Non-official translation

Defendant
Apple Inc.
1 Infinite Loop, Cupertino, CA 95014, USA

Duly authorised representatives of the Apple Inc.
address 1: Apple Rus LLC, 4 Romanov Lane, bldg. 2, floor 6, office II, room 54, Moscow, 125009, Russia
address 2: "Baker & McKenzie - CIS, Limited", White Gardens, 9 Lesnaya Street (10 floor), Moscow, 125047, Russia

Plaintiff
Laboratoriya Kasperskogo AO (Kaspersky Lab)
39A Leningradskoe Highway, bldg. 2, Moscow, 125212, Russia

Related party
Apple Rus LLC
4 Romanov Lane, bldg. 2, floor 6, office II, room 54, Moscow, 125009, Russia

RULING

ON THE CASE No. 11/01/10-24/2019

Moscow

Resolutive part of the ruling announced on August 10, 2020
Full and complete ruling issued on August 28, 2020

Commission of the Federal Antimonopoly Service for consideration of the case on violation of the antimonopoly legislation No. 11/01/10-24/2019 composed of Chairman of the Commission – <...> members of the Commission: <...> (hereinafter – the Commission),

having considered the case No. 11/01/10-24/2019 on the grounds of violation by Apple Inc. (1 Infinite Loop, Cupertino, CA 95014, USA) Part 1 of the Article 10 of

the Federal Law No. 135-FZ of July 26, 2006 "On Protection of Competition" (hereinafter – the Law on Protection of Competition),

at presence during the hearing of

- duly authorised representatives of Apple Inc.: <...> (by power of attorney);
- duly authorised representatives of Apple Rus LLC: <...> (by power of attorney);
- duly authorised representatives of Laboratoriya Kasperskogo AO: <...> (by power of attorney),

ESTABLISHED:

I. Preliminary statement

The FAS Russia received the application[1] of Laboratoriya Kasperskogo AO (39A Leningradskoe Highway, bldg. 2, Moscow, 125212) (hereinafter – Kaspersky Lab, Plaintiff) on signs of violation of antimonopoly legislation by Apple Inc. (hereinafter – Apple, Defendant) (Plaintiff and Defendant – hereinafter Parties).

According to the Plaintiff, Apple abused its dominant position in the market of iOS mobile devices by limiting the functionality of the mobile application Kaspersky Safe Kids for parental control (hereinafter – KSK) in order to promote its own similar (competing) application Screen Time (hereinafter – Screen Time).

As part of the consideration of the application, the FAS Russia conducted analysis of the state of competition in the relevant commodity market, during which the dominant position of Apple in the distribution market for applications for iOS mobile devices was established.

Based on the results of the consideration of the application, the materials revealed signs of abuse by Apple of its dominant position in the aforementioned market through the commission of technological, regulatory and behavioral actions.

Based on the results of document evaluation, signs of abuse of a dominant position in the aforementioned market were revealed in the form of inclusion in the mandatory documents for iOS application developers (license agreements, technical regulations, etc.) provisions that negatively affect activities of developers.

More specifically, <...>

[1] Application of Kaspersky Lab of March 19, 2019 No. 3-5-2019/39 (incoming letter No. 45492-ДСП/19 of March 19, 2019) (volume 1-ДСП, inventory position 1, sheets 10-412, second copy of the application – volume 2-ДСП, inventory position 1, sheets 1-238)

Taking the foregoing into consideration, the FAS Russia made a decision to initiate a case against Apple Inc. on the grounds of violation of the Part 1 of the Article 10 of the Law on Protection of Competition.

II. Statement of the case

By the order of the FAS Russia No. 1060/19 of August 6, 2019[2], a case No. 11/01/10-24/2019 against Apple Inc. was initiated on the grounds of violation of the Part 1 of the Article 10 of the Law on Protection of Competition.

By the ruling of the FAS Russia No. АГ/68786/19 of August 8, 2019[3] (hereinafter – ruling on consideration) consideration of the case was scheduled on September 13, 2019. Plaintiff and Defendant were requested to provide documents and information.

By the ruling of the FAS Russia No. АГ/82251/19 of September 20, 2019[4] (hereinafter – ruling on postponement No. 1) the consideration of the case was postponed to November 1, 2019. At the request of the Plaintiff proceedings were transferred to closed consideration, the Defendant was requested to provide documents and information.

By the ruling of the FAS Russia No. АГ/82256/19 of September 20, 2019[5] at the request of the Defendant, an interpreter for the English-speaking representatives of the Defendant was involved in the consideration of the case.

By the ruling of the FAS Russia No. АГ/98616/196 of November 11, 2019[6] the period for consideration of the case was extended until May 8, 2020.

By the ruling of the FAS Russia No. АГ/98618/19 of November 11, 2019[7] (hereinafter – ruling on postponement No. 2) the consideration of the case was postponed to December 13, 2019. Plaintiff and Defendant were requested to provide documents and information. Apple Rus LLC (4 Romanov Lane, bldg. 2, floor 6, office II, room 54, Moscow, 125009, Russia) was involved in the consideration of the case as a related party.

By the ruling of the FAS Russia No. АГ/6517/20 of January 31, 2020[8] (hereinafter – ruling on postponement No. 3) the consideration of the case was postponed to March 2, 2020. Plaintiff and Defendant were requested to provide documents and information.

---

[2] volume 9, inventory position 3, sheets 19-20
[3] volume 9, inventory position 5, sheets 22-32
[4] volume 9, inventory position 10, sheets 46-48
[5] volume 9, inventory position 9, sheets 44-45
[6] volume 9, inventory position 17, sheets 75-76
[7] volume 9, inventory position 18, sheets 77-86
[8] volume 9, inventory position 28, sheets 125-128

By the ruling of the FAS Russia No. АГ/17830/20 of March 6, 2020[9] (hereinafter – ruling on postponement No. 4) the consideration of the case was postponed to April 7, 2020. Defendant was requested to provide documents and information.

