run unrelated background processes, such as cryptocurrency mining.'⁸²

'Apps that transmit viruses, files, computer code, or programs that may harm or disrupt the normal operation of the operating system and/or hardware features, including Push Notifications and Game Centre, will be rejected. Egregious violations and repeat behaviour will result in removal from the Developer Program.'⁸³

4.3 Harmful content

Critics of app store providers argue that these restrictions may be applied or interpreted in ways which are unrelated to concerns about security or user privacy⁸⁴, but that there is no independent body (other than the app store owner itself) to whom such appeals can be made. It is alleged that apps developed by third parties which represent commercial threats to services or applications provided by the integrated firm are excluded from the app store for other, apparently legitimate, reasons⁸⁵. It is difficult for us to assess the validity of such claims.

The review process will also reject apps which contain what Google or Apple consider to be inappropriate content. Some advocates of 'neutrality' rules argue that firms with gatekeeper control

⁸⁰ Article 3(3) at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02015R2120-20201221&from=EN>.

⁸¹ As Google did in relation to certain contractual restrictions which it imposed on device manufactures, known as 'anti fragmentation agreements'.

⁸² <https://developer.apple.com/app-store/review/guidelines/#hardware-compatibility>, para 2.4.2.

⁸³ Ibid 2.5.3.

⁸⁴ See ARCEP, p.36 re: anti-virus software, https://en.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018-ENG.pdf.

⁸⁵ <https://www.nytimes.com/2019/04/27/technology/apple-screen-time-trackers.html> and <https://www.inc.com/jason-aten/apple-has-been-removing-apps-from-app-store-why-you-should-pay-attention.html>.



should not make editorial decisions about the source or type of content which can be accessed by users through their devices, and that to allow them to do so threatens media pluralism and freedom of expression. These are matters which have come into sharp focus in recent months through debates about the responsibility of digital platforms such as Facebook to remove and then block unlawful or otherwise harmful content that is uploaded onto their platforms by users. Similar concerns arose in relation to 'net neutrality', where it was alleged that network operators might disrupt the delivery of content which did not adhere to their editorial policies.

05

POLICY RECOMMENDATIONS

5 Policy recommendations

5.1 Key objective: Ensuring alternative routes to content for consumers

Our considerations have started from the realisation that net neutrality regulation alone does not ensure openness, non-discrimination and transparency of the whole internet access value chain, because 'devices' and 'online platforms' are also key components through which users access content online, and where discriminatory conduct may arise. Before discussing our policy recommendations, we believe it is important to first take a step back and to ask whether 'neutrality regulation', i.e., regulation build firmly on the three pillars of openness & non-discrimination, fairness and transparency is the right approach to regulating the internet access value chain; and whether sector-specific regulation is needed at all.


In the previous sections we have introduced many types of conduct relating to devices which might be said to violate neutrality principles. Some of these are discriminatory and might be expected to be prohibited under competition law. Others may be exploitative rather than exclusionary (or may be both). As showcased by the EC's Android case, competition law requires a long time before an abuse can be stopped, and in the presence of significant network effects, the harm is often irreversible as the market has recalibrated to a new equilibrium. Moreover, it is often difficult to delineate relevant markets and to establish market power, especially as there exist complex interactions between the different layers and various markets.

Some neutrality advocates argue that the principles of neutrality are so important and universal that they should apply to all firms and, in this context, all devices, irrespective of whether or not the provider of the hardware or the software enjoys a dominant position in a relevant market. In this spirit, also net neutrality regulation applies to all network operators, irrespective of their market position and dominance; although in practice regulatory authorities have taken the integrated firm's market position into account when assessing certain types of conduct. Our discussion so far has presumed that a firm exercises 'gatekeeper control' over some layer of the device value chain. This is similar to the approach taken by competition law and by the proposed Digital Markets Act or DMA, which designates 'gatekeepers' based on their size and relevance for the internal markets as well as their entrenched control of key 'core platform services', which include services at the layer of the operating system, and the application discovery layer and content discovery layer (search engines, video sharing services, and online intermediation services such as app stores)⁸⁶. In our view, it is very difficult to see how device neutrality regulation could be justified in relation to firms that do not exercise gatekeeper control⁸⁷.

Furthermore, we have highlighted that there exists a myriad of potentially problematic practices at various layers of the value chain. To be clear, not all of them have been exercised and therefore many only represent a potential harm. However, the same was true for net neutrality, and nevertheless policymakers regarded these potential harms as relevant enough to enact net neutrality regulation so that the potential harms would not materialize in the future. In contrast to net neutrality, however, there are far more possibly problematic practices in the context of 'device neutrality' and those stretch across several layers, and involve deeply integrated businesses. Some of the potential conducts are more problematic than others, but, as we have argued above, a coherent 'neutrality' regulation would need to be applied to all layers of the internet access value chain, and not just to parts of it. However, regulating 'device neutrality' on all layers (as opposed to just the network layer in case of net neutrality) would be much more complex and would require deep expertise by regulators at all layers, which is currently scant. Many of the practices are difficult to monitor (e.g., hidden access to APIs) and to evaluate (e.g., security risks), and subject to fast pacing technological advancements. At the same time, regulators would have to step in very quickly

⁸⁶ We recognise that the DMA's criteria for identifying 'gatekeepers' differ from those that might be adopted to find that a firm has a position of dominance under competition law. However, for the purposes of this report and our conclusions, this distinction is not significant. References to 'gatekeeper' firms can be taken as references to 'dominant' firms and vice versa.

⁸⁷ It is difficult to see why other firms would benefit from preferring their own applications and services if third parties could simply bypass them and users could switch to other devices.



due to the presence of indirect network effects, which can quickly tip a market following an abuse. We believe that there will seldomly be clear cut cases of discriminatory conduct which may not also be justifiable by reference to better security, compatibility, 'user experience', or simply 'innovation'.

Thus, there are often credible arguments as to why some types of conduct undertaken by firms with gatekeeper control which might violate neutrality principles might nonetheless be justified, either because they benefit consumers by promoting higher levels of investment in devices and related software, because they enable the effective operation of the device or because they protect consumers from harms from malware or applications which would compromise their rights to privacy. Especially the notion of openness and non-discrimination, which is inherent to 'neutrality regulation', is a disputed policy objective in this context, because too much openness is likely to reduce innovation and investment incentives, and can harm consumers, as we have detailed in the previous section.

European competition law can undertake a 'balancing act' in such circumstances, assessing any distortion of competition that may arise from the conduct in question against other benefits which the parties themselves claim to justify the conduct. In such circumstances the burden of proof is reversed. The Commission bears the burden of proof in demonstrating that the conduct distorts competition and is thereby presumed unlawful but the defendant bears the burden of demonstrating that the conduct can be justified. In the Google Android case referred to earlier, Google advanced various 'objective justification' arguments in relation to its practices of bundling the Google Search app with Play Store and requiring OEMs to pre-install it⁸⁸. However, the Commission concluded that Google had not demonstrated that it needed to bundle the Search app with Play Store in order to support a license-free Android OS and to provide the Play Store for no fee (which Google argued allowed it to compete with Apple and supported the production of low cost devices). Instead, it considered that Google could monetise the Play Store by other means (which as noted above, it subsequently did by changing its business model). The Commission also concluded that Google would have had an interest in supporting the Android OS in any event and could obtain revenues from Google Search without bundling. It also considered that whilst pre-installation might benefit consumers, this did not mean it was not necessary to restrict OEMs to the pre-installation of the Google Search app (rather than other apps) and that Google had other ways to ensure a 'consistent experience' across Google apps without requiring pre-installation. The Commission also rejected Google's objective justifications for the requiring OEMs to adhere to anti-fragmentation obligations for the Android OS when installing the Play Store⁸⁹ (which Google had argued was required to ensure interoperability and to protect its reputation) and for revenue sharing arrangements with OEMs (which Google argued were required if OEMs were to adopt Android and to compete with Apple)⁹⁰. This example demonstrates that the burden on firms under competition law to justify their conduct is relatively high.


