

The calling card of Russian digital antitrust[☆]

Natalia S. Pavlova^{a,b,*}, Andrey E. Shastitko^{a,b},
Alexander A. Kurdin^b

^a *Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia*

^b *Lomonosov Moscow State University, Moscow, Russia*

Abstract

Digital antitrust is at the forefront of all expert discussions and is far from becoming an area of consensus among researchers. Moreover, the prescriptions for developed countries do not fit well the situation in developing countries, and namely in BRICS: where the violator of antitrust laws is based compared to national firms becomes an important factor that links competition and industrial policy. The article uses three recent cases from Russian antitrust policy in the digital sphere to illustrate typical patterns of platform conduct that lead not just to a restriction of competition that needs to be remedied by antitrust measures, but also to noteworthy distribution effects. The cases also illustrate the approach taken by the Russian competition authority to some typical problems that arise in digital markets, e.g. market definition, conduct interpretation, behavioral effects, and remedies. The analysis sheds light on the specifics of Russian antitrust policy in digital markets, as well as their interpretation in the context of competition policy in developing countries and the link between competition and industrial policies.

Keywords: digital antitrust, competition policy, industrial policy, platforms, multi-sided markets, essential facilities, consumer bias.

JEL classification: K21, L41.

1. Introduction

Russian antitrust as a direction of economic policy has a relatively short history, but a rich experience in the application of antitrust laws in areas that are considered digital. On some issues the Russian antitrust authority has even proven to be a leading force, such as prohibiting Google's conduct of precluding the pre-installation of competing search services on Android devices almost three years before a similar decision by the European Commission (EC). In itself,

[☆] The article was prepared as part of research for the state assignment of RANEPa.

* Corresponding author, E-mail address: pavl.ns@yandex.ru

the specifics of Russian antitrust in the digital sphere deserves attention. Perhaps this high activity is associated with weaker path-dependency when compared with jurisdictions with a longer history of antitrust enforcement. It is also possible that such active immersion into digital competition issues is due to the fact that competition threats arise from companies whose headquarters are located outside of Russia, in developed countries, while the parties suffering from anticompetitive effects are, conversely, Russian companies. A number of cases are quite illustrative: namely, Yandex–Google, Kaspersky Lab–Microsoft and Kaspersky Lab–Apple. This sort of approach is easily explained when considering the goals of competition authorities, which are primarily tasked with promoting the public (or consumer) welfare at the national level (Shastitko and Pavlova, 2019).

Russia, like other BRICS countries, has been and remains a country with a developing market economy, where the agenda is historically different from that of developed countries, where the issue of balancing protective and active instruments of competition policy, as well as industrial policy, is not so acute. However, it is law enforcement in digital cases that points to a tight connection between antitrust and industrial policy, which can become a reason to consider their balance not only in the BRICS countries, but also in the countries where a developed market economy is believed to have established itself completely and irrevocably.

Competition policy in the digital sphere is, indeed, a complicated endeavor. On the one hand, digital giants have been a source of unprecedented innovations, which are closely linked to their ability to capitalize on network effects.¹ Positive network effects—both direct and indirect²—contribute to the fact that larger firms become more efficient, which, in turn, poses a problem for competition authorities: these firms become a threat to competition, yet curtailing their expansion can slow down innovation and lead to lower consumer welfare in the long run. On the other hand, abuse of market power by such companies can have significant negative consequences due to their sheer size and infiltration into consumers' lives. This is exacerbated by the nature of platform businesses that have recently gained so much economic power.

In terms of the platform theory, namely platforms' main characteristics, which contribute to the formation of their behavior in digital markets as opposed to traditional firms, at least two recent works have been published that contain thorough overviews of relevant literature (BRICS Competition Law and Policy Centre, 2019, pp. 128–169; Shastitko and Markova, 2020). For the purpose of this paper it is important to note that one of a platform's main characteristics is its ability to set the rules for players on a multi-sided market and for their trans-

¹ Two concepts used in economic literature are mutually substitutable: network externalities and network effects. Yet the term “network externality” means more than the dependence of the utility of consumers on the number of consumers, since the very concept of externality relates to costs and benefits not reflected in prices or in contract clauses. So, the internalization of externalities due to the use of different institutional arrangements might mean the move to Pareto-improvement, while network effects are simply the material basis for that.

² In platform economics, direct network effect takes place when a user's utility or benefit from the platform's service depends on the number of users on the same side of the platform (or, in other words, from the same group of users) (see, e.g., Katz and Shapiro, 1985), while indirect network effects take place when one group's user's benefit depends on how well the platform does in attracting users from another group/on another side of the platform (Armstrong, 2006).

actions. Consequently, as noted in BRICS Competition Law and Policy Centre (2019, p. 129), “...along with the enhanced resource efficiency, the large size of [multi-sided platforms] may cause a strong impact on competition in platform and downstream markets. In their value chains, large [multi-sided platforms] act as dominant players (‘lead’ firms in the sense used by the theory of global value chain). Governance in value chains represents not only rule-setting and enforcement but also reallocation of value created in the value chain in favor of the dominant participant. The share of value distributed towards independent participants in downstream markets may decrease.”

Additionally, there are at least two severe complications to this statement that currently distinguish competition policy’s agenda. One has already been mentioned: if the dominant companies are based in developed countries and the consumers or other types of customers are based in developing countries, then the abuse of dominance leads to a redistributive effect from lower-income countries to higher-income ones. But it is not just about the producers’ and the consumers’ welfare on isolated markets: the effects can have consequences in terms of global value chains in the digital sphere. As pointed out in BRICS Competition Law and Policy Centre (2019, p. 84), the expansion of geographic market boundaries due to increased digitalization can potentially induce an effect analogous to the Vanek–Reinert effect (Reinert, 2007), where a sudden transition to free trade can destroy the most efficient industries in a less developed country and send it into a vicious circle of poverty. Similarly, the expansion of global digital giants on developing countries’ domestic markets can potentially hurt these countries’ own technological companies, with the developing countries potentially being forced out of the sectors with the most value added and characterized by the highest rates of innovation (BRICS Competition Law and Policy Centre, 2019, pp. 84–85). Consequently, competition policy and industrial policy need to find a balance in light of redistributive effects along the global digital value chains.