By the ruling of the FAS Russia No. АГ/35039/20 of April 24, 2020[10] Apple's application for adjournment of the case due to the challenging epidemiological situation associated with the spread of coronavirus infection was accepted and consideration of the case was postponed to May 12, 2020.

By the ruling of the FAS Russia No. АГ/39708/20 of May 13, 2020[11] Apple's application for adjournment of the case due to the challenging epidemiological situation associated with the spread of coronavirus infection was accepted and consideration of the case was postponed to June 8, 2020.

By the ruling of the FAS Russia No. АГ/48314/20 of June 8, 2020[12] Apple's application for adjournment of the case due to the challenging epidemiological situation associated with the spread of coronavirus infection was accepted and consideration of the case was postponed to July 3, 2020.

By the ruling of the FAS Russia No. АГ/56853/20 of July 6, 2020[13] the consideration of the case was postponed to August 7, 2020 due to the adoption of a statement on the circumstances of the case No. АГ/56924-ДСП/20 of July 6, 2020[14].

The Parties presented their standings regarding the statement on the circumstances of the case No. АГ/56924-ДСП/20 of July 6, 2020 (hereinafter – position of Kaspersky Lab[15] on the statement and position of Apple [16] on the statement respectively). The Commission has analyzed the submitted arguments of the Parties. In the given ruling, the arguments are given a corresponding assessment.

III. Analysis of the state of competition in the commodity market

As part of the consideration of the application, the FAS Russia conducted analysis of the state of competition in the distribution market for applications for iOS mobile devices, the results of which are reflected in the Analytical report[17].

---

[9] volume 9, inventory position 39, sheets 421-424
[10] volume 13, inventory position 9, sheets 152-154
[11] volume 13, inventory position 12, sheets 159-161
[12] volume 13, inventory position 15, sheets 164-166
[13] volume 13, inventory position 19, sheets 185-187
[14] volume 14-ДСП, inventory position 2, sheets 292-370
[15] Letter of Kaspersky Lab No. 3-5-2020/70 of July 22, 2020 (incoming letter No. 128648-ЭП/20 of July 27, 2020), volume 13, inventory position 20, sheets 188-234
[16] Letter of Apple Inc. No. 050820 of August 5, 2020, volume 13, inventory position 22, sheets 236-269
[17] Analytical report on the state of competition in the market for distribution of applications for iOS mobile devices (volume 4, inventory position 9, sheets 131-175)

Time frame of the research.

Since July 11, 2008 (according to media reports[18] and official Apple press release[19]), along with the start of global sales of iPhone 3G smartphones, the App Store was included in the iOS operating system.

It is generally known that developer and copyright holder of the iOS operating system and the App Store is Apple Inc. <...>[20].

The App Store is the only source of installation of applications on iOS mobile devices by end-users (not developers, not testers, etc.), which is generally known <...>[21] and is confirmed by the results of a survey of developers.

There are third-party undocumented ways for end-users to install applications on iOS devices (jailbreak, Cydia, Cyrushub, etc.).

However, such methods violate Subparagraphs "d" and "e" of the Paragraph 2 of the "Apple iOS Software License Agreement"[22] (in terms of iOS decompilation and reproduction of pirate content) that is concluded with end-users, as well as other license agreements, <...>[23], and may require special knowledge and expenses.

In this regard, these installation methods were not taken into account in the analysis and the App Store was identified as the only source of installation of applications on iOS mobile devices by end-users.

Thus, the time frame of the market research is the period from July 2008 (emergence of the App Store) to 2019.

The Commission notes that during the period from 2019 to August 2020, there were no changes in the distribution market for applications for iOS mobile devices.

Description of the App Store.

---

[18] https://appleinsider.com/articles/08/07/10/apples_app_store_launches_with_more_than_500_apps
[19] https://www.apple.com/newsroom/2008/09/09App-Store-Downloads-Top-100-Million-Worldwide/
[20] Item 1 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 7, sheets 418-419)
[21] Item 10 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 177-178)
[22] iOS software license agreements:
iOS 11: https://www.apple.com/legal/sla/docs/iOS11.pdf
iOS 12: https://www.apple.com/legal/sla/docs/iOS12.pdf
iOS 13: https://www.apple.com/legal/sla/docs/iOS13.pdf
[23] Item 11 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 174-176)

Apple describes[24] the App Store on its website as a platform for building applications: *"We provide developers with a flexible platform"*. Apple also describes[25] the App Store as a marketplace: *"The App Store is the world's safest and most vibrant marketplace, giving you the opportunity to deliver your apps and services across iPhone, iPad, Mac, Apple TV, and Apple Watch in 175 countries and 40 languages"*.

When interacting with developers of applications for the App Store, Apple does the following:

<...>

In order to place an application in the App Store, the developer should submit ready-to-use application (including the source code of the application) for review by Apple <...> Thus, when developing an application for the App Store, developers should create App Store-compatible app prior to submitting it to Apple.

After submission, Apple reviews the application and if it meets all the requirements set for developers by the relevant documentation, approves and places it in the App Store. Following that, the application becomes available for download (installation) for users of iOS devices.

Thus, the App Store is a technology platform for hosting applications and Apple provides services for hosting applications on its platform.

Product boundaries of the commodity market.

Possibility of distributing applications intended for use on subscriber devices was determined as a functional purpose of the product.

According to open sources, developers can design applications that operate on subscriber devices running both desktop and mobile operating systems (iOS, Windows[26], Windows Mobile[27], Android[28] and others).

In accordance with the above, the product boundaries are preliminarily defined as the distribution market for applications for subscriber devices: smartphones, tablets, audio players.