The types of conduct we discussed in previous sections may be difficult to detect and difficult to prosecute under competition law, but may in the meantime have significant adverse effects for competition in related markets. If users cannot, or cannot easily, access third party services and applications then those third party firms, many of whom may be small developers, may be forced to exit the market. Alternatively, the length of time and uncertainty associated with prosecuting conduct under competition law may deter firms from complaining or from developing the services and applications in the first place. An ex ante regime, in which obligations are clear from the outset and enforcement is quick and effective, may promote investment and innovation by third parties when reliance on competition law would not⁹¹. However, if competition law is insufficient to ensure device

⁸⁸ Para 993-1008 at https://ec.europa.eu/competition/antitrust/cases/dec_docs/40099/40099_9993_3.pdf.

⁸⁹ Para 1155-1183, *ibid*.

⁹⁰ Para 1323-1332, *ibid*.

⁹¹ One feature of the Open Internet Regulation is the high degree of disclosure that is required from the firms that are subject to it. Firms are expected to disclose and explain the technical measures which they apply when managing their networks and what impact those measures may have on the user's experience. In addition, they are required to have procedures to address complaints from end users (but not from third party content or service providers) relating to their ability to access content and services through their internet connection. More recently, the Platform to Business Regulation has introduced obligations on app



neutrality, because its intervention is too slow and because competition is not likely to be feasible in the near future, an alternative regulatory approach might be suggested by that adopted for relatively complex value chains in telecommunications. The principle here is that regulators should undertake the analysis by first considering whether to intervene to promote competition in the market furthest upstream from the user, and whether, by doing so, it will then enable entry to occur and competition to develop in the downstream markets without further intervention directly in those markets⁹². In other words, if gatekeepers can be disintermediated by introducing more competition in markets for upstream inputs, then application and service developers will have other routes by which they can reach users without requiring further regulation. If, on the other hand, disintermediation is only possible in downstream markets, then regulation to prohibit exclusionary or exploitative conduct by the gatekeeper in upstream markets is likely to be required.

This approach proceeds on the assumption that behavioural remedies (i.e. prohibitions or obligations imposed on the integrated telecoms firms) can be used to remove competitive distortions that might otherwise arise because firms are vertically integrated. It does not contemplate removing the incentives of an integrated firm to engage in exclusionary conduct by structurally separating or disintegrating them, e.g., by prohibiting hardware device manufacturers from also developing its own software applications, or its own OS. Competition law allows for structural separation as a remedy to concerns about vertical integration, but these are rarely applied and difficult to apply in practice.

In light of this we suggest that the regulation of the Internet access value chain should not centre on the notion of 'neutrality', especially if the view is broadened to also include devices. Instead, with regard to personal general internet access devices (see 3.1.1), regulation of the internet access value chain should focus on


- **maintaining alternative routes for content** to the consumer, starting upstream in the value chain
- **avoiding a fragmentation of content** (i.e., that some content is not reachable for some consumers).

As we have explained above, consumers' internet access is often characterized by a **termination monopoly**, where at any given point in time, ex-post a consumer's access relies only on one connection or one device, although the consumer had a choice between different connections or devices ex-ante. In these cases, it usually does not suffice to just ensure consumer's choice ex ante (e.g., being able to choose between different smartphones). In order to resolve the termination monopoly, content would need to be able to reach the consumer through alternative routes after the consumer has chosen their device.

Here we also see a fundamental difference between the device layer (especially operating system and application discovery layer) and the network layer. At the network layer consumers typically only have one physical connection to the internet through which they must access content. At the device layer, in contrast, it is often possible to introduce different routes to accessing content (e.g., through side-loading apps, or by use of progressive web apps instead of native apps) at the same time. There is role for regulation when this choice is limited, either because access to content through alternative routes (e.g., to side-load apps on iOS) is blocked, or choice is distorted, because consumers are not aware of it or because using the alternative route has significant drawbacks (e.g., web apps perform worse than native apps).

store controllers to notify users of changes in their terms of business, give reasons if admission to the app store is refused, and provide a process by which they can appeal a decision by the app store controller.

⁹² Recital 24 'When defining the relevant wholesale markets which may be susceptible to ex ante regulation, a national regulatory authority should start by analysing the market which is most upstream of the retail market in which competitive problems have been identified. A national regulatory authority should conduct an analysis of the markets that are situated downstream from a regulated upstream input, to determine whether they would be effectively competitive in the presence of regulation upstream, until it reaches the retail market.', https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68858.



Therefore, instead of imposing 'neutrality' rules on a monopoly route to content, we suggest that device regulation is needed to introduce alternative routes to content on devices in order to resolve gatekeeping power. In the next section, we detail this approach.

5.2 Interventions at the Operating System Layer

5.2.1 *Enabling side-loading of apps*


Consumers' access to content can become severely restricted, if their access to content becomes filtered through app stores, especially if the operating system only provides one integrated app store, as is the case under iOS. Even irrespective of arguments in favour of a 'level playing field', relating to behavioural biases by which users opt for pre-installed software or ease-of-use when downloading apps from app stores, there arises a fundamental question of whether users shall actually 'own' their device in the sense that they can install software onto it as they wish.

Integrated device manufactures often argue that side-loading is potentially harmful to consumers, because they may install malicious or buggy software that endangers the security and integrity of the device, and may compromise user's privacy. Such concerns should be taken seriously, and they need to be evaluated considering the specifics of the case as well as the threat scenarios and the current technologies to defeat such threats. However, security and integrity concerns should not be a catch-all argument to avoid any type of regulation. For example, on desktop operating systems, in principle the same concerns would arise, and here side-loading of apps (e.g. by downloading them from websites or installing them through removable drives) is generally possible. Desktop operating systems have implemented security measures to warn consumers about potential risks, and consumers can fine-tune system access privileges for software, but ultimately it is the consumers' decision whether to install software that was not explicitly approved by the operating system provider, or not. The threat scenarios may be evaluated differently for mobile devices, for example, because such devices are carried with the consumer at all times, and are equipped with more sensors, such that they are able to collect more sensitive data. The burden of proof would lie with the integrated device manufacturer and we would note that many users will sync their data between mobile devices and stationary devices, especially if they use devices that belong to the same ecosystem of devices, such that security risks in one system, may also compromise the other system. Also, there is a clear industry trend to unify operating systems across different types of devices,⁹³ which bears the question whether the 'desktop view' or the 'smartphone view' on security and integrity concerns will (or should) prevail in the long run. In any case, we argue that the regulatory presumption should be that consumers can decide for themselves which app they want on the device they own (after having been warned about the possible consequences), unless a convincing case can be made that the potential risks outweigh the benefits for consumers.

Enabling side-loading of apps can be compared to the liberalization of terminal equipment in telecommunications markets. Initially consumers were only allowed to attach terminal equipment to the telephone network that was approved by the telecommunications provider, who argued that otherwise the security and integrity of the telecommunications network were to be compromised. Introducing competition for terminal equipment, and providing consumers a choice which devices they want to attach to the network, provided they meet certain technical standards, was typically the first step in the liberalization of the telecommunications market. For example, in 1968 the Federal Communications Commission ruled in a landmark decision, known as the 'Carterfone decision' that 'any lawful device' may be connected to the telephone network. No significant dangers have occurred from this liberalization, but instead it allowed for innovations such as answering machines, fax machines and modems.

We therefore concur with Article 6(c) of the DMA proposal, which requires providers of operating system that are a 'core platform service' to allow for side-loading of apps, notwithstanding measures to ensure the integrity of the operating system. As part of Article 6, this provision is subject

⁹³ For example, Apple now equips its new MacBooks with the M1 processor. This processor is based on the ARM chipset, which is also used in Apple's mobile devices. Similarly, Huawei has announced that its HarmonyOS is designed to be run on various devices, including both laptops and smartphones.



to being further specified. In our view, such specification would need to address predominantly the boundaries for reasonable measures to ensure integrity, how restrictive these can be, and how burdensome it is for consumers to overrule them, with the burden of proof lying with integrated device manufacturer. Moreover, issues of liability in case consumers choose to ignore warnings (including in relation to device warranties) need to be addressed. The same general rules should be applied to all apps.