To clarify our approach, we stress the differences between antimonopoly policy and competition policy, since emerging market economies confront unique challenges to finding a dynamic balance between protective and active components of competition policy. While active competition policy includes reforms of regulation and a market-oriented system of public administration, as well as reforms of industries with a natural monopoly component and competition advocacy, antitrust at its core includes deterrence of dominance abuse, deterrence of anticompetitive agreements (primarily, hardcore cartels) and control of mergers. We will also discuss how antitrust policy corresponds with some active measures of competition and industrial policy.

Section 2 describes three big recent cases in Russian antitrust that illustrate this narrative and highlight the associated issues: the Yandex–Google case (2015), the Kaspersky–Microsoft case (2017) and the Kaspersky–Apple case. We describe the details of these cases, the FAS Russia (Federal Antimonopoly Service) decision on each and the possible underlying theoretical interpretations of the conduct with some elements of discussion on decisions adopted. Section 3 explains how these cases illustrate the general traits of antitrust in the digital sphere, as well as the realities of digital competition policy in the BRICS countries and specifically in Russia. Section 4 concludes with the main results and ways to develop research on this subject matter.

2. The cases

2.1. The Yandex–Google case

Details of the case and theoretical interpretation. The case may be familiar due to a corresponding case recently decided by the European Commission. The nature of the infringement was that Google prohibited mobile device manufacturers from pre-installing applications that competed with Google’s own services, and as a consequence these competing services, such as Yandex’s search app, started losing market share. Yandex filed a complaint with the FAS Russia in February 2015 and the case was decided in September of the same year,³ while the EC case was still being investigated.

It might be considered the first case in Russia that dealt with platform behavior. Yet platforms and multi-sided markets were not defined in Russian competition law at this time (and haven’t been defined to this day, although the proposed “Fifth antimonopoly package” of amendments addresses that), so the interpretations used in this case gravitated to more traditional concepts. The FAS Russia defined the relevant market as pre-installed app stores for Android devices for apps localized for distribution in the Russian Federation, with Google dominant on the market by virtue of owning Google Play. Device manufacturers were considered to be the buyers in this market.

Initially, the behavior of Google was interpreted in terms of unfair competition (prohibited according to Article 14 of the law “On protection of competition”), although later the case was requalified in terms of abuse of dominance, prohibited by Article 10. The anticompetitive behavior, as established by FAS, consisted of the following. Being dominant in the market for pre-installed app stores for Android, Google tied Google Play with the GMS package (consisting of Google Search, Google Chrome, Google Maps and other Google services), demanding that Google Search be the default search option on the device—although, as established by FAS, from a technical standpoint picking Google Search as the default search option was not necessary for all the other GMS services to work correctly. Google also made demands on the specific places on the screen where its services were supposed to appear, which ensured that their services would be used more frequently. There were separate agreements with device manufacturers disincentivizing the pre-installation of apps that competed with Google’s services from the GMS package—which resulted in device manufacturers refusing to pre-install Yandex’s search app. Finally, Google imposed anti-fragmentation requirements on device manufacturers, and the pre-installation of competing services could be deemed a violation of these requirements.

FAS concluded that by unduly tying Google Play, in the market for which Google holds a dominant position, with GMS services that operate on competitive markets, Google created barriers to entry in the markets for competing apps, and uneven conditions for existing apps, since they effectively lost access to pre-installation as a distribution channel. FAS pointed out that pre-installation is the most efficient tool for promoting apps, *inter alia* for the reason of customer “passivity”—the fact that customers tend to stick with pre-installed options.

³ <https://br.fas.gov.ru/ca/upravlenie-regulirovaniya-svyazi-i-informatsionnyh-tehnologiy/ad-54066-15/> (in Russian).

The pre-installation effect was exacerbated by a lack of options for deleting the pre-installed GMS services, which can only be de-activated. Uneven conditions were compounded by Google using its dominant position to insist on certain places on the screen where the app icons should appear.

Summing up the competition authority's approach, we can see that the violation is interpreted in terms of anticompetitive tying, which is a "traditional" type of antitrust violation. A factor that puts "a new spin" on it is that Google Play can be considered to be a platform on a multi-sided market with at least three distinct groups of users: portable device manufacturers, consumers of devices (and applications) and independent producers of applications. Consequently, even though the customers on the market are defined as device manufacturers, dominance is in fact preconditioned on the inability of end consumers (users of devices and applications) to switch to a different means of app installation.

The anticompetitive effects also appear on markets that are different from that where Google has a dominant position—on markets for services analogous to the ones in the GMS package, namely search services. This can be seen as a leveraging strategy: by tying Google Play with the GMS package Google leverages its market power on to the markets for apps. But what makes this strategy so successful is another specific trait of digital markets, and that is the exploitation of consumers' cognitive biases. In this case, pre-installation as a strategy becomes such an efficient channel—and precluding access to pre-installation for independent developers becomes such a powerful way to restrict competition—because of the status quo bias (Samuelson and Zeckhauser, 1988), in which people exhibit a preference for the current state of affairs. It is interesting to note that the bias's effect is taken into consideration by the competition authority not on theoretical grounds, but based on the results of consumer surveys that demonstrated the reluctance of end-consumers to switch away from the default search service.

The FAS Russia decision. FAS found a violation of competition law. After a lengthy conflict with Google which at first attempted to avoid abiding by the authority's decision and paying the appointed fine, the sides reached a settlement agreement in court.⁴ According to this agreement, not only were device manufacturers allowed to pre-install services that competed with Google's, but new and even current owners of Android phones were informed of their ability to choose their default search service via a special window—a condition resembling the one imposed in the EC case against Microsoft that addressed the choice of default browser.

Discussion. Indeed, the vast majority of users are not carriers of expert knowledge regarding the comparison of useful properties of applications for the same functional purpose. And if in the public space credible sources do not give a clear advantage to applications of independent developers (in this case, Yandex), then the rational approach of uninformed users is to prefer the status quo even to the detriment of the useful effects of installing more effective applications (taking into account the properties of the user profile). However, the FAS decision was challenged by Google, in particular, on the basis of the following arguments: (1) the complex use of the single Google app package might facilitate safe and secure use of devices (taking into account that Android OS is also initially produced by Google), while the intervention by other application producers could probably

⁴ <https://en.fas.gov.ru/press-center/news/detail.html?id=49774>

result in interoperability problems, so the “efficiency defense” could be used to justify Google’s behavior; (2) the definition of market boundaries as pre-installed app stores might be erroneous due to the substitution between different ways of downloading and installing apps.