The following goods are defined as potential substitutes:

---

[24] https://www.apple.com/ios/app-store/principles-practices/
[25] https://developer.apple.com/app-store/
[26] https://en.wikipedia.org/wiki/Microsoft_Windows
[27] https://en.wikipedia.org/wiki/Windows_Mobile
[28] https://en.wikipedia.org/wiki/Android_(operating_system)

- distribution of applications for stationary devices (running various operating systems, including Windows, macOS[29], Linux[30] and others, or for a specific operating system);
- distribution of applications for mobile devices running a specific mobile operating system (iOS, Android, Windows Mobile, etc.).

Identification of product properties, definition of substitutes and product boundaries of the market under investigation is carried out by a selective survey of consumers – developers of mobile applications for iOS devices.

In order to assess substitutability of the above goods (services), a consumer survey was conducted by sending a questionnaire[31] to Russian and foreign developers (including Defendant and Plaintiff) of software and mobile applications with various functionalities and purposes, in particular: solutions for online banking, call for a taxi, messengers, social networks, e-mail, antivirus programs, parental control software, online cinemas, carpooling (joint long trips by car), car sharing (short-term car rental), navigators, maps, as well as customized programs and applications from any other categories.

Given that the application distribution market is a multilateral market, the analysis also took into account the opinion of end-users – users of applications on subscriber devices.

The following conclusions follow from the results of the analysis of the answers received[32]:

- most developers will not give up developing applications for mobile devices, as it is economically irrational and will result in the loss of a huge user base;
- many developers design applications simultaneously for both iOS and Android, and most of them have separate teams of specialists as these operating systems are substantially different;
- developers are not ready to abandon the development of applications for one mobile OS in favor of any other, because this will lead to loss of users and income;
- only small proportion of developers believe that TVs, game consoles and web versions of applications are an alternative to the App Store for distributing content (subscriptions, etc.);
- most developers consider the App Store as the only way to distribute apps and content for iOS;

---

[29] https://en.wikipedia.org/wiki/MacOS
[30] https://en.wikipedia.org/wiki/Linux
[31] Request of the FAS Russia No. АГ/32418/19 of April 18, 2019 to developers (volume 3, inventory position 1, sheets 1-38)
[32] volumes 3-4, 5-ДСП (all inventory positions), 6-ДСП (inventory position 1-2, sheets 1-53)

- all developers believe that there is no alternative to App Store for distributing iOS applications;
- many developers indicate that developing iOS applications without using the App Store to distribute it would be unprofitable and would not allow entering the mobile applications market.

Thus, for software and mobile application developers, the iOS operating system is not substitutable with any other mobile or desktop operating system. At the same time, most developers consider the App Store as the only channel for distributing content, and all developers consider it as the only channel for distributing mobile applications.

According to consumer (user) surveys conducted by Apple[33] <...> According to Kaspersky Lab surveys[34], 80% of users of iOS devices and 71% of users of Android devices are not ready to abandon their device and switch to a device with a different operating system in case of an increase in the average monthly time and effort spent on finding and installing applications by 10%, while 78% of users of iOS devices and 80% of users of Android devices are not ready to abandon their device and switch to a device with another operating system in the event of an increase of 10% average monthly expenses for purchasing applications, paying for subscriptions and/or additional functions.

Taking the foregoing into consideration, the product boundaries of the market under investigation are defined as the distribution market for applications for mobile devices operating under the iOS system.

Geographical boundaries of the product market.

According to the survey, developers distribute their applications for iOS devices through the App Store and most of them do not set regional restrictions on the installation of applications by end-users (except for the cases where a certain application or certain functionality is prohibited by the laws of the relevant state[35]). Thus, end-users of devices, regardless of their location, can install apps from the App Store without regional restrictions (apart from the exceptions mentioned above).

---

[33] Response of Apple Inc. No. 140220 of February 14, 2020 (incoming letter No. 27723-ДСП/20 of February 14, 2020) to the ruling on consideration (volume 11-ДСП, inventory position 1, sheets 1-92)

[34] Application of Kaspersky Lab No. 3-5-2020/20 of February 25, 2020 (incoming letter No. 34039/20 of February 25, 2020) on deposit of the scientific research to the case materials (volume 9, inventory position 30, sheets 129.1-249)

[35] In a number of states, including the United Arab Emirates, any VoIP services providing video calls are legally prohibited, and therefore applications such as Viber, WhatsApp, Skype, etc. are not available in the App Store on the territory of these states.

It does not matter where the developer is located as software development, including mobile applications, can be carried out anywhere. At the same time, it is well known that Apple supplies iOS mobile devices worldwide.

In this regard, the geographical boundaries of the commodity market under investigation go beyond the territory of the Russian Federation and are defined as global boundaries (world market).

Composition of economic entities operating on the commodity market.

As previously established, the copyright holder of the iOS operating system and the App Store is Apple. End-users can install apps on the iOS devices only from the App Store. Placement of the app in the App Store is possible only after Apple's prior approval.

Thus, Apple is the only seller in the market under investigation that provides developers with the services for placing applications in the App Store and, as a result, distributing these applications to end-users of iOS devices.

Commodity market size and shares of its participants.

Since Apple is the only seller in the market under investigation, the market share of Apple is 100% and it was the same throughout the entire existence of the market.

Determination of concentration ratio of the commodity market.

During the entire existence of the commodity market, the market concentration coefficient is defined as 100% and the Herfindahl Hirschman market concentration index is equal to 10,000. In this regard, the concentration ratio of the market under investigation is defined as high[36].

Determination of barriers to entry.

Since the App Store is the only distribution channel for iOS applications and Apple is the sole copyright holder for iOS and the App Store, developers cannot distribute iOS applications in any other way than by placing them in the App Store.

Taking the foregoing into consideration, the entrance to the market for distributing applications for iOS mobile devices is closed.

Definition of dominant economic entities.

According to the Paragraph 1 of the Part 1 of the Article 5 of the Law on Protection of Competition, dominant position is recognized when an economic entity has a share in the certain goods market that exceeds fifty percent.