5.2.2 De-installation and user consent for pre-installed apps

The pre-installation of the OS and other software on the device before it is supplied to the user is another key source of gatekeeper control. Again, Apple exercises this control directly and determines what software will be pre-installed. Most will be provided by Apple itself. Where Apple requires third party software, it may monetise its gatekeeper position by seeking bids from suppliers. Thus, Google make significant payments to Apple to pre-set its Google Search service as the default search engine on Apple's browser and for its operating system. This reveals the commercial value of pre-installation and default settings on digital devices, even if users can subsequently deinstall applications and replace them with other that they have downloaded themselves (which survey evidence suggests few users do). We note in this context that we view pre-setting (such as being the default search engine in a browser) and pre-installation (such as baking an app into the factory settings of a device) as two practices that essentially have the similar effect, which is to leverage a consumer's default bias, and thus do not differentiate between them for the purposes of this report. Henceforth, we refer to them simply as pre-installation. We also note that there may exist a continuum of similar practices on the continuum between pre-setting and pre-installation. For example, apps may not already be pre-installed ready-to-use on a device, but may reside merely as an icon on the home screen, and are downloaded and installed only after the user has clicked on them for the first time with the user only noticing a slightly longer loading of the app on its first use.

We also acknowledge the value which users themselves place on having devices which can be booted up and which offer the range of services they expect without the need to install additional software. However, pre-installation also runs the risk of bloatware (apps consumers do not want or need) being placed on the smartphone (cp. Section 3.3.2.1.). Device manufacturers must navigate this trade-off when pre-installing apps. Likewise, regulators must consider that interventions which require hardware to be supplied without software which users expect to be pre-installed are unlikely to be attractive or effective. Hence, interventions need to be designed to allow pre-installation of the OS and other software on the device to continue.

Control of the OS provides many opportunities for an integrated firm like Apple or Google to favour its own services over those of rivals. First, the OS provider decides which functions and capabilities will be exposed to enable third party software developers to develop complementary products and services to run on top of the OS. These could differ from the functions and capabilities available to services created by the integrated firm itself. In practice, it seems that the OS providers have many other ways of favouring some services over others, although there have been concerns about platform owners withdrawing access to APIs once they have copied and incorporated the work of third parties into their own software. Second, even if pre-installed apps have access to the same functionalities of the OS, there may be an advantage, because pre-installed apps will typically not require separate user consent to enable certain privileges. For example, apps that are loaded through the app store will typically have to ask for permissions to access contacts, cameras and other functionalities and data on the device. Pre-installed apps have such access already and do not require separate consumer consent.

Second, an OS provider which supplies its OS to other device manufacturers may seek to ensure that its services are pre-installed into the device by tying, through contractual terms, the licensing of the OS with the pre-installation of other services. Both Microsoft and Google have been found to do this in the past. The Commission's Google Android decision is intended to enable third party device manufacturers and mobile operators to pre-install non-Google software, including apps stores and browsers, on Google Android devices. Pre-installation of Apple devices will continue to be controlled by Apple itself. Whether Android devices include more non-Google apps when shipped in the future will depend upon how users react to devices which do not include the Google apps which they have



come to expect when they first purchase a device, and upon the economic incentives which Google, or third parties, can provide to the OEMs to pre-install their apps rather than those of rivals. If regulators wished to promote the pre-installation of non-Google apps on Android device they would need to devise some other 'neutral' means by which device producers would determine which apps to pre-install, but would also need to consider how the loss of revenues for manufacturers or mobile operators might affect their incentives to invest and innovate. The alternative would be either to prohibit pre-installation of any apps on the device, leaving it to users themselves to download the applications they want, or to present users with a 'choice screen' of different apps when the device is first booted up. Neither of these options appears very attractive from a user point of view, and so we consider any intervention to disintermediate pre-installation - beyond that already taken by the European Commission - to be very challenging and likely undesirable.

More problematic may be the case where the OS provider is itself inviting bids from third parties for their services to appear on a choice screen alongside its own service when the user boots up the device (as Google has done for Search services on Android OS devices in Europe). In such a case the auction may be unfair if the integrated firm is effectively transferring money from one part of its organisation to another, whilst third parties instead face real cash costs to bid. Such arguments were adopted by the Federal Communications Commission in relation to 'net neutrality' when AT&T offered to zero rate traffic of third party content providers in return for payment whilst its own content service provider paid by making an internal transfer payment within the same company in order to obtain the same privileges⁹⁴.


The better alternative in our view is to seek to disintermediate the pre-installation gateway by taking measures to ensure that users are better able to discover, download and run third party applications and services after they have purchased the device. This pushes us towards a focus on the two gateways through which users access such third party services - browsers and app stores.

Browsers are themselves apps that are being pre-installed, and web apps, by definition, are accessible freely through the browser and do not require to be installed. To date (progressive) web apps have more limited access to the OS and other device functionality (and no access to device identifiers) than native apps and most commentators (and users) seem to regard them as inferior. We therefore make the following recommendations in order to establish a more level playing field as between pre-installed apps and apps that might be subsequently downloaded.

First, pre-installed apps should **notify customers on first use about access privileges** in the same way as this would be the case for apps that are installed later (either by side-loading or through an app store). So, for example, if an app in the app store would have to provide a 'privacy label' in order to show which personal data it collects, then the same would have to hold true for pre-installed apps. Moreover, users need to be able **to exercise the same level of control over access privileges for pre-installed apps as for other apps**. That is, users should be able to revoke access and grant access rights at any time in the same way as would be possible or required for third party apps.

Second, users should be allowed to de-install all non-essential apps and be able to replace them with alternative. This requires that **pre-installed apps can be truly removed, freeing up their storage space on the device**. In reverse, this means that it is not enough to just being able disable or hide the app, because in this case the app will still occupy the devices limited resources and create switching costs for consumers. This proposal is consistent with **Article 6(b) of the DMA proposal**, although clarifications are needed what exactly qualifies as a un-installation and what are non-essential apps.

⁹⁴ https://cdn3.vox-cdn.com/uploads/chorus_asset/file/7575775/Letter_to_R._Quinn_12.1.16.0.pdf.



Third, **consumers should not be discouraged (e.g., by nudging or through financial means) or otherwise restricted (e.g., by technical means) when trying to switch apps.** This is consistent with **Article 6(e) of the DMA proposal.**⁹⁵

Fourth, **third party app developers should have the same ability to access functionalities and APIs of the operating system than those apps that have been pre-installed, subject to proportionate security and integrity measures.** This proposal is more contentious, because it will be difficult to delineate what would present a proportionate security and integrity risk. Generally, we view this in the same way as the possibility to side-load apps (see above). However, with respect to the replacement of pre-installed apps, we argue the security and integrity measures need to be evaluated even more closely. Since the operating system provider chooses to pre-install these apps, it seems difficult to justify that such apps present a security or integrity risk per se. Thus, there is an ex-ante presumption that the same functionalities should also be granted to third party apps in the same way subject to a specific case-by-case security assessment of the given app. This qualification of side-loading with respect to pre-installed apps is currently not being made in Article 6(c) of the DMA proposal. However, **Article 6(f) makes a similar proposal, but our proposal differs in two important ways. First, we argue that Article 6(f), which is currently restricted to 'ancillary services', should be extended and generally refer to apps pre-installed by the gatekeeper (including those shipped as part of the OS), if those pre-installed apps can be technically offered on a standalone basis by third parties.** Second, as it stands Article 6(f) does not explicitly take security and integrity concerns as a limiting principle into account (in a similar way as Article 6(c)). **We suggest that also Article 6(f) should provide the gatekeeper with a possibility to bring forward security and integrity concerns (i.e. they bear the burden of proof) and the possibility to take appropriate measures when opening up OS functionality to third-party providers.**


Our recommendation also bears an important implication that is worth highlighting. **If the gatekeeper also operates the pre-installed app store, then those categories of apps that are able to replace preinstalled apps by the gatekeeper should generally be allowed into the pre-installed app store,** again subject to a non-discriminatory security and integrity assessment. In our view this also includes the category of alternative app stores (see below). That is, if an app store is pre-installed on a device, then this app store should also generally admit other app stores, in order to facilitate that the pre-installed app store can be substituted. We will come back to this issue more specifically in Section 5.3.1.