2.2. *The Kaspersky–Microsoft case*

Before considering the details of this particular case, it is worth looking back briefly at the history of antitrust enforcement against Microsoft.⁵ Among these cases we will focus on the U.S. case against Microsoft that concerned the Internet Explorer (IE) browser and two EC cases: the Windows Media Player case and the Internet Explorer case.

In the U.S. case the object was the practice of tying the IE browser with the Windows operating system. Netscape’s independently developed browser Navigator previously held around 70% of the market for browsers when Microsoft started developing its own solution and aggressively marketing it. Microsoft was selling Internet Explorer together with the operating system; it precluded PC manufacturers from deleting IE and regulated the place on the screen that the IE icon was supposed to hold relative to other icons. It was also using exclusivity clauses in contracts with internet providers such as America Online and AT&T Worldnet, where, for example, Microsoft provided them with a free version of IE, but it needed to be integrated into the software provided to consumers for internet access and the internet company took on obligations not to promote an alternative browser. A special feature of this case is that anticompetitive effects were argued to have manifested not just in the market for browsers, but for the operating system itself: the use of Netscape Navigator together with Java programming language could potentially “allow software applications to run on hardware independently from the desktop OS” (Etro, 2007, pp. 218–219). As such, the Navigator browser allowed developers to create software that was compatible with alternative operating systems, which could eventually lead to a decrease in switching costs from Windows to alternative operating systems, so by eliminating Navigator Microsoft could be said to be strengthening its position on the operating system market.

The initial court decision imposed a structural remedy: the company was to be divided into separate businesses, one dealing with the operating system and the other with browsers and other software. The decision was appealed and eventually the settlement imposed only behavioral remedies without any structural requirements. The logic that allowed the requirements to be softened was based on the concept of network effects: by virtue of having a large user data base Microsoft was encouraging software developers and computer hardware markets to focus their efforts on Windows, which led to a positive feedback loop that elevated Windows against competing services.

The EC cases against Microsoft were similar in facts, yet different in their approach to interpretation. The first case focused on Microsoft not sufficiently disclosing information to server OS developers in order to ensure compatibility, as well as Windows Media Player (WMP) being pre-installed and tied with

⁵ The details of these cases can be found, for example, in Gavil and First (2014) and in Russian in Kosyakina and Podlesnaya (2018).

the operating system. It is important to note that because of Microsoft's dominant position in the OS market, the company was found to be obligated to provide data to ensure compatibility with its product. But the most relevant part of the case for us is the issue of WMP. The competition authority found that the pre-installation of this software was the most efficient channel of distribution. Additionally, WMP could not be deleted. Moreover, WMP benefited from compatibility with other software and access to various content that was compatible with the player. The EC concluded that Microsoft would need to additionally distribute a version of their OS without the pre-installed WMP, so consumers would choose whether they needed it. In the next case the logic was similar: Internet Explorer was found to be a separate market from the Windows operating system; by tying IE to Windows Microsoft was engaging in anticompetitive behavior, ensuring that their product (IE) would get unfair competitive advantages that would not have been otherwise enjoyed by it. The wide distribution of IE along with Windows led to developers actively creating software for it, strengthening the network effects. The prescribed remedy was aimed at allowing device manufacturers to pre-install alternative browsers, and for consumers to have more ease of switching.

Comparing the U.S. approach with the EC one, part of the difference lies in the treatment of network effects. If in the U.S. they are seen as a source of efficiency, then in the EC they are interpreted to be an element of switching costs that exacerbates the anticompetitive effects. Additionally, in the EC decision the concept of essential facilities was applied to the Windows operating system when dealing with the interoperability issue (the significance of this will be explained in detail below). Finally, there is an obvious difference on the surface of these investigations: that Microsoft is an important domestic player for the U.S., but for the EU it is a foreign company with significant market power in its markets.

Having the details of these cases for context, we turn to the Russian antitrust case against Microsoft.

*Details of the case and theoretical interpretation.*⁶ In 2015 Microsoft released its Windows 10 OS edition which came with pre-installed antivirus software—Windows Defender. The release coincided with a change of policy towards independently developed antivirus software, which caused Kaspersky Lab to file a complaint with the FAS Russia. The actions of Microsoft that became the reason for the complaint were the following:

- Microsoft unilaterally deleted independent antivirus software (drivers that enabled the software to launch), having detected its incompatibility (as assessed by Microsoft) with Windows 10;
- Microsoft reduced the time for antivirus developers to ensure the compatibility of their software by providing them with the newest Windows version just one week in advance;
- Microsoft actively induced (utilizing the built-in visualization options available to them) users to turn on the pre-installed antivirus software (Defender) in such a manner that would lead to independent antivirus software being de-activated;
- Microsoft precluded independent antivirus software from actively using visual notifications to remind customers about the need to renew their licenses in the next three days after the license expires;

⁶ This section relies heavily on our previous article (Shastitko and Kurdin, 2017).

- if two independent antivirus programs start to function with Windows 10 simultaneously, both are de-activated (due to a restriction on the number of antivirus programs that can run at the same time) and Defender is automatically turned on instead of them.

Kaspersky Lab pointed out that this behavior could have produced anticompetitive effects on the market for antivirus software because it led to unfair advantages for the pre-installed Defender in relation to independent antiviruses, and taking into account the dominant position of Microsoft on the market for operating systems for PCs those advantages posed a serious risk to the position of Defender's competitors. Microsoft, in return, accentuated the security benefits of providing a pre-installed antivirus. While the case was still being considered by the competition authority, Microsoft had made certain alterations to its practice and policies which mitigated part of the antitrust concerns.

Considering the possible interpretations of Microsoft's actions, alternative theories and concepts can be implemented.

Firstly, the OS can be interpreted as a platform that provides services to different participants of a two-sided market—the sellers of applied software that want their software to be installed on PCs with a certain OS, and users that want to buy certain software.

Secondly, the OS can be thought of as a primary product, the functionality of which requires that users buy a complementary (aftermarket) product—applied software.

Thirdly, emphasis can be put on the high specificity of applied software, developed specifically to work with a given OS, which automatically gives the developer of the OS an advantage when dealing with software developers.