[36] In accordance with the Section VII of the Procedure for analyzing the state of competition in the commodity market, approved by the Order of the FAS Russia No. 220 of April 28, 2010

The only seller in the market under investigation is Apple, the market share of this company is 100% and it was the same for the entire existence of the market. Thus, Apple has a dominant position in the market under investigation with a 100% share.

During the consideration of the case, the Defendant presented objections to the analysis of the state of competition in the market for distributing applications for iOS mobile devices.

According to the Defendant, Apple does not have a dominant position in the commodity market under investigation and cannot have a decisive influence on the commodity circulation.

The Defendant believes that the product boundaries of the commodity market defined by the FAS Russia are significantly narrowed, which led to the incorrect determination of the number of sellers and, accordingly, to the incorrect determination of the shares of economic entities – sellers.

Thus, the Defendant states the following.

The survey of developers conducted by the FAS Russia, which determined the product boundaries of the market under investigation, is incorrect, since only 27 developers out of 20 million were interviewed, the sample of surveyed developers is unrepresentative and consists of those developers who make applications that have nothing in common with parental control applications.

Mistakes were made during performance of the hypothetical monopolist test, including incorrect wording of the questions for developers.

According to the Paragraph 3.9 of the Procedure for analyzing the state of competition in the commodity market, approved by the Order of the FAS Russia No. 220 of April 28, 2010 (hereinafter – the Procedure), opinion of the buyers on the composition of the group of substitutes is determined as a result of the hypothetical monopolist test. In order to do that, buyers answered the question: "With what goods and in which amount would you prefer to replace a predetermined product if the price for it increases in long-term by 5-10 percent (longer than one year), and the prices for other goods remain unchanged?"

In the Paragraph 5 of the Guidelines of the FAS Russia No. 17 "On certain issues of analysis of the state of competition" (approved by the Protocol of the Presidium of the FAS Russia No. 3 of April 4, 2019, hereinafter – the Guidelines) it is stated that the consumer survey is conducted using the wording in exact accordance with the Paragraph 3.9 of the Procedure.

Apple argues that the product boundaries of the market under investigation should not be limited to the iOS operating system, but should be defined as a market for the distribution of mobile devices operating on various operating systems.

Apple submitted relevant materials and research to the case file[37], according to which, in Apple's opinion, <...>

The Commission examined the arguments and materials presented by the Defendant and notes the following.

According to the Paragraph 5 of the Guidelines, a full-design study involves a survey of each buyer. It is advisable to conduct it in cases where it is possible to identify and interview all buyers, that is, when the number of buyers is small (for example, no more than 100), they are easily identifiable, have the opportunity to take and participate in the survey.

However, a full-design study of buyers cannot be used in all cases. For example, when there are a lot of buyers or an indefinite range of persons, as well as when the subjects of the target population may be unavailable for one reason or another, or if conducting a full-design study will require large labor and financial costs. In such cases, a sample survey of buyers is carried out.

Obviously, it is impossible to interview 20 million developers. In this regard, 53 Russian and foreign developers selected in a random way were interviewed during the analysis of the market under investigation.

Since the App Store contains not only parental control applications, but also applications from many other areas, among the surveyed developers there are creators of various applications with different functionality and purpose, in particular: parental control applications, solutions for online banking, call for a taxi, messengers, social networks, e-mail, antivirus programs, parental control software, online cinemas, carpooling (joint long trips by car), car sharing (short-term car rental), navigators, maps, as well as customized programs and applications from any other categories

The Commission notes that the case file contains the position of the developers of parental control applications on the possibility of the Defendant's decisive influence on the circulation of goods in the commodity market under investigation. Thus, the Plaintiff (developer of parental control applications) indicates the dominant position of the Defendant in the given commodity market.

Moreover, the case file contains an appeal from the developer of the parental control application Minder.Expert[38], which was received by the FAS Russia during the consideration of the case.

---

[37] Response of Apple Inc. No. 140220 of February 2, 2020 (incoming letter No. 27723-ДСП/20 of February 14, 2020) to the ruling on consideration (volume 11-ДСП, inventory position 1, sheets 1-92)

[38] Appeal of the Minder. Expert (incoming letters No. 210172-ЭП/19 of November 27, 2019 and No. 212590-ДСП/19 of December 2, 2019), volume 10-ДСП, inventory position 5, sheets 242-246

The Analytical report (page 7) emphasizes that the list of developers is not exhaustive, but it demonstrates the fact that software and mobile app developers from different fields were interviewed, many of which do not overlap functionally with each other, but their applications are distributed in a similar way.

In this regard, according to the Commission, the survey of developers on how to distribute these applications is focused on consideration of all possible ways of distributing applications and evaluating their substitutability in order to avoid narrowing product boundaries of the commodity market.

In addition, according to the Commission, relatively low response dispersion of the respondents also indicates the representativeness of the sample.

In this regard, the Commission finds unreasonable arguments of Apple regarding the non-representativeness of the sample, absence of parental control application developers among the interviewed developers, and need to interview only developers of parental control applications.

The Commission considers that the survey of developers conducted during the analysis of the commodity market meets the requirements of the Procedure and takes into account specifics of the commodity market under investigation.

According to the Commission, the Defendant's position on the improper conduct of consumer survey does not take into account specifics of the digital markets.

Digital markets are fundamentally different in their nature and functioning from the markets of goods, works, and services distributed for a fee.

Digital markets are characterized by a variety of ways to monetize products, for example, placing apps in the App Store does not require any payment for the fact of placement or download. However, absence of the fee does not mean that the app is not monetized (not profitable).

Most of the apps in the App Store are free, which is well known and confirmed by survey results, as well as repeatedly confirmed by Apple. In this regard, the question of substitutability of goods with zero price in case of price rise by 5-10%, given by the FAS Russia to developers, would be meaningless and would not allow to properly establishing the product boundaries of the commodity market under investigation.