5.2.3 Transparency about APIs and Monitoring of Standards

Allowing third party apps to be side-loaded onto a device, so that consumers can use 'any lawful app' and are able to replace pre-installed apps, is an important first step. However, unfettered competition between apps requires that third party apps are able to integrate as smoothly with the operating systems as pre-installed apps. We already addressed that apps should be given access to the same functionalities and APIs as pre-installed apps. In our view, a prerequisite for this is that the operating systems functionalities and available APIs are fully transparent and available to apps in a non-discriminatory way. As we have discussed above, the OS provider has an incentive to make details about the APIs available and transparent in order to stimulate third-party development. However, we have also pointed to instances where some app developers were given access to hidden APIs or functionalities that were not generally known or accessible. Moreover, developers have complained about the notice periods by which they were informed about API changes, in particular in relation to major changes of the OS.⁹⁶ Third party developers are then not able to provide a properly working app in time, also because they additionally need time to the approval in the app store. This can distort competition in favour of integrated and pre-installed apps, who have access to such

⁹⁵ We note that Article 6(e) additionally prohibits devices from being locked to a particular network provider (net locking), which is often a restriction imposed by the network provider when selling subsidized devices, and not a restriction that originates from the operating system provider. In case the market for devices remains competitive, and consumers have a choice between devices with and without net lock, we do not think this additional provision is necessary.

⁹⁶ See, for example, <https://www.theverge.com/2020/9/16/21439674/ios-14-developers-iphone-surprise-release-golden-master-beta-development>.



information earlier and do not need to seek app store approval. With regard to transparency in regard to operating systems, we submit the following policy recommendations.

First, we suggest that dominant operating system providers should **make publicly available the specifications of all APIs and functionalities that can be invoked by apps**, irrespective of whether these are restricted to be used by some apps, including those that are pre-installed or integrated with the OS. Moreover, the operating system providers shall **make publicly available the conditions under which apps can invoke those APIs and functionalities of the OS**. These transparency obligations will also help third party developers and regulators to determine whether or not any limitations to access APIs and functionalities (for example for apps that have been side-loaded or replace pre-installed apps), are in line with the self-prescribed rules, or applied in a discriminatory way. While operating systems generally do make available the specifications of most APIs and functionalities, it is not generally clear which non-public functions exist, especially in proprietary operating systems. Thus, legal obligations to publicize these and the corresponding access conditions would go beyond the status quo. This proposal is similar to what is demanded by the Platform-to-Business Regulation (EU Regulation 2019/1150) in regard to online intermediation services. However, this regulation does not apply to operating systems (see Recital 11), although it does apply to app stores.

Second, we suggest that dominant operating system providers shall adhere to a **minimum notice period before changing APIs and interfaces that may significantly impact the performance of apps**. The minimum notice period should be long enough, such that independent app developers have sufficient time to implement and test necessary changes, and should include enough time so that the update can be reviewed for admittance to the app store. Such timely access to new features and changes, which are typically scarce before and in the first weeks after an OS update, have been shown to be very valuable to app developers and are able to spur innovation at the application layer.⁹⁷

Third, we concur with the assessment of ARCEP⁹⁸ that it would be valuable to **create a system for monitoring the implementation of standards**, such as web standards adopted by the W3C, in operating systems and devices. More transparency, particularly which standards have been implemented and to which extent, and how long it took to implement such standards could be fruitful, both for assessing incentives and intentions in providing an environment that is conducive to complementary innovation and competition, as well as to raise public awareness by consumers and developers alike.

5.2.4 Data portability for devices

Devices to access the Internet, especially mobile devices, are often very personal to consumers. They accumulate a large amount of personal data about them (e.g. numbers called, browsing history, bookmarks, contacts, which apps are regularly accessed), as well as other data, e.g. on device settings or save games. Such data can be stored by the device and apps in a number of ways. First, they can reside on the device itself, managed by the operating system. But, in addition, data may also be sandboxed, i.e., stored by the individual apps that generated it (e.g., the browsing history by the browser), and are therefore stored in a format that is proprietary to the app. Second, it may also be stored in the cloud, either by the operating system or individual apps. Some applications may only work in conjunction with a cloud service, such as voice assistants that send recording to the cloud to be transcribed and evaluated. Taken together, such data constitutes a switching cost, because loss of access to apps and/or data on the device may be a major impediment to switching devices, especially if this included switching between operating systems.

Although facilitating switching between devices does not resolve the termination monopoly per se, it may contribute to more competition between ecosystems for existing users. Therefore, we argue

⁹⁷ Foerderer, J. (2020). Interfirm Exchange and Innovation in Platform Ecosystems: Evidence from Apple's Worldwide Developers Conference. *Management Science*, 66(10), 4772-4787.

⁹⁸ ARCEP ibid, p. 65.

that it is important that **policymakers also consider the importance of data portability with respect to devices.**

There already exist a number of provisions at the EU level that shall facilitate data portability; however these may have a number of limitations with respect to switching devices. Most notably, Art. 20 of the General Data Protection Regulation (GDPR) applies only to 'personal data' that was 'provided' by the consumers, so it is questionable whether it applies to data on settings or saved games, for example. Moreover, Article 16 of the Digital Content Directive (DCD) provides consumers with the possibility to transfer also non-personal data. The DCD applies to all traders that supply digital content and are remunerated either by taking a price, or by taking consumers data. It is thus not clear whether it would also apply to operating systems. Moreover, under the DCD the consumers have a right to port non-personal data only after terminating the contract with the trader. Finally, the Free Flow of Data Regulation (FFDR) includes under Article 6 a data portability provision. The FFDR applies to porting of non-personal data in B2B relationships and only requires self-regulatory codes of conduct.⁹⁹ A full legal assessment for the express purpose of data portability for devices is beyond the scope of this paper, but it appears that the existing legal regime does not necessarily equip users with a comprehensive right to transfer all relevant data (as far as it is meaningful in a particular case) from one device to another. In part, this is also because the data resides at different software layers (OS, apps) and legal entities (OEMs, app developers, OS developers), and both physically on the device as well as in the cloud.

Nevertheless, there also exist a number of apps that seek to facilitate the transfer of data from one device to another. For example, Apple provides the app 'Move to iOS' (indeed an Android app) and Samsung provides the app 'Smart Switch' for the express purpose of switching to an iOS device from and Android-device, and vice versa.¹⁰⁰ Of course, when switching from one device to another, especially when switching to another OS, there will always be some settings or applications that cannot be ported. In part that is due to incompatibility. For example, apps that exist under Android but not under iOS cannot be ported. However, even if the same app exists, installing the app may require downloading it from the respective app store (possibly requiring also paying for it again).¹⁰¹ The existence of incompatibilities between devices and operating systems is not a concern in itself, however. In fact, OS and devices must be able to differentiate themselves if they are to compete for consumers. However, it appears that apps that facilitate switching devices (in the best way possible) are still limited in the data that they can access. And (integrated) OS providers could seek to deliberately interfere with this process in a number of ways, e.g., by restricting access to APIs, by means of encrypting data or by not allowing data portability apps in the app store.

Given the availability of data portability apps, we do not suggest this is the most urgent area in which policymakers need to intervene, but it is an area that requires monitoring and possibly soft law. Specifically, similar **as under the FFDR, policymakers could establish codes of conduct for user-initiated porting of data between devices, including the development and agreement of standards for this process.** The porting should be as comprehensive as possible, including app data and settings. Indeed, the COVID-19 crises has shown that OS providers can agree on common standards, when they devised a common API, known as the Expose Notification System, together¹⁰², which allowed for a privacy preserving contact tracing across Android and iOS devices. The API was then integrated in both operating systems, and even added to older versions of the operating system to include devices that were not able to run the newest OS.


In order to facilitate switching between devices, continuous, real-time data portability (e.g., as it is envisioned in Article 6(h) of the DMA) is in our opinion only necessary insofar, as it allows the consumer to transfer data immediately and at any given point in time. For example, when a consumer has bought a new device, she should be able to transfer her data from

⁹⁹ For a more detailed description of the data portability provisions in EU law, we refer to Krämer, Senellart and de Streel (2020). Making Data Portability More Effective for the Digital Economy. Available at: https://cerre.eu/wp-content/uploads/2020/07/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf.

¹⁰⁰ See <https://support.apple.com/de-de/HT201196> and <https://www.samsung.com/us/support/answer/ANS00061001/>.

¹⁰¹ If side-loading apps were possible, the transfer of apps could possibly also be facilitated.