Fourthly, we consider it possible to examine the OS as a natural monopoly, an infrastructure industry of a sort, which users—developers and consumers of software—“connect” to, although, at first glance, the development of an OS hardly resembles traditional infrastructure industries. But from this point of view a concept that seems to explain rather accurately the behavior of Microsoft in this case is the concept of essential facilities.

Essential facilities are assets “the use of which is a necessary condition for production in a given industry and duplicating which is unfeasible for technical or economic reasons” (Golovanova, 2014, p. 112; Golovanova and Pavlova, 2018, pp. 19–20). In Russian antitrust the concept is not defined and thus is not widely used. But from the point of view of economics, the use of this concept to interpret the case in question seems appropriate. Software developers necessarily require the opportunity to connect their software to the user's OS, without which the use of the software is impossible. At the same time, network effects of a large scale generated by the OS as a single platform for access to different kinds of software, dramatically limit the opportunity of alternative operational systems to gain popularity and be installed on the same devices (PCs), which would allow software developers to switch to these alternative operating systems. In this sense, the developers of operating systems can be considered as owners of facilities that are essential to software developers.

Another important aspect is the ability of the OS developers to manipulate access to information, which became a major point in this case. The developers of the OS have exclusive access to an incomparably important communication

channel for users—system messages on their PCs. This allows the OS developers to exploit the users' cognitive biases stemming from their bounded rationality.

Control over essential facilities for the software markets and the ability to provoke and exploit the cognitive biases of users allow the developers of OSs to (a) leverage market power from the market for OSs (if they have it) on to the markets for applied software, and (b) implement methods of unfair competition. Can this leveraging become anticompetitive? In our opinion, it can, if the OS developer is simultaneously a participant in a market for applied software. Such was the situation in the Kaspersky–Microsoft case, as well as in the cases against Microsoft that dealt with internet browsers and media players.

The FAS Russia decision. FAS found elements of a violation of the law “On the protection of competition” in the actions of Microsoft. Microsoft exhibited elements of abusing its dominant position in the market for RTM-versions⁷ of operating systems for stationary devices used for adapting applied software developed in the Russian Federation by creating discriminatory conditions for antivirus developers, namely giving unfair advantages to Defender over the antivirus by Kaspersky Lab, which could have led to a restriction of competition in the market for antivirus software in Russia. The uncovered elements of the violation ended up being more numerous compared to the original basis for opening the case. These included the reduction of time to work with the RTM-version before release, additional charges of unfair rules of notifying users of the status of their antivirus license, a lack of clear notification that their independent antivirus would be turned off and replaced with Defender after upgrading to Windows 10, as well as unequal access to undocumented APIs.⁸ So the competition authority issued a warning to Microsoft, demanding that the company cease the actions in question and modify its behavior to ensure competition. Microsoft adhered to the warning and the antitrust case was closed.

Discussion. Microsoft was justifying its behavior using, in particular, two arguments. First, in order to protect the whole global network of Windows users it might be necessary to impose some level of obligatory antivirus protection on any Windows user notwithstanding his/her ability or desire to install antivirus software voluntarily. Thus, it could be the case to use the “efficiency defense.” Probably, the very presence of Defender as a part and parcel of Microsoft as a market offer might create a presumption on the side of some consumers: since there is pre-installed defense, they do not have to care about the issue. Second, the market dominance of Microsoft might be questioned if FAS took into account the presence of Apple as a potential strong competitor or considered the market for OSs in larger boundaries including also OSs for mobile devices, although the substitutability between mobile devices and PCs is very doubtful.

2.3. The Kaspersky–Apple case

Details of the case and theoretical interpretation. In this case Kaspersky Lab filed a complaint with the FAS Russia concerning a change in policy imple-

⁷ RTM (Release to Manufacturing) version—a version provided to application manufacturers in order to make possible their adaptation to changes in OS.

⁸ API (Application Programming Interface) is a mechanism providing specific OS services to applications.

mented by Apple pertaining to the rules of its App Store. The parental control app Kaspersky Safe Kids (KSK) had been denied the opportunity to be distributed via App Store, with Apple citing that KSK implemented MDM profiles in violation of App Store's policies. A period of communication followed, with Kaspersky Lab pointing out that it did not in fact use MDM-profiles, but configuration profiles in its app, that were not explicitly prohibited by the App Store. Apple reiterated their ban on MDM-profiles, adding that configuration profiles were banned as well, then loosened its policy and added that in some cases it would allow the use of these technologies, but without giving Kaspersky Lab an answer on the conditions when such a ban could be lifted. This period of Apple's alteration of its de-facto implemented policy (Apple insisted that the policy had been enacted earlier, but it appears that it at the least was not enforced as strictly) that led a number of independently developed apps to be excluded from the App Store coincided with the introduction of a new version of Apple's mobile operating system iOS 12 that had a pre-installed app—Screen Time—that could be used, among other things, as a means of parental control. This led Kaspersky Lab to cite in its antitrust complaint the possibility that Apple was using its App Store's rules to disadvantage independent parental control apps in favor of its own product—Screen Time, while simultaneously giving Screen Time extra advantages that stem from its pre-installation on devices and access to technologies and options that were denied to independent developers.

In this case, as well, different theories could be applied to interpret Apple's conduct. One of these is, again, the essential facilities concept. Although different apps or classes of apps differ in their ease of adapting to an alternative mobile OS (from iOS to Android, for example), parental control apps are among those that are difficult to adapt, as they use different approaches to utilizing each system's capabilities to ensure their function and are often developed by different specialists, specializing only on one of the popular mobile OSs. In order to gain access to customers the parental control app, developed for a certain mobile OS, needs to be installed onto the device with this OS. In this sense, access to the OS is an essential facility: it is technically and economically impossible for parental control app developers to reach their customers without installation on the OS. For Apple devices the only approved way of installing independent apps is via the App Store, which means that access to the App Store for app developers is an essential facility as well. The combination of iOS and App Store exhibits all the necessary characteristics of essential facilities (OECD, 1996):

- control of the essential facility by a monopolist: Apple owns iOS and App Store, and due to its own policies, there are no official alternative operating systems for Apple devices, or app markets for iOS. The situation for Apple differs from that of, for example, Android devices, where official alternative app stores are available (such as Amazon AppStore, Samsung Galaxy Apps, etc.);
- a competitor's inability practically or reasonably to duplicate the essential facility: once again, this is a consequence of Apple's own policy and its orientation on a closed eco-system. Alternative stores for apps that have been introduced (Cydia, AltStore) either require a "jailbreak" or have an otherwise reduced functionality that makes them a marginal phenomenon;
- the denial of the use of the facility to a competitor: use of the App Store and access to iOS has been denied to Kaspersky Lab and other parental control apps that compete with Apple's own pre-installed Screen Time app;

- the feasibility of providing the facility: it stems from the fact that previous versions of KSK that also utilized configuration profiles had earlier been approved for the App Store: the original app, 20 more updated versions before the tightening of Apple's policy on using MDM-profiles, 5 more after the policy change and before the introduction of iOS 12, and even one full updated version after the introduction of iOS 12 (later versions were approved only with reduced functions).