Apple[39] suggested the following wording for this question: "Suppose the App Store raised commissions, or approval process became longer and harder, or it worsened its terms of interaction with developers so that your spending on interaction with the App Store increased by 5-10%. In this case, are you ready to partially (or completely)

[39] Position of Apple on the statement on the circumstances of the case (Paragraph 1.1.3, page 9)

switch to development of apps for other mobile operating systems, for example, by updating the task priorities for the development team? If so, to what extent?"

In the opinion of the Commission, the wording of the question does not correspond to the Paragraph 3.9 of the Procedure.

The Commission believes that such wording would lead to incorrect results, since each developer may have a different vision of what the deterioration of interaction with Apple means and accordingly developers may have incomparable methodology for estimating the change in the cost of such interaction by 5-10%. In the end, this would lead to biased results.

Regarding the assessment of substitutability of goods in digital markets in terms of deterioration of conditions for interaction with the seller, the Commission notes the following.

A key characteristic of assessing the substitutability of goods in terms of a price change of 5-10% is measurability: it seems possible to calculate the exact costs of the buyer. For example, an industrial manufacturer from the theoretical perspective can replace one raw material with another or, as in Apple's example[40], consumer can reduce the amount of consumed vegetables in favor of fruits due to the rising prices of the former.

Therefore, in relation to physical markets, the question of increasing the value of a distributed for a fee product by 5-10% is reasonable, measurable and the answer to such a question may indicate the presence/absence of substitutability of goods.

However, the costs of interaction between developer and Apple for placing apps in the App Store or the conditions for such interaction cannot be estimated in such a way that the methodology for such evaluation is the same for each developer. Thus, the wording of the question proposed by Apple is judgmental, unmeasurable and unverifiable, and using the answers to such a question would lead to a misrepresentation of the assessment.

In this regard, a questionnaire was sent to the developers containing a list of questions that cannot be interpreted ambiguously and to which the developer can accurately answer: applications for which devices he develops, on which operating systems these devices function, is the developer ready to abandon the desktop operating system in favour of the mobile one, is the developer ready to abandon a specific operating system, can the developer develop applications simultaneously for several operating systems, whether this requires separate teams of specialists or such development can be carried out by the same specialists, etc.

From the obtained results, it was estimated that for developers of software and mobile applications, the iOS operating system is not substitutable with any other

[40] Position of Apple on the statement on the circumstances of the case (Paragraph 1.1.3, page 9)

mobile or desktop operating system. However, most developers consider the App Store to be the only channel for distributing content, and all developers consider he App Store to be the only channel for distributing mobile apps.

According to the Paragraph 3.2 of the Procedure, the definition of product boundaries of the commodity market is based on the opinion of buyers (both individuals and legal entities) on the substitutability of goods. The Commission believes that the Analytical report properly defines the product boundaries of the market under investigation, and the assessment of the substitutability of goods is based on the opinion of buyers (developers). In this regard, the Commission finds unreasonable argument of Apple regarding incorrect wording.

The Commission, having evaluated the arguments and materials submitted by the Defendant regarding the incorrect definition of product boundaries of the commodity market in connection with the network effects and the existing facts of user switching between subscriber devices functioning on different operating systems, notes the following.

The Analytical report provides an assessment of the impact of network effects on the circulation of goods in the commodity market under investigation, as well as describes and takes into account the multi-sided nature of the market.

In connection with the above, the Defendant's argument that the Commission did not take into account the multi-sided nature of the market, as well as did not investigate the impact of network effects, is rejected by the Commission as untenable and does not correspond to the case file.

The market for the distribution of applications for subscriber devices is characterized by network effects, namely the increase in the consumer value of a product due to an increase in the number of users of such a product, or an increase in demand for products and applications that are produced in addition to the main product.

The network effect itself cannot be considered as a factor that contributes to or hinders the emergence of a dominant position – existence of network effects should be evaluated taking into account other conditions of product circulation on the commodity market.

In particular, free switching of users can neutralize the influence of network effects as a significant barrier to enter the commodity market.

The Commission notes that during the consideration of the case, an analysis of the market for the distribution of applications, but not the implementation of subscriber devices, was carried out, the assessment of switching on which is provided by the Defendant.

As indicated in the Analytical report, the application distribution market is multi-sided and when evaluating the substitutability of goods the Commission takes into

account the positions of both app developers and app users – that is, the opinions of both sides of this market are taken into account.

As for the Defendant's arguments regarding the free switching of users in the market for distribution of subscriber devices, the Commission notes the following.

The existence of free switching in the market is such if the consumer does not bear any significant costs. However, in order to switch from one mobile device to another, the consumer should incur significant financial costs in order to purchase a new device, as well as change his own habits of using the device's navigation and certain interface. The Commission is convinced that such costs do not testify to free switching.

Besides, 20% of consumers who switch or are ready to switch to another subscriber device (according to Kaspersky Lab[41]) to <...> (according to Apple[42]), cannot indicate an actual free switching of consumers.

Based on the above, the Commission concludes that the Defendant's argument regarding the consumers' free switching is unjustified.

Defendant argued that Apple has the lack of market power, including the need to invest in development, R&D and attraction (retention) of developers, presence of competition from other platforms (TVs, smart technology, game consoles, etc.), new device manufacturers entering the market, increase of market share of existing device manufacturers, device obsolescence, consumer desire to purchase a new product or device instead of a faulty (malfunctioning) device, increase in the number of costs or lack of required applications. Nevertheless, the Commission considers Defendant's arguments not relevant to the circumstances of the case and the market under investigation and not contradicting the findings of the Analytical report.

Having regard to the above, the Commission comes to a decision that Apple has a dominant position in the distribution market for applications for iOS mobile devices.

IV. Kaspersky Lab's application

Kaspersky Lab is the developer and copyright holder of the Kaspersky Safe Kids (hereinafter – the KSK) iOS application for parental control, designed to prevent children from information security threats such as unwanted and dangerous materials, the content of which is age-restricted.