¹⁰² See <https://covid19.apple.com/contacttracing>.



the old smartphone immediately (using the APIs suggested above), without needing to request access, which may then be granted after some time (as, e.g., is the case under GDPR). However, such a transfer will usually be a one-off transfer, as consumers seldomly multi-home between devices; and even if they do, the devices will serve different purposes and hence are configured differently. Syncing of data that is relevant for multi-homing (e.g. contacts) is typically warranted via cloud services anyway. As it stands, Article 6(h) would apply also to operating systems (which are 'core platform services'). We therefore suggest to clarify the meaning of 'real-time', and 'continuous' data portability to be in the sense discussed above and to consider this when the Commission provides specific directions and evaluates compliance via Articles 7 and 25 of the DMA. It should be clear that the scenario for data portability discussed above is different as when, for example, a consumer wishes to continuously port her social media posts to another platform.

5.3 Interventions at the Application Discovery Layer

As detailed above, the application discovery layer and specifically app stores are a crucial gateway for consumer to access content, and, in our view, represent the most significant bottleneck to content on devices. We therefore suggest a number of remedies that seek to alleviate this bottleneck.

5.3.1 Enabling alternative app stores

The main source of market power and the issues with respect to consumer's choice of content on devices seems to reside with the existence of a dominant pre-installed app store. Consumers engage predominantly with content through apps, and thus, admittance to the pre-installed app store is almost a prerequisite for being easily accessible by consumers. Currently, progressive web apps are not a viable substitute for pre-installed apps or for apps accessed via an integrated firm's app store¹⁰³. In this respect, we **argue that the app store in itself is a 'core platform service' and not just the 'operating system'. It is our understanding that app stores are 'online intermediation services' under Article 2(2)(a) of the DMA proposal and therefore covered as a separate 'core platform service'**. In line with this view, the DMA proposal also recognizes that app stores are important sources of gatekeeping power (see Recital 47 and 51) and suggests a number of provisions that should apply for gatekeepers.


Article 6(c) demands that side-loading of app stores onto operating systems shall be possible as long as the safety and integrity of the operating system is preserved. This would provide an alternative route to content for consumers, and is consistent (and indeed necessary for consistence) with our earlier recommendation that users should be able to side-load 'any lawful app' on their device (see 5.2.1). Once again, we therefore **concur with Article 6(c), also with respect to side-loading app stores**. Again, potential security and integrity concerns should be taken seriously when specifying this provision, but with the burden of proof lying with the device manufacturer.

However, a number of additional provisions may be necessary in order to truly enable the emergence of third party app stores, and their ability to compete with. In particular regulators might seek to constrain the conduct of the gatekeeper app store controller by prescribing the kinds of rules for admission into the app store which can be imposed on third party app providers. Specifically, we make two recommendations in this regard.

First, app developers should not be discouraged from providing and selling their apps also through third-party apps stores, including the **ability to set different prices and conditions in the alternative app store**, without having to fear repercussions in the dominant app store. This is **consistent with Article 5(b) in the DMA proposal**.

Second, we submit **that gatekeeper app stores, which are also being pre-installed on a device, should not exclude other app stores from being admitted into the (pre-installed) gatekeeper app store. This recommendation is currently not directly reflected by the DMA proposal, albeit Article 6(k) requires fair and non-discriminatory general conditions of access to app stores**. Our recommendation is internally consistent with our previous view that pre-

¹⁰³ For a similar conclusion see <https://www.acm.nl/sites/default/files/documents/market-study-into-mobile-app-stores.pdf>. 49-




installing apps and app stores should generally be allowed, but comes with the caveat that it is then required that the gatekeeper needs to ensure that pre-installed app can be replaced without difficulty (see Section 5.2.1). In case of a pre-installed app store, this means that it should be possible to load alternative app stores through the pre-installed app store. Alternatively, if the gatekeeper also controls the operating system level, it could choose not to pre-install an app store, and instead to offer consumers a choice screen featuring both its own and alternative app stores that can be installed. In this case, the obligation to allow the loading of alternative app stores through the pre-installed app stores would clearly not apply.

Admittance of other app stores should be subject to the same scrutiny as other apps with respect to quality and safety standards, but a per se exclusion is in our view not warranted given the dominant app store's crucial role at the application discovery layer. However, it should also be acknowledged that app stores are a special category of apps, in the sense that – after being installed – they themselves would be responsible for the security and integrity of the apps that can be downloaded through them. Thus, when downloading an app store from another app store, the hosting app store should be exempt from liabilities arising from activities that it cannot control anymore. We therefore suggest that alternative app stores should be clearly labelled as such and can be placed in a special category within the hosting app store, for which consumers are made aware of the consequences. This would also facilitate that this special category within the app store would only need to be visible on those devices on which the app store has been pre-installed (e.g., devices already in the market). We are fully aware that this recommendation is potentially very far reaching, and it would also require significant changes to the existing app stores. Compliance within six months, as envisioned by the DMA, can therefore not be expected in this case. However, in our view, such an obligation is feasible and would also be proportionate, especially in concert with an obligation for side-loading apps. In effect, the same liability exemptions and additional security measures that are necessary for side-loading apps directly (say through a website) would also apply to apps that are side-loaded through an alternative app store. Thus, if side-loading in the sense of Section 5.2.1 and Article 6(c) is considered feasible and proportionate by policymakers, then side-loading through a dominant or gatekeeper app store should be considered feasible and proportionate as well.

Third, **alternative app stores should be free to use a payment system other than that of the dominant app store provider, or operating system provider.** This is in part because alternative app stores may compete with and differentiate themselves from the dominant app store on the basis of the payment services they offer and the level of commission fees they seek from app providers. In particular, we suggest that this is also true when the third-party apps store was downloaded via the dominant app stores (according to our previous recommendation). De facto this could mean that a third-party app store is offered as a 'free' app in the dominant app store,¹⁰⁴ but could use another payment method than that of the dominant app store for the apps listed in the third-party app store. **A more complicated question that arises from this layering of app stores (one app store being downloaded from another) is whether the first (dominant or gatekeeper) app store could still require a commission fee from 'in app purchases' in the second (third-party) app store. We do not suggest that this should be the case, as it will significantly complicate the contractual relationship. Especially if, as we suggest above, the hosting app store is exempt from liabilities arising from the third-party apps store, then it would also be justified that the alternative app store does not have to pay a commission fee to the hosting app store.**

Alternatively, if commission fees apply, then each app being sold in the third-party app store would be subject to two commission fees, one coming from the third-party app store and the other coming from the dominant, hosting app store. This clearly would yield a double marginalization problem, where the third-party app store would not be able to host competitive offers. Say the alternative app store demands a 10% commission fee and the dominant app store a 30% commission fee for in-app purchases. If in the alternative app store an app is sold for 1€, then the dominant app store may demand 30 cents from that trade, and the third-party app store would demand 10 cents. Thus, if the

¹⁰⁴ If third-party app store providers would choose to demand a price (for downloading the app store) in the dominant app store, then in our opinion the standard commission fee for paid apps should apply.




third-party app store would have to pay the 30 cents, it would make a loss. But if the developer would have to pay both commission rates, then he would pay a higher commission rate than in the dominant app store, which makes participating in the third-party app store unattractive. We see two ways out of this. (1) In-app purchases, when relating to a third-party app store that has been downloaded from a dominant app store, are not subject to the dominant app store's commission rate. In the example above, this would mean that the third-party app store retains 10 cents and the developer 90 cents of the trade, whereas the dominant app store receives nothing. (2) The dominant app store can only take a commission rate as a percentage of the third-party app store's commission rate. In the example above this would mean that the developer retains 90 cents of the trade, the dominant app store receives 30% of 10 cents, i.e., 3 cents, and the third-party app store retains the remaining 7 cents. We argue in favour of the second approach, because it balances out the involved party's interests, would be easier to enforce, and still allows for differentiated price setting by developers.