If applied, the essential facilities concept leads to the logical implication that Apple does in fact have the obligation to provide non-discriminatory access to the App Store and the iOS for the apps of independent developers and its own apps. It is important to note that it is not just the App Store that the non-discriminatory access is applied to, but also the operating system itself, as, for example, Screen Time comes pre-installed on the device and does not need to be downloaded via App Store.

Regulating the rules of access to an essential facility can be seen as a means of leveraging market power, but even without addressing the concept of essential facilities Apple's conduct can also be interpreted as leveraging market power on the market for app stores for Apple devices onto the market for parental control apps for Apple devices.

Another side to the leveraging approach is added by considering Apple's bundling strategy: its mobile devices come with a pre-installed OS (iOS), a pre-installed app store (App Store) and pre-installed app that can be used for parental control (Screen Time). And if the OS market and app store market for Apple devices are already monopolized, Screen Time competed against other parental control apps for iOS. Bundling a product from a competitive market with a monopoly product can be considered a form of abuse of dominance.

Another alternative to the essential facilities approach would be an interpretation in terms of platforms, which, as has already been noted in the description of the Yandex–Google case, appears to be valid when dealing with any app store. App Store connects developers of mobile apps for iOS, including parental control apps, and app users that search for the apps and install them by using the App Store. The more app developers are represented on the platform, the more apps there are for the users to choose from and the higher the utility of the users; and the more users are looking for apps with the help of the platform, the more attractive the platform is for app developers. This shows us that the App Store is a platform characterized by two-way cross-side network effects. The fact that users do not easily switch between platforms (that would entail a need for a new device, as only Apple devices support iOS) coupled with Apple's orientation on building an eco-system of devices and software means that consumers become locked in when initially choosing a platform: they are single-home rather than multi-home with their mobile devices. In this case, losing access to a platform means losing access to its clients, and as Apple's clients are the ones spending a larger share on services in spite of owning a smaller share of devices,⁹ losing access to them can put a significant strain on independent app developers and ultimately eliminate competition in this sphere.

⁹ <https://gs.statcounter.com/os-market-share/mobile/worldwide>; <https://sensortower.com/blog/app-revenue-and-downloads-2019>

The FAS Russia decision. FAS declared that Apple had abused its dominant position in the market for distribution of mobile applications by creating unlawful obstacles for third-party apps in the iOS ecosystem.¹⁰ Apple insisted that any restrictions (even if they existed) could be excused for its intention to improve users' security without any other viable motivation, while final consumers were always able to change their mobile platforms. However, the investigation by FAS generally supported the rationale provided by Kaspersky Lab. According to its conclusions, Apple's dominance in the market for mobile apps distribution on its own platform was sufficient to restrict competition between mobile apps and promote Apple's own application ScreenTime. The control over the single legal application store for iOS combined with the contractual right to reject any third-party apps provided exclusive opportunities to block or suppress competing mobile apps.

3. Epicrisis for competition restrictions in the digital area and Russian remedies

Whichever interpretation of the abovementioned cases is used, the result is not only a judgement on the efficiency outcome, but also a cause to consider redistribution. In this section we will analyze the common traits of these cases in light of more general tendencies in competition policy in the digital sphere, tendencies specific for the BRICS countries, as well as traits that are characteristic of competition policy in Russia and their relation to industrial policy.

What the antitrust cases have in common is that all three of them seem to illustrate a typical strategy for platforms that deal with so-called dual distribution. Originally dual distribution means that a manufacturer simultaneously sells to distributors, who then supply end-consumers, and to end-consumers directly. This is similar to platforms, many of which perform the dual role of marketplace and online retailer or manufacturer. In all three cases, the owner of the platform (Google, Microsoft, Apple) is also the owner of a product that is distributed via that platform (Google search, Microsoft Defender, Screen Time app) and appears to use his position as a platform to manipulate its rules in order to promote his own product. One possible interpretation for this behavior is the well-known concept of leveraging: the owner uses his market power on the platform market and leverages it to increase market power in an adjacent market. This is the sort of market strategy that is becoming widely recognized throughout the world, while the need to deal with it turns into a major point for political campaigns (see, e.g., Elizabeth Warren's arguments during her presidential campaign in the U.S.¹¹).

For developing countries, such as BRICS countries, this sort of leveraging strategy has additional implications. The three cases illustrate a typical situation of the sort: we see that the platform with the market power is owned by a global corporation, while the market where the anticompetitive effects occur has among its participants national (Russian) IT-firms, and these firms suffer the consequences of the anticompetitive practice by losing profits and market share. In

¹⁰ <http://en.fas.gov.ru/press-center/news/detail.html?id=54965>

¹¹ Breaking the political influence of market-dominant companies. <https://elizabethwarren.com/plans/break-monopoly-influence>

each case, a “laissez-faire” attitude could have had severe consequences for the national firms, contributing perhaps to raising the risk of the Vanek–Reinert effect. Consequently, by protecting competition the antimonopoly authority contributed as well to protecting a prominent national competitor—an effect in line with the goals of industrial policy in the IT sphere.