Required protection in the KSK is provided for by the security systems, including:

---

[41] Application of Kaspersky Lab No. 3-5-2020/20 of February 25, 2020 (incoming letter No. 34039/20 of February 25, 2020) on deposit of the scientific research to the case materials (volume 9, inventory position 30, sheets 129.1- 249).

[42] Response of Apple Inc. No. 140220 of February 14, 2020 (incoming letter No. 27723-ДСП/20 of February 14, 2020) to the ruling on consideration (volume 11-ДСП, inventory position 1, sheets 1-92)

- "Internet Usage Monitoring": allows parents to limit child's access to web sites with unsuitable content on the iOS device and to know which web sites their child visits. The limitation of unsuitable (dangerous for the child) content is carried out by hiding the Safari icon (where such a restriction cannot be implemented);
- "App Control": allows parents to limit their child's access to apps on the iOS device.

These security (blocking) features can be used in iOS applications through configuration profiles or MDM technology. Configuration profiles and MDM technology are more specifically covered by the following sections of the given ruling. Kaspersky Lab pointed out in the application that MDM has never been used in the KSK, security features of the app were carried out only through configuration profile.

Chronology of the KSK application placement in the App Store

<...>

On December 19, 2017, Apple tightened the Paragraph 2.5.1 of the App Store Review Guidelines by adding the following provision: "Apps should use APIs and frameworks for their intended purposes and indicate that integration in their app description". This provision remains in the later versions of the guidelines.

On September 17, 2018, Apple released iOS version 12, which includes Apple's built-in Screen Time parental control application. It has similar features to the parental control application, including security systems mentioned above.

<...>

All the interaction described above, as well as correspondence between Apple and Kaspersky Lab can be found in Annex 12 to the application.

Thus, the Commission, in accordance with the substance of the application concluded that <...>

Kaspersky Lab claims that <...>

Thus, according to the Plaintiff, Apple had misused its dominance by excluding the KSK application from the App Store as a competitor of the Screen Time service, which has resulted in the restriction of competition against the Plaintiff.

Document evaluation carried out by the FAS Russia showed that <...> it may lead to restriction of competition by Apple in relation to the developers of applications for iOS devices.

V. Technological and regulatory aspects of the circumstances of the case

Having analyzed the state of competition in the market under investigation, established the dominant position of Apple and considered the case materials, the Commission finds it necessary to set out in detail how Apple reviews and places third-party applications in the App Store (including its requirements), what is it like and what kind of functionality do the KSK application and the Screen Time service have, what constitutes a configuration profile and MDM technology and what differences do they have.

Apple application review and regulations

A developer who plans to place an iOS application in the App Store has to register with the Apple Developer[43] and enter into the Apple Program Developers License Agreement, which becomes available after the registration. The agreement is entered into by electronic means in the private office of the system upon the acceptance of its implementation and payment by the developer.

The developer then gains access to the App Store Connect[44] system with the same account as for the Apple Developer, develops the application and sends it to Apple[45] for a review, guided by a number of Apple regulatory documents, including:

- App Store Review Guidelines[46];
- <...> [47];
- Apple Developer Agreement[48];
- Device Management[49];
- Mobile Device Management Protocol Reference[50];
- Configuration Profile Reference[51].

These regulations contain Apple's technical, content and user requirements for third-party applications, guidelines for legal inquiries, intellectual property rights, use of personal data, confidentiality protection etc. The list of these regulations is not exhaustive, however, according to Apple[52], <...>

---

[43] https://developer.apple.com/
[44] https://appstoreconnect.apple.com
[45] <...>
[46] App Store Review Guidelines: https://developer.apple.com/app-store/review/guidelines/
[47] <...>
[48] Apple Developer Agreement: https://developer.apple.com/terms/apple-developer-agreement/
[49] Device Management: https://developer.apple.com/documentation/devicemanagement
[50] Mobile Device Management Protocol Reference: https://developer.apple.com/business/documentation/MDM-Protocol-Reference.pdf
[51] Configuration Profile Reference: https://developer.apple.com/business/documentation/Configuration-Profile-Reference.pdf
[52] Item 4 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheet 196)

After the application is sent to Apple by the developer <...>[53] <...>[54];

<...>

Parental control apps, key features, KSK app and Screen Time service

In connection with the development of information technologies and spread of mobile devices among children, developers present apps and programs for parental control, which protect children from unwanted information by tracking and filtering web sources, restricting the use of some applications, restricting calls, tracking the location of child's device etc. Kaspersky Lab has also developed a parental control application called Kaspersky Safe Kids.

Description of functional characteristics of parental control apps

According to the survey of Roskachestvo "High quality parental control applications"[55] published on June 1, 2018, the main functional characteristics of parental control applications include the following:

- password protection of parental control settings;
- hiding of browser and applications;
- ban on installing and deleting applications;
- ban on in-app purchases and request for permission to purchase;
- filtering the content of online stores by age qualification;
- filtering web sites on the principle of "allowed/prohibited all except";
- restriction on the volume of the music;
- restriction on the use of mobile data;
- restriction on the use of the device and blocking the device in a certain time interval, as well as the possibility of remote blocking;
- tracking the location of the child;
- panic button (in case of emergency it allows the child to press the panic button, and the information about this accident will be urgently sent to the parent device along with the child's coordinates);
- phone history monitoring, SMS tracker;
- device usage statistics.