Finally, it is worth highlighting that the Google Play Store and Apple App Store will nevertheless remain a significant competitive advantage over third-party app stores, on Android and iOS devices respectively, even if these recommendations are followed. Both app stores could still be pre-installed, and – as detailed above – we do not object to pre-installation, and even if alternative app stores are hosted within these app stores, consumers would still have to take additional steps (searching and downloading) to install them. Given the strong evidence that consumers stick with the default settings, alternative app stores remain at some disadvantage. Moreover, customers will likely trust pre-installed app stores more, and if security or integrity concerns are significant for them, will likely stay with the dominant, pre-installed app store nevertheless. Furthermore, both app stores host a significant number of apps, more than any other app stores, and this provides them with a far stronger network effect. Thus, it is likely that consumers will rather multihome between app stores, if they install an alternative app store at all. Thus, we expect Google's and Apple's app stores to remain the main entry point for consumer's search for new apps¹⁰⁵, at least for the foreseeable future, although other app stores may gain a foothold for certain app segments – similar as is the case for web search. Both Google and Apple also have invested and innovated in their apps stores and mobile operating systems and thus deserve to be in this position. We would also expect both firms to continue to invest and innovate in the respective app stores and mobile operating systems; not only because they retain a competitive advantage in app stores, but also because this is conducive to their other business activities (e.g., selling advertisements or selling devices). However, recognizing that app stores are 'core platform services', we argue that the above measures are proportionate and effective. They enable content an alternative route to consumers, and thereby alleviate the concerns associated with gatekeeping.

5.3.2 Unbundling of the dominant app store for compatible operating systems

As discussed above, it is reasonable to assume that even if alternative app stores can be side-loaded on the devices, the currently dominant app store remains the dominant entry point for consumer's discovery of new apps due to existing network effects. In this sense, the dominant app store is a must-have app that consumers would expect on a device. This can be exemplified by a recent 'natural experiment'. Following the US export ban for Huawei, the company was no longer allowed to pre-install Google services, including the Play Store, on their new devices. Following the ban, Huawei's smartphone shipments dropped by almost 60% from Q3 2019 to Q3 2020 in Western Europe, which is about 9 times worse than the market average, and cannot be attributed to the COVID-19 pandemic

¹⁰⁵ We are not aware of comprehensive study that establishes conclusive evidence on how important the app store itself is for app discovery versus other means to discover new apps. However, there exists strong circumstantial evidence that the app store is indeed very important for app discovery. For example, in 2018 a slight change in the Play Store's algorithm has altered the ranking in which apps appeared, and in turn led to a drop in downloads of some apps in the range of 70-90% (<https://variety.com/2018/gaming/news/developers-sudden-drop-downloads-on-google-play-store-1202861850/>). The effect of the app store on app discovery will likely also depend on the app category. Across all categories of apps it is believed that the app store is the most significant single channel for app discovery, albeit it is estimated that only 40% of smartphone users browse for apps in the app store (<https://www.mobixed.com/mobile-app-marketing-insights-how-consumers-really-find-and-use-your-apps/>). Various other marketing techniques, including plain advertising are also used to make an app known to a consumer (see <https://uplandsoftware.com/localytics/resources/blog/app-discovery-101-6-ways-to-get-your-app-discovered-by-your-target-audience/>).



alone¹⁰⁶ (see also Figure 2). Comparably, in the Chinese market, where the Play Store is not the dominant app store, Huawei continued to increase its market share in the same period.¹⁰⁷

Thus, having access to the dominant app store is important for being competitive in the market for device. Generally, Google also has an incentive to license its app store to as many device manufacturers as possible, and to be pre-installed on Android devices, because in this way it can maintain the leadership in app stores for Android-based devices. In the Commission's Android case, Google was fined, however, for trying to leverage market power stemming from the Google Play Store to its other services, particularly Search and Chrome, and for trying to suppress the emergence of non-Google approved AOSP forks. Following the European Commission's Android decision, these issues appear to have been resolved. In particular, this means that Google cannot make the licensing of the Play Store conditional on an anti-fragmentation clause, which would prevent OEMs to also ship devices with non-Google approved forks. Moreover, it cannot make the licensing conditional on installing other Google apps. In effect, this means that the Play Store has been unbundled from GMS and can be installed on compatible operating systems for a licensing fee.

We argue the status quo established after the Google Android case is also very desirable from a 'device neutrality' perspective and, should the market for app stores change in the future, also apply in other instances where a dominant app store provider may withhold licensing the app store in order to suppress competition in the market for devices. That is, (1) notwithstanding the possibility to install alternative app stores, **device manufacturers should be able to pre-install a dominant app store by acquiring a license on FRAND terms.** (2) **Dominant app store providers shall not bundle the app store with other apps that are not essential for the functioning of the app store.** (3) The dominant app store provider **shall not prevent device manufacturers, through contractual or technical means, from pre-installing other app stores**, or apps, competing with the provider of the dominant app store. (4) The dominant **app store provider shall have the possibility to deny licensing the app store if it can demonstrate that this would cause significant harms (e.g., on reputation), it is technically incompatible, or would infringe other rights** (e.g., violate export restrictions).

It is important to highlight that we only suggest that the dominant app store is made available for 'compatible' operating system at FRAND terms in case such compatible operating systems exist. It does not require to license a compatible operating system as well. We therefore do *not* suggest that proprietary operating systems (such as iOS) would need to be licensed to independent hardware manufacturers. Hence, if no compatible OS exists, then there would not be a requirement to license the dominant app store on a non-discriminatory basis.


Article 5(f) of the DMA proposal may be viewed sceptically in this context. It requires that providers of a core platform service cannot require that (business) users also subscribe to another core platform service of that provider. **The fact that both operating systems and app stores are each 'core platform services' also means the operating system and app store would need to be unbundled to some degree in order to comply with Article 5(f).** For example, if both iOS and the Apple App Store are considered to be a core platform service, then it is questionable how Apple would allow usage of the App Store without requiring to users to subscribe to iOS as well, as Article 5(f) seems to require? Moreover, Article 5(f) is designed to be self-executing and is not intended to be specified further by the Commission. **We believe this may be an unintended consequence of Article 5(f) that would warrant to move it at least under the list of provisions under Article 6 that require further specification.**

5.3.3 No self-preferencing in browsers and app stores

No self-preferencing in browsers relates first to the issue of pre-installation, which we have addressed above, but also to related factors such as whether control over the APIs enabling browser extensions or inclusion in an associated app store, allows an integrated firm to block or otherwise discriminate against services which compete with (in the case of third party cookies) or disrupt (in the case of ad

¹⁰⁶ https://www.phonearena.com/news/huawei-samsung-apple-xiaomi-oppo-western-europe-sales-q3-2020_id128602.

¹⁰⁷ See <https://www.statista.com/statistics/387124/smartphone-shipments-in-china-market-share-vendors/>.



blocking software) its own services. To date, the debate has tended to focus on the pre-installation issue, but the focus now appears to be moving towards concerns about other ways in which an integrated firm may use its gatekeeper control over a browser to favour or protect affiliated services and advertising revenues. As we have shown above, the market for browsers has become very limited, especially on smartphones, where almost all of iOS users employ Apple's Safari, and almost all Android users employ Google's Chrome (or a variant thereof). Thus, self-preferencing of own content in the browser, is likely to become a more prevalent issue in the future.

We have raised a related issue that Apple requires all mobile browsers on iOS to use the same web rendering engine, which may stifle competition among browsers and competing access to content through 'progressive web apps'. We do not think, however, that this issue needs to be addressed directly by allowing browser providers to use their own web rendering engine - although this is possible under Android and thus it does not present a security threat per se. As long as all browsers, including the pre-installed browser, have to adhere to the same standards, then this is not an issue of self-preferencing, but rather an issue of controlling access of content by users. This issue however, can be addressed more directly by allowing side-loading and alternative app stores onto the system, which we have already proposed. This, coupled with transparency provision about the use and adoption of standards (see 5.2.3) is in our view sufficient to balance the trade-off between ensuring that content can reach consumers, and preservation of system integrity and security by controlling common standards that all apps, integrated and non-integrated ones, have to adhere to. We also deem it likely that the existence of alternative routes to native apps, will reduce the incentives to slow down or forestall the implementation of standards that would enable progressive web apps.¹⁰⁸

The issue of self-preferencing in app stores can arise when third-party app developers compete with the integrated app store provider. It is not an issue that relates just to devices, and has been at the centre of the Google Shopping case and other ongoing antitrust investigations, such as that against Amazon. Self-preferencing also has been at the centre of concern in the net neutrality debate, primarily in the US, where large broadband providers are vertically integrated with content providers. The question thus is not whether such a practice is problematic and should be sanctioned or stopped. The question is rather how unfair self-preferencing can be detected, enforced against and remedied.