All of these cases, as has been noted, can also be interpreted in terms of denial of access to essential facilities. Of course, this approach has its own drawbacks that are commonly associated with applying the essential facilities doctrine to industries other than natural monopolies (Motta, 2004, pp. 67–68). At the same time, in the above cases the owner of essential facilities is a giant transnational digital company, while the anticompetitive effects are experienced by national companies that are relatively smaller, although they also compete at the international level. Denial of access to essential facilities to favor the owner’s services is not only a question of competition, but also, again, a question of wealth-transfer between countries. Let us note that the essential facilities doctrine has already been applied to a digital giant—in the EC case against Microsoft on grounds of refusal to supply information on interoperability.

Beside the general characteristics of platform strategies and the BRICS-specific (or specific for developing countries) effects, the three cases also illustrate some special traits that are characteristic of antitrust in Russia. Considering the antitrust policy itself, although all three cases can be interpreted in terms of platforms, that is not the approach chosen by the antimonopoly authority.¹² Economics of platforms or even the concept of platforms are not explicitly used to explain any of the features of the relevant markets or the behavior of the firms in question.¹³ On the one hand, this can lead to the omission of some important aspects, such as the role of the opinion of end-consumers in defining the market between the platform and the manufacturers, and denounces the opportunity to use models of platforms to support a theory of harm. On the other hand, this approach also allows escaping many conceptual problems that appear when dealing with platforms, such as their definition (an issue still lacking consensus among researchers), market definition with indirect network externalities, etc.

A possible reason for not utilizing the platform concept is that platforms are not yet defined in the Russian law “On protection of competition”: introducing a working definition of platforms into the legislation is one of the main points of the “Fifth antimonopoly package” that is currently being discussed at the government level. The Yandex–Google case is older than the first version of the package that was introduced to the public and probably influenced its creation. But in later cases avoiding using the platform logic can be taken as an effect of the primacy of the legal over the economic that is prominent in Russian antitrust policy and is noted by experts. Additionally, for a legal concept to be implementable, a key factor is the role of meso-institutions (Ménard, 2017; Shastitko, 2019). Here the norms that appear from antitrust enforcement, as well as the body of legal documents and soft law clarifying the use of the upper-level norms were also

¹² Similarly, other BRICS countries aren’t rushing to implement platform economics in their decisions, either—see Avdasheva and Korneeva (2019).

¹³ The exception here is the Kaspersky Lab–Apple case, where the FAS Russia explicitly uses such terms as “platform” and “multi-sided market” in its recent decision, but although the concepts are named, many of their aspects remain ignored in the decision.

not flexible enough—and did not incorporate some key economic concepts—to make possible the explicit use of platform economics in the authority’s decisions.

But while the platform interpretation is not explicitly used by the competition authority in these cases, neither is the alternative approach provided by the European case against Microsoft—the essential facilities doctrine. The concept of essential facilities is not defined explicitly either by Russian competition law, or its practice, even for natural monopolies. The question is, then, what approach *was* taken.

3.1. Market definition

In the Yandex–Google case and the Kaspersky–Microsoft case the competition authority solved the market delineating issue by defining markets narrowly, including focusing on only one side of a multi-sided market. In the Yandex–Google case the market boundaries were defined as pre-installed app stores for OS Android, localized for distribution in the Russian Federation. The buyers on this market were defined to be the manufacturers of mobile devices, which pre-install app stores in order to resell them bundled with their devices to end-consumers. In the Kaspersky–Microsoft case the market was defined as RTM-versions of OS for stationary devices for adapting application software developed in the Russian Federation. In each case the multi-sided nature of the market is not addressed explicitly, but the role of consumer (end-consumer) switching patterns is taken into account (see the next point), although the role of indirect network effects is never brought up.

A similar case in this regard is the Yandex–Uber joint venture (2017). A major challenge in the case was market definition. Although consumers tend to equate aggregator services with taxi services, neither Yandex nor Uber provided the taxi services themselves. The FAS Russia ended up defining the product market as “organization of informational interaction between drivers and passengers of taxis,”¹⁴ which corresponds to the nature of the transactions. It also underlines that the aggregator deals with both the drivers and the passengers as customers exhibiting quasi-demand for its services—a distinct feature of a two-sided market (Rochet and Tirole, 2003).

3.2. Market power/dominance

What these cases do recognize explicitly is the role of switching patterns in adjacent markets as a source of market power on the markets in question. In the Yandex–Google case the fact that only pre-installed app stores (for OS Android) are included in the market is not only due to the inability of users to download Google Play on their own, but their strong preference for devices with a pre-installed app store (from 63.3% to 69% of users hold the opinion that an app store is a necessary prerequisite for a device they are willing to buy¹⁵). In the Kaspersky–Microsoft case the RTM-versions of OS for stationary devices—a market where the “buyers” are software developers that need the RTM-version to ensure that their software is compatible with the new OS updates—was defined in such a way

¹⁴ <http://en.fas.gov.ru/press-center/news/detail.html?id=52562>

¹⁵ <https://br.fas.gov.ru/ca/upravlenie-regulirovaniya-svyazi-i-informatsionnyh-tehnologiy/ad-54066-15/> (in Russian).

due to the switching patterns of end-consumers that do not consider mobile and stationary devices to be substitutable. Accentuating that operating systems have no value in absence of devices to use them on, the competition authority relies on these results to delineate RTM-versions (which are considered in the authority's decision to be the same as the OS versions end-consumers use) for stationary devices into a separate market.

In the Kaspersky–Apple case as well the inability or at least strong reluctance of app developers to switch is not only due to additional costs they would have to incur (hiring new personnel that specializes on app development for another operating system, letting go the ones that specialize on the OS that the company is switching from or retraining them), but also the loss of profits that stems from brand-loyalty of end-consumers of mobile devices.

As for the markets where anticompetitive effects occurred (search apps, anti-virus software, parental control apps), they were not defined as rigorously as the markets where the dominant position was proven, but the fact that dominance on one market was abused to suppress competition in another market indicates that the competition authority was using (if not explicitly) the leveraging concept in its decision.

3.3. *Theory of harm*

For those who control and supply the platform, pre-installing and making a service the default solution on the platform is a powerful tool of promoting their own services. This tying strategy is made even more effective by the effects of bounded rationality of end-consumers, such as inertia and the status quo bias. In both the Yandex–Google and the Kaspersky–Microsoft case the competition authority used anticompetitive tying as a theory of harm. We see that all the cases recognize consumer bias as an exacerbating factor for the ability of the platforms to restrict competition.