This survey also provides a comparison of the functional characteristics of these applications on the iOS and Android operating systems, as well as the differences between them in the applications from different developers, including the KSK application developed by the Defendant:

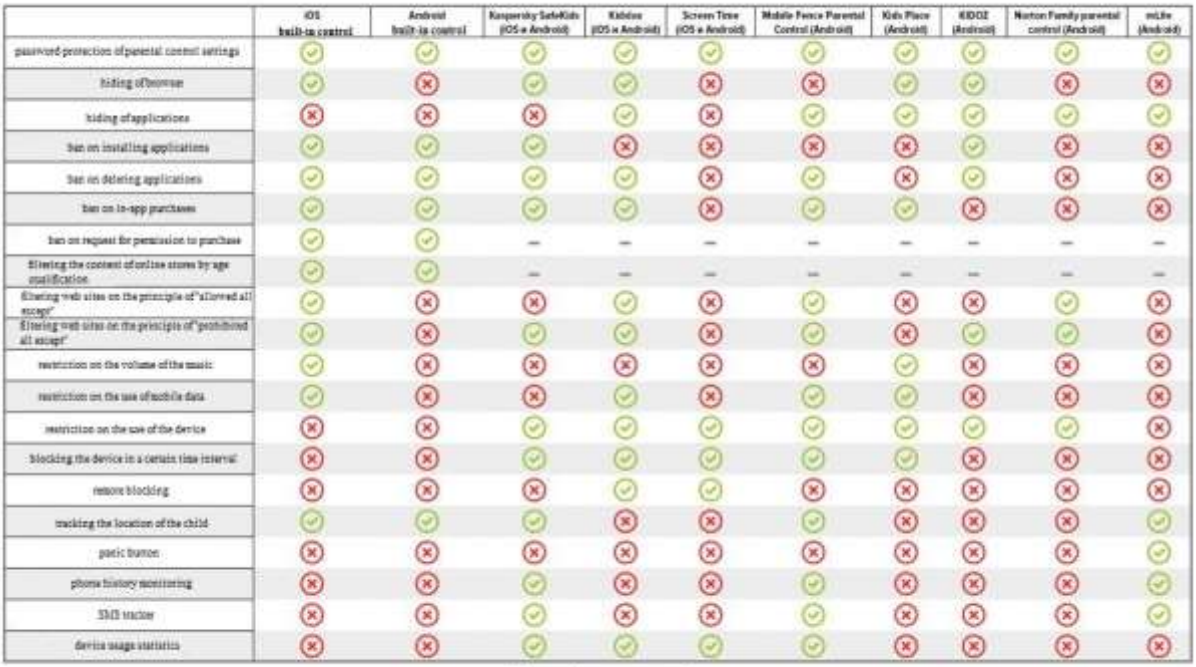
---

[53] Paragraph 7 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 179-182)

[54] <...>

[55] https://rskrf.ru/news/roskachestvo-opredelilo-naibolee-kachestvennye-prilozheniya-dlya-roditelskogo-kontrolya/ (available only in Russian)

FUNCTIONAL CHARACTERISTICS OF PARENTAL CONTROL APPS



	iOS built-in control	Android built-in control	Kaspersky SafeKids (iOS и Android)	Kiddos (iOS и Android)	Screen Time (iOS и Android)	Mobile Fence Parental Control (Android)	Kids Place (Android)	KIDOZ (Android)	Norton Family parental control (Android)	mLife (Android)
password protection of parental control settings	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
hiding of browser	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗
hiding of applications	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓
ban on installing applications	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗
ban on deleting applications	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗
ban on in-app purchases	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗
ban on request for permission to purchase	✓	✓	–	–	–	–	–	–	–	–
filtering the content of online stores by age qualification	✓	✓	–	–	–	–	–	–	–	–
filtering web sites on the principle of "allowed all except"	✓	✗	✗	✓	✗	✓	✗	✗	✓	✗
filtering web sites on the principle of "prohibited all except"	✓	✗	✓	✓	✗	✓	✗	✓	✓	✗
restriction on the volume of the music	✓	✗	✗	✗	✗	✗	✓	✗	✗	✗
restriction on the use of mobile data	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗
restriction on the use of the device	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗
blocking the device in a certain time interval	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗
remote blocking	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
tracking the location of the child	✓	✓	✓	✗	✗	✓	✗	✗	✗	✓
panic button	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓
phone history monitoring	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓
SMS tracker	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓
device usage statistics	✗	✗	✓	✓	✓	✓	✗	✗	✗	✗

РОС КАЧЕСТВО

Kaspersky Safe Kids App (KSK)

Some of the main features of the KSK app for the iOS operating system (version 1.24, rejected by Apple on November 13, 2018) are:

- "Internet Usage Monitoring": allows parents to limit child's access to web sites with unsuitable content on the iOS device and to know which web sites their child visits;
- "App Control": allows parents to limit their child's access to apps on the iOS device.

Other features that are available in the KSK app include monitoring of device usage time, detection of child's location, monitoring of battery charge, monitoring of social media activity, and others[56].

These features are integrated in the KSK app using a configuration profile in accordance with Apple "Configuration Profile Reference".

Right after installing the KSK app, the configuration profile is not yet installed on the iOS device and the security features do not work. To activate them, the parent should launch the KSK app on the child's device, accept the license agreement, and complete the necessary installation procedures:

[56] Full list of the KSK features: item 2 of the response of Kaspersky Lab No 3-5-2019/103 of August 22, 2019 (incoming letter No. 150042-ДСП/19 of August 26, 2019) to the ruling on consideration (volume 2-ДСП, inventory position 2, sheets 8-9); Annex 2 to this response (sheets 306-314). Full list of the KSK features is also available on the Kaspersky website: https://www.kaspersky.ru/safe-kids

- create an account (or use an existing one) in the Safe Kids service[57], log in using it;
- select that the child is using device, enter his name and age;
- agree with the proposal of the KSK to install the configuration profile: the app will report that after installation (1) Safari app icon (browser)[58] that is preinstalled on iOS devices will be hidden (become invisible) and that the child instead will be able to use a safe browser KSK, (2) iOS app icons with age restrictions (in accordance with the age of the child)[59] will be hidden from the home screen (become invisible);
- parent will be redirected to the local web page created by the KSK on the parent's device to download generated configuration profile, then the parent should confirm the profile installation by agreeing to the device's warnings and alerts[60].