We think that it is important to make the ban of self-preferencing explicit, as it is done in **Article 6(d) of the DMA proposal**. In the present context, this would mean that app stores shall not treat affiliated apps more favourably in the app store by giving them more prominence.

However, we see two main issues that arise from this rule. First, a ban of self-preferencing does not mean that app stores (or other 'core platform' operators) cannot offer **sponsored listings**, i.e., award more prominence against some payment. But then the question again arises whether the integrated app store provider can acquire a sponsored listing as well and if so, whether there can be a fair mechanism how the sponsored listing is awarded in the presence of an integrated rival that can bid with 'wooden dollars'. The same issues have arisen in the Google Shopping case, where it has proven to be difficult to find an effective remedy in this case. We do not intend to elaborate on this issue further here, and instead refer to our related CERRE report.¹⁰⁹

Second, even when prominence is not awarded through sponsored listings, but rather determined through an organic ranking (or other forms of prominence, e.g. through 'boxes', 'showreels' or as a 'pick of the day' that are not paid for), the issue remains **how self-preferencing can be detected and proven**. After all, it is the very purpose of platforms to organise content and to bring it in some order for consumers. If the integrated app store provider indeed offers the best matching service

¹⁰⁸ ARCEP, ibid, p. 65. makes the proposal to require dominant app stores to index Progressive Web Apps, such that they are discoverable through the app store. This is certainly technically feasible, but may also be achieved through a general web search, rather than the app store. Moreover, since PWAs are not subject to a review process by the app store, and can be changed at any point in time without notice to the app store. One would have to think carefully how such an obligation could be implemented, while not making the app store liable or damaging the app store's reputation. So, if this path is pursued, indexed PWAs would probably need to be subjected to the same review process for being listed in the app store as native apps.

¹⁰⁹ Feasey, R. and Krämer J. (2019). Implementing effective remedies for anti-competitive intermediation bias on vertically integrated platforms. CERRE Policy Report. Available at: https://www.cerre.eu/sites/cerre/files/cerre_intermediationbiasremedies_report.pdf.



according to some objective and non-discriminatory standard, then listing it first would not be self-preferencing. However, what could such an objective standard be? The ranking algorithms typically employ hundreds of ranking factors and change frequently over time. Proving that a certain ranking is discriminatory may therefore be very difficult. Indeed, the European Commission is reported to be struggling to build a case against Amazon's alleged self-preferencing¹¹⁰, and it is not clear whether this is due to lack of conduct, or lack of proof. In the Google Shopping case, the Commission has relied on internal communication and found that Google hardcoded exceptions for its own shopping service into the ranking algorithm. Future instances of self-preferencing may not be as blunt. In the DMA proposal, the Commission is given extensive powers to investigate gatekeepers, including the right to request access to data bases and algorithms (Article 19). It can also bring in external experts, although only for purposes of monitoring and compliance (Article 24). If the proposal is adopted, it will have to be seen whether the Commission is indeed equipped to detect and enforce against self-preferencing.

5.3.4 Transparency and redress mechanisms for dominant app stores

Finally, a comprehensive policy at the application discovery layer would also need to increase the transparency about actions that would affect consumers' discovery of new apps and content, especially with regard to admission to the app stores and how the ranking is performed. Such transparency obligations are also traditionally part of a 'neutrality regulation' as discussed in the introduction.


App stores should generally be able to compete based on the selection of content, design, editorial policy, organisation of content, and other dimensions relevant for differentiation. But due to their dominance, a special duty of care applies.

Much progress has been made in this regard already with the introduction of the Platform-to-Business Regulation (P2B), which requires all 'online intermediation services' (irrespective of whether they are dominant or not), including app stores, to be transparent about their ranking factors and access conditions. Moreover, the P2B regulation requires online intermediation services to set up an internal complaint handling system and means of mediation in order to provide for more effective redress by business users. However, the P2B regulation does not prevent discriminatory conduct per se, but requires online intermediation services to be transparent about it. It is too early to say how effective the P2B regulation will be, but since it applies to all intermediation services, irrespective of size, its provisions are necessarily relatively moderate. Thus, we agree that they need to be complemented by more targeted provisions for gatekeepers.

Dominant app stores are likely to fall under the realms of both, the DMA and the Digital Services Act (DSA), in addition to the P2B. The DSA establishes additional provisions with respect to content moderation and transparency. In particular, under the DSA, dominant app stores will likely qualify as "very large online platforms", that are subjected to even more obligations and scrutiny. This includes an assessment of systemic risks with respect to illegal content, fundamental rights and intentional manipulations of their service. This does not seem very relevant in the context of app stores. However, it also contains a specific provision on recommendation systems (Article 29), which – similar as the P2B – would require app stores to be transparent about its ranking (which is in our view a form of a recommender). In contrast to the P2B, the DSA also allows for data access through APIs and scrutiny, also by vetted external researchers, in order to be able to monitor compliance (Article 31). This possibility may also prove useful to detect self-preferencing in the context of the DMA (Article 6(d)).

Both, the DSA and the P2B provide for more transparency about rankings and recommendations being made in the app stores, as well as better possibility for redress through internal complaint handling systems, but also mediation. The DMA complements these by adding in Article 5(d) that business users should not be discouraged from raising issues relating to the practice of gatekeepers with any relevant public authority.

¹¹⁰ See <https://www.ft.com/content/d5bb5ebb-87ef-4968-8ff5-76b3a215eefc>.



Since all three pieces of regulation (P2B, DSA, and DMA) provide for transparency and redress obligations, their concurrent application needs to be considered and carefully co-ordinated. Since DMA and DSA are devised as a legislative package, and both are designed as complements to the P2B, this can be expected to be the case, but the co-ordination of oversight may be challenging. **Although, at this point, and in conjunction with the recommendations made above, we do not see for additional transparency and redress obligations beyond those made in the P2B regulation and the proposals for DSA and DMA, it may be necessary to establish a new institutional mechanism to ensure proper co-ordination of the regulations. This might take the form of a working group within the Commission but might also form the basis for a specialised 'app store regulator' to oversee the application of regulation to this critical component of today's internet value chain.**

Taken together, these obligations should provide that (1) dominant app stores must be transparent about their policies for admission to the app store, and apply these policies in a non-discriminatory way; (2) dominant app stores must be transparent about factors that determine rankings and allow for a continuous monitoring thereof, and (3) dominant app stores must install effective mechanisms for redress and shall not discourage content providers from using them.

5.4 Interventions at the Hardware Layer

So far as device hardware is concerned, it needs to be examined in each circumstance whether it is sufficient to ensure only access to an OS and the Application Layer, particularly the app store and under which circumstances device providers may have to allow third party providers equal access to the OS and device hardware. For the time being, we do not see the necessity to intervene at the hardware layer in its right. Thanks to the availability of AOSP, an open-source OS is available that device manufacturers can customize and develop further. Even if some of AOSP core functionalities, such as calendar, browser, and contacts have not been developed further by Google and have since become proprietary, we believe that this would nevertheless not preclude the ability to compete with a well-functioning device. Larger players, such as Samsung, Amazon, Xiaomi or Huawei would be well capable of developing such apps themselves, tailored to the devices that they produce – and in many cases this has already been done (e.g. as with Samsung's browser). The remaining competitive bottlenecks reside with the app store, which we have suggested should be supplied to compatible OS on a FRAND basis. Since only AOSP is currently open-source and used by OEMs, this currently means that Google would have to supply its Google Play store for a licensing fee for all compatible AOSP-forks, but irrespective of whether the same OEM also supplies devices with non-compatible operating systems, and independent of whether it pre-installs other Google apps. This is essentially what the EC's Android decision already calls for, and thus, we do not think that further interventions are required. The availability of competitive Android devices (hardware, operating system, and dominant app store) will also exert competitive pressure on Apple, which would not have to supply its app store because currently, no other OS compatible with iOS exists.