We can also conclude that Russian antitrust incorporates the phenomenon of leveraging. In all three cases we deal with a firm that is dominant in one market, but abuses that dominance to influence competition in another, previously competitive market. We also see that the quantification of the effects of restriction of competition in this latter market is not at the center of these cases—the main market analysis pertains to the product where the violator potentially has dominance. This, perhaps, stems from the fact that in Russian competition law, and namely in Article 10 of the law “On protection of competition” that deals with abuse of dominance, definitive proof of negative effects for competition is not necessarily needed to prove a violation: conduct that leads to “infringement of the interests of other persons (economic entities) in the sphere of entrepreneurship activity or indefinite range of consumers”¹⁶ can also be considered abuse of dominance.

Currently the FAS Russia proposes a set of amendments for competition law known as the “Fifth antimonopoly package” or the “digital package.” Platforms are at the center of the proposed amendments:¹⁷ the law creates new criteria for dominance, such as ownership of the digital program that is used to organize

¹⁶ <http://en.fas.gov.ru/documents/documentdetails.html?id=14737>

¹⁷ <https://pravo.ru/story/223072/> (in Russian).

transactions between sellers and buyers, and network effects. The market share criteria for dominance are proposed to be lowered for platforms and set to 35% of the market (compared with the current 50%). All of these measures put platforms in the spotlight of Russian antitrust, providing a legal definition and a framework of reference for identifying platform markets. Yet what the proposed amendments lack is a vision of the theories of harm for platform markets that can be quite different from traditional forms of antitrust violation, as well as the specific concept of efficiencies related to platform businesses. Without these the proposed law will only partially help transform competition policy towards platforms and risks raising the level of type I and II enforcement errors.

3.4. *Efficiency defense*

The efficiency defense based on the ground of network effects provided by platform owners and of interoperability between a platform itself and its after-market products and services does not seem to be an attractive argument for FAS. It may be attributed partially to the shift towards European antitrust tradition (here we refer, in particular, to the abovementioned Microsoft case with a hostile EC attitude towards network effects), partially—to the low “countability” of efficiencies in the antitrust analysis. One more explanation may be added if we take into account the national residence of the companies concerned: negative effects from competition restrictions are experienced by domestic companies, while benefits from additional efficiencies are distributed internationally among the global community of platform users, which makes them less notable for the regulator.

In fact it means, on the one hand, a certain distribution of the burden of proof between the platform owners and the regulator, and, on the other hand, a challenge for the potential beneficiaries of the efficiency defense arguments to create demand for knowledge of this type.

Thus, one of the key points of probable agenda for an antitrust upgrade in Russia as well as in other BRICS countries in line with challenges of systemic digital transformation of national economies is to search for adequate instruments of theoretical and applied research for antimonopoly law enactment and enforcement.

3.5. *Room for behavioral economics in antitrust?*

Although the cases recognize some of the effects of consumer bias due to bounded rationality, these are never addressed on a theoretical level: rather, they are addressed by introducing information from consumer polls to confirm the effects of these biases (in the Yandex–Google case—how rarely consumers tend to switch away from a pre-installed option).

The issue with incorporating behavioral biases on a theoretical level is well-known: the instruments of economic analysis that are used in antitrust and the norms shaped by them rely mostly on neoclassical economics where unbounded rationality is presupposed. Behavioral economics, although more realistic in some of its predictions, does not yet offer a full alternative for the “traditional” theory and system of instruments of economic analysis for antitrust (Wright and Stone, 2012). Consequently, incorporating bounded rationality on the level of assumptions would entail a throw-back for antitrust practitioners.

By only acknowledging behavioral bias *ex post*, antitrust—not just in Russia, but in other countries as well, including the U.S.—aims to get “the best of both worlds”: remaining theoretically sound as well as empirically accurate.

In this vein, the importance of status quo bias was explicitly uncovered in the Yandex–Google case that then reverberated in the Kaspersky–Microsoft and Kaspersky–Apple cases. It illustrated how pre-installation could guarantee significant competitive advantages for software, even when monetary and time switching costs (but not cognitive switching costs) for consumers are low. This ended up influencing not just Russian competition policy—we see that the effects of pre-installation are addressed as concerns in all three cases—but also the country’s industrial policy.

3.6. *The junction of competition policy and industrial policy*

The FAS Russia is sufficiently active in the field of industrial policy and regulation, and one of FAS’s initiatives was the enactment of a legal obligation for smart-devices to have pre-installed Russian software on them in order to be sold in Russia. The measure, which had sparked a heated discussion over its potential effectiveness and possible consequences (Apple, for example, has been rumored to threaten to leave the Russian market¹⁸), was signed into law in December 2019, and starting July 2020 enters into force.¹⁹ This is a clear causal link between antitrust and industrial policy, and this case is not unique in illustrating their close junction. The fact that many consumers are critical of this measure also demonstrates the sort of complicated trade-off that industrial policy faces when supporting national business in these cases. On the one hand, boosting the country’s IT industry can be seen as more than just a “rooting for your own team” stance, but also an effort to keep up dynamic competition in the industry. On the other hand, the transnational companies do have an efficiency defense to rely on, as well as being supported by consumers who might experience a short-term loss of welfare due to additional restraints on their global suppliers.

The digital cases in Russian antitrust do not go alone. The relationship between digital and “traditional” markets might be much more complex. One recent example is the Bayer–Monsanto merger (2018) that was cleared by antitrust authorities in a number of countries, including BRICS. Although all the BRICS competition authorities were interested in the merger, the risks posed to competition differed significantly depending on the sort of crops and agricultural products for which each country was dependent on the companies. There was also a digital aspect to the case: the merging firms aimed at introducing a digital platform of precise farming that could help farmers optimize their work. In Russia, the link between antitrust and agricultural policy shaped a unique remedy issued by FAS alongside the approval of the merger: the merged company was to take ac-

¹⁸ <https://www.forbes.com/sites/zakoffman/2019/12/05/its-apple-vs-putin-as-russias-new-smartphone-ban-approaches/#11c556bb1786>

¹⁹ The legislation will presumably cover devices that will be sold in Russia starting in 2021. It is worth noting that the proposed legislation does not include the names of any specific apps that need to be installed, but rather categories of apps corresponding to three types of devices: smart devices with sensor-screens; stationary devices, PCs and laptops; smart TVs. The categories of apps include search apps and browsers, antivirus software, maps, e-mail services and others.

tions aimed at “the development of competition in the Russian agro-technical area through creation of potential competition of Russian companies.”²⁰ This included the “technological transfer of molecular selection tools and germplasm of the selected crops necessary to create highly productive seeds,”²¹ as well as non-discriminatory access to digital platforms of precise farming and accompanying data. The unique conditions of the remedy were supported by the creation of a special “Technology Transfer Center” to select recipients interested in the technology transfer and to monitor the execution of the remedy.