06

CONCLUSIONS

6 Conclusions

'Device neutrality' has been posed as a 'missing link' for the regulation of an open, non-discriminatory and transparent internet access regime, above and beyond 'net neutrality'. In a nutshell, device neutrality shall ensure that consumers can access the content that they want irrespective of the device that they use to access the internet.


We have highlighted in this report in the context of mobile devices for general internet access (i.e., smartphones and similar devices) that a regulation of devices proves to be much more nuanced and complex than a regulation of networks. If the approach taken in the Open Internet Regulation were adopted for device neutrality it would mean that regulation would prohibit certain types of conduct irrespective of the market position of the regulated firm and would accord users certain rights in respect of all devices (of a defined type). This would be at odds with the findings of this report as well as Commission's proposals for a Digital Markets Act which feature a number of ex ante obligations which seem expressly intended to implement aspects of 'device neutrality' but which would apply these only to a comparatively small group of designated platforms.

Numerous 'device neutrality' provisions are contained within the proposed DMA (although some of them are not specific to devices):

- a. Article 5(b), which would allow app developers to set different prices and conditions for their apps in alternative app stores;
- b. Article 5(c), which would allow app developers to conclude contracts with consumers also outside of the app store, so that they are not required to use the app store's payment system;
- c. Article 5(f), which requires that a provider of a core platform service cannot require (business) users to subscribe to any other core platform service;
- d. Article 6(b), which would require device providers to allow users to uninstall any pre-installed apps provided they do not compromise the performance of the OS or device by doing so;
- e. Article 6(c), which would require device providers to allow users access to third party apps, including third party app stores (but also via side-loading), provided they do not endanger the integrity of the OS or device;
- f. Article 6(d), which would prevent an app store controller preferencing its own apps in search results, or in other ways in their app store;
- g. Article 6(e), which would require device providers not to technically restrict the ability of users to switch between apps accessed via the OS;
- h. Article 6(f), which would require device providers to allow third party providers of 'ancillary services' (which includes payment services) equal access to the OS and device hardware);
- i. Article 6(k), which would require app store providers to allow fair and non-discriminatory access by third party app developers to the app store;
- j. Article 6(h), which would facilitate data portability between devices, thereby reducing switching costs.

Generally, we concur with all of these provisions, but have made a number of suggestions on how these may be adapted or specified in the context of devices.

Specifically, we pointed to the fact that Article 5(f) may have unintended consequences, because it requires some degree of unbundling of the dominant app stores from operating system, if both are supplied by the same provider. That is, if taken literally the provider of a gatekeeper app store like Apple would not be allowed to require users to subscribe to its dominant operating system. This interpretation would hinge on the legal meaning of 'subscribe', of course, but in any case, we believe



this is not what the Commission had in mind when drafting Article 5(f). In this sense, Article 5(f) would at least need further specification and clarification.

We also suggested that Article 5(c) of the DMA would require further specification when considered in the context of app stores. In particular, an issue may arise if alternative app stores are admitted to the dominant app store – which is another recommendation that we make for those dominant app stores that are pre-installed on devices. We argue that a ‘must carry’ obligation for pre-installed gatekeeper app stores in respect of alternative app stores should come the possibility to treat the latter as a special category of apps for which the gatekeeper app store is excluded from liability. In this case, a requirement to host alternative app stores within a dominant, pre-installed apps store seems as reasonable and proportionate as an obligation for side-loading app stores, which is already foreseen under Article 5(c). However, the recommendation to have the possibility for a must carry obligation for alternative app stores (still subject to appropriate security and integrity measures) with limited liability for the apps that are being installed through those alternative app stores is currently not reflected in the DMA.


Furthermore, by virtue of Article 5(b) app developers should be able to set different prices if listed in the alternative app store. But this also requires that alternative app stores, although being listed in the dominant app store, need to be able to use their own payment system and have the freedom to set different commission rates for their app developers. To achieve, this, and in order to avoid contractual complications and dependencies between a nested app store and a hosting app store, we suggest that alternative app stores should be considered as a special type of free app for which no commission fees are to be taken from in-app purchases. This seems reasonable in light of the liability exemptions for the hosting app store. Otherwise an issue of double marginalization would occur, which renders the alternative app store unattractive for consumers and developers.

We also do not object to pre-installing apps as provided for in Article 6(b), but suggested that they customers need to consent to the privileges that are granted to pre-installed apps in the same way they would need to do so for apps that are installed later.

We further recommended that Article 6(f) should be widened and not only refer to ‘ancillary services’ provided by the gatekeeper, but also refer to apps pre-installed by the gatekeeper (including those shipped as part of the OS), if those pre-installed apps can be technically offered on a standalone basis by third parties. Likewise, if the gatekeeper also operates the dominant app store, then apps that are able to replace a pre-installed app by the gatekeeper should generally be allowed to the app store, subject to a non-discriminatory security and integrity assessment.

We also note in this context that there are some inconsistencies between Article 6(c) and Article 6(f) is not very clear. While Article 6(c) calls for the ‘effective use’ of third-party applications interoperating with the OS, Article 6(f) requires access to ‘the same OS, hardware and software features’ for ‘ancillary services’. Thus, 6(f) seems to provide more far reaching access to hardware and software features, but it is limited to ‘ancillary services’, which are not well defined. Further, Article 6(c) allows for ‘proportionate measures’ to ensure system integrity and security, Article 6(f) does not contain a similar limiting principle. We suggest that Articles 6(c) and 6(f) should be harmonized better, or even integrated into one Article under the DMA. Specifically, we argue that gatekeeper operating system providers should make publicly available the specifications of *all* APIs and functionalities that can be invoked by apps, irrespective of whether these are restricted to be used by some apps, including those that are pre-installed or integrated with the OS, and also make publicly available the conditions under which apps can invoke those APIs and functionalities of the OS. Further, we distinguish between apps that are pre-installed by the gatekeeper, and those that are not (rather than between ancillary services and other apps). Whenever a gatekeeper decides to pre-install apps, then equivalent apps should be able to receive the same level of access and integration subject to appropriate security and integrity measures (e.g., a code review or requiring user consent).

Moreover, to level the playing field between vertically integrated app developers and third-party app developers, we recommended that before changing APIs and interfaces in the OS that may significantly impact the performance of apps, OS providers should adhere to a minimum notice



period. Rather than through the DMA, this recommendation could also be addressed through a revision of the P2B regulation, which currently does not apply to operating systems. It would also be valuable to create a system for monitoring the implementation of standards (e.g., standards adopted by standardization bodies like the W3C) in operating systems. This could all be added through an additional transparency provision for operating systems.¹¹¹

Which input markets and how far upstream or downstream a regulator would intervene in an attempt to disintermediate the gatekeeper is the key issue for regulating devices. We have highlighted that a key policy objective should be to maintain alternative routes for content to reach consumers, e.g. by giving consumers the choice to install 'any lawful' app on their devices. We identify **operating systems and app stores** as the main bottlenecks for content on devices. This is in line with the DMA, where operating systems, as well as online intermediation service (which also encompass app stores) are in the list of 'core platform services'. However, even by focussing on these parts of the value chain, and on the regulation of app stores in particular, the Commission will have a great deal of work to do to ensure 'device neutrality'. It will be important that this work is properly co-ordinated and retains its focus alongside the many other objectives which the Commission is seeking to achieve in digital markets.

¹¹¹ In this context, we also point at the importance of considering how the various provisions that may apply to gatekeepers (under the DMA, DSA and P2B) interact and apply in concert for each designated gatekeeper and its core platform services. In this report, we have taken a device-specific view and identified a large number of individual obligations under the DMA, DSA and P2B regulation that would apply or could apply in this context – including several which are not directly considered 'device neutrality' provisions by the Commission. The same would need to be carefully done in other contexts. While each of the provisions under the DMA, DSA and P2B seems reasonable in its own right, policymakers should carefully evaluate which (e.g., technical and economic) trade-offs may arise in applying them jointly or in combination, and whether the joint application of these obligations is then still reasonable and proportionate.



cerre

Centre on Regulation in Europe

📍 Avenue Louise, 475 (box 10)
1050 Brussels, Belgium

📞 +32 2 230 83 60

✉ info@cerre.eu

🌐 cerre.eu

🐦 [@CERRE_ThinkTank](https://twitter.com/CERRE_ThinkTank)