Finally, another digital aspect of the junction between competition and industrial policy, and for which the FAS Russia is also responsible, lies in the field of government procurement. In Russia, the competition authority also enforces government procurement laws, which leads to a close link between anticorruption and antitrust rules. Recently the problem of electronic bid-rigging has been gaining momentum. To combat this type of violation Russia’s competition authority is developing software for detection of bid rigging (the project is whimsically called “Big Digital Cat”) that is akin to the Brazilian “Cerebro” system in its functionality (the South African Republic’s authority is also starting its own version).²² This also highlights another aspect of digital antitrust relevant for all the BRICS countries: in order to keep up with the violators, the competition authorities themselves need to “go digital.”

4. Conclusion

All in all, the cases discussed appear to be, on the one hand, in line with existing international practice, but, on the other hand, they are clearly restricted in the use of modern economic concepts that have not yet found their way into Russian competition law. Faced with the same problems as other competition authorities in defining digital markets and interpreting the behavior of digital firms, the FAS Russia has managed to outpace in some of its decisions even the more experienced authorities such as the EC. Additionally, so far it has been successful in its attempts to alter the behavior of global digital platforms in Russia’s domestic market to the benefit of local competition.

Yet, looking at just these three high-profile cases, it can already be said that the competition authority is somewhat constrained in its choice of instruments of economic analysis. As their use is closely linked with evidence standards, the limitations can become critical with the inevitable increase of scale of dealing with digital companies, which, in turn, might lead to an increase in the frequency of enforcement errors.

Finally, high profile digital cases demonstrate the challenges for authorities of countries with national producers competing with global giants. This explains the pioneering character of Russian antimonopoly law enforcement vis-à-vis the EU and US, in spite of a deficiency of economic analysis. Thus, to some extent, standards of proof are the price for timeliness of industrial policy decisions, where FAS is among the pioneers both at the national and international levels.

²⁰ <https://en.fas.gov.ru/press-center/news/detail.html?id=52952>

²¹ Ibid.

²² <http://en.fas.gov.ru/press-center/news/detail.html?id=54816>

References

- Armstrong, M. (2006). Competition in two-sided markets. *RAND Journal of Economics*, 37(3), 668–691. <https://doi.org/10.1111/j.1756-2171.2006.tb00037.x>
- Avdasheva, S., & Korneeva, D. (2019). Does competition enforcement prevent competitive strategies of digital platforms: Evidence from BRICS. *Russian Management Journal*, 17(4), 547–568. <https://doi.org/10.21638/spbu18.2019.408>
- BRICS Competition Law and Policy Centre (2019). *Digital era competition: A BRICS view*. HSE–Skolkovo Institute for Law and Development.
- Etro, F. (2007). *Competition, innovation and antitrust: A theory of market leaders and its policy implications*. Berlin and New York: Springer.
- Gavil, A., & First, H. (2014). *The Microsoft antitrust cases: Competition policy for the twenty-first century*. Cambridge, MA: MIT Press.
- Golovanova, S. (2014). The concept of “comparable markets” in Russian antitrust practice. *Ekonomicheskaya Politika*, 5, 99–115 (in Russian).
- Golovanova, S., & Pavlova, N. (2018). Access to essential facilities as a condition for competitiveness in adjacent markets. In S. Avdasheva, & A. Shastitko (Eds.), *Antitrust policy on adjacent markets: Theory and practice* (pp. 19–63). Moscow: Delo (in Russian).
- Katz, M. L., & Shapiro, C. (1985). Network externalities, competition, and compatibility. *American Economic Review*, 75(3), 424–440.
- Kosyakina, A., & Podlesnaya, A. (2018). Counteraction to monopolistic activity in the field of software on the example of cases against Microsoft. *Scientific Research of Faculty of Economics*, 10(2), 29–52 (in Russian).
- Ménard, C. (2017). Meso-institutions: The variety of regulatory arrangements in the water sector. *Utilities Policy*, 49, 6–19. <https://doi.org/10.1016/j.jup.2017.05.001>
- Motta, M. (2004). *Competition policy: Theory and practice*. Cambridge University Press.
- OECD (1996). The essential facilities concept. *OECD Policy Roundtables*, No. OCDE/GD(96)113.
- Reinert, E. (2007). *How rich countries got rich ... And why poor countries stay poor*. Carrol & Graf.
- Rochet, J.-C., & Tirole, J. (2003). Platform competition in two-sided markets. *Journal of the European Economic Association*, 1(4), 990–1029. <https://doi.org/10.1162/154247603322493212>
- Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty*, 1, 7–59. <https://doi.org/10.1007/BF00055564>
- Shastitko, A. (2019). Meso-institutions: Proliferating essences or evolving economic research programme? *Voprosy Ekonomiki*, 5, 5–25 (in Russian). <https://doi.org/10.32609/0042-8736-2019-5-5-25>
- Shastitko, A., & Kurdin, A. (2017). The effects of market power expansion of the essential facility owners in software markets. *Upravlenets (The Manager)*, 4(68), 43–52 (in Russian). <https://doi.org/10.29141/2218-5003-2017-6-4-6>
- Shastitko, A., & Pavlova, N. (2019). National antitrust in a global context. *Modern Competition*, 13(3), 5–15 (in Russian). <https://doi.org/10.24411/1993-7598-2019-10301>
- Shastitko, A. E., & Markova, O. A. (2020). An old friend is better than two new ones? Approaches to market research in the context of digital transformation for the antitrust laws enforcement. *Voprosy Ekonomiki*, 6, 37–55 (in Russian). <https://doi.org/10.32609/0042-8736-2020-6-37-55>
- Wright, J., & Stone, J. (2012). Misbehavioral economics: The case against behavioral antitrust. *Cardozo Law Review*, 33(4), 1517–1533.