After this procedure, the device can be given to the child. You can also password-protect the configuration profile[61] on your child's device so that the child cannot delete it. Then, the parent installs the KSK app on his device, logs in under a previously created account, selects that it is parent's device and receives parental control.

Installation of the configuration profile on the child's device in the KSK app is as follows[62]:

<...>

Screen Time service

Under the application of Apple[63], <...>

Screen Time allows you to set a number of restrictions[64] on an iOS device, including:

---

[57] https://my.kaspersky.com/en

[58] In the next versions of the KSK, the Safari icon hiding feature has been degraded due to Apple's actions, as described below

[59] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p.1.2, page 2)

[60] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p.1.3, page 3)

[61] In the next versions of the KSK, the function of protecting the configuration profile with a password against deletion has been degraded due to Apple's actions, as described below

[62] Slides 22-23.4 of the Annex 1 (presentation) to the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) for ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheets 466-474)

[63] Item 16 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 167-168)

[64] Description of Screen Time features is also available on Apple's website: https://support.apple.com/en-us/HT208982

- ban on purchases from iTunes, App Store, and removing apps from device;
- ban on the use of built-in applications and functions;
- restricted access to adult content in Safari and other apps, as well as possibility to add certain web sites to an approved or blocked list.

Under the application of Apple, <...>[65].

Thus, the Commission concludes that the functionality of the Screen Time service is similar to the functionality of parental control applications, including the KSK app, in terms of security features and parental control. Consequently, the Screen Time and the KSK are competing products.

Configuration profile

The term configuration profile, description of its operation and technical parameters for implementing the functions that the profile provides to the application are contained in the Apple "Configuration Profile Reference".

As for what the configuration profile is and what functionality it can provide, the preamble of the reference indicates:

"A configuration profile is an XML (extended markup language) file that allows you to distribute configuration information. If you need to configure a large number of devices or to provide lots of custom email settings, network settings, or certificates to a large number of devices, configuration profiles are an easy way to do it.

A configuration profile contains a number of settings that you can specify, including:

- *Restrictions on device features*
- *Wi-Fi settings*
- *VPN (virtual private network) settings*
- *Email server settings*
- *Exchange settings*
- *LDAP (lightweight directory access protocol) directory service settings*
- *CalDAV calendar service settings*
- *Web clips*
- *Credentials and keys"*

As for how the configuration profile can be installed on an iOS device, the preamble of the reference states:

"There are five ways to deploy configuration profiles:

- *Using Apple Configurator 2, available in the App Store*
- *In an email message*

[65] Item 2 of the response of Apple Inc. No. 200220 of February 20, 2020 (incoming letter No. 31968-ДСП/20 of February 20, 2020) to ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheets 308-309)

- *On a web page*
- *Using over-the-air configuration*
- *Over the air using a Mobile Device Management Server*[66]*".*

Having regard to the above, the Commission believes that a configuration profile is a file with parameters that is created with direct involvement of the corresponding iOS application (or without such involvement using certain software, such as Apple Configurator 2, iMazing, etc., or created manually in a text editor in XML format) and installed on an iOS device in five different ways. The Commission considers it necessary to note that the KSK application uses only one of them for installing configuration profile on the device ("On a web page")[67].

The configuration profile is created in typewritten form using program code. "Configuration Profile Reference" contains a detailed description of the functions that could be embedded in the configuration profile and how it could be done.

The section "Configuration Profile Keys" of the reference provides a list of profile properties that contain certain keys at the top level. For example, the key "PayloadDisplayName" can be written with a value to which the developer will add any name, such as "Name_1". This means that when installing a configuration profile on an iOS device, the user will see that this profile is called "Name_1".

All other configuration profile keys also start with the words "Payload" that determine how the profile will work and what features it can add to the iOS app and iOS device when it is installed.

A configuration profile can contain several payloads. Each payload contains a set of keys. There are keys that are common to all payloads and describe the payload itself, including "PayloadType", "PayloadDisplayName" and others. There are also payload-specific configuration keys.

Further, the reference contains sections related to the payload code content. In "PayloadDisplayName" code, the developer can specify any value and it will be the profile name that the user sees. However, in most other codes, the developer should specify only those values that the iOS operating system will understand. Those values are contained in these sections.

For example, the section "Restrictions Payload" *("allows the administrator to restrict the user from doing certain things with the device, such as using the camera"*) contains a list of values applied to the Payload. These values include "allowSafari". If you indicate for "allowSafari" the value "false", i.e. "allow Safari is false", this means that Safari is forbidden. In practice, this will mean the following (from the description in the reference):

---

[66] The term is abbreviated as "MDM"

[67] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p.1.7, page.4)

"When false, the Safari web browser application is disabled and its icon removed from the Home screen. This also prevents users from opening web clips. This key is deprecated on unsupervised devices."

To put that into perspective, the Commission provides an example of several lines of program code for the above-mentioned payloads:

```
<dict>
        <key>PayloadDisplayName</key>
        <string>Kaspersky Safe Kids</string>
        <key>PayloadContent</key>
        <array>
            <dict>
                <key>PayloadType</key>
                <string>com.apple.applicationaccess</string>
                <key>PayloadDisplayName</key>
                <string>Restrictions</string>
                 <key>allowSafari</key>
                 <false/>
            </dict>
        </array>
</dict>
```

As reflected from the above lines, the key for "PayloadDisplayName" with the value "Kaspersky Safe Kids" (shows the user that the configuration profile is called "Kaspersky Safe Kids") is applied here together with the key with the value "false" for "allowSafari", which means hiding the Safari browser icon from the desktop[68].

Thus, if the user (parent) of the KSK app during its initial configuration on the child's device enables the "Internet Usage Monitoring" feature, which includes hiding the Safari icon from the device's desktop, the KSK application generates a configuration profile using the "allowSafari" configuration key with the value "false", which [profile] the parent will later download from the local web page on the KSK web server[69].

---

[68] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p. 1.8, page 5-6)

[69] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p. 1.9, page 7)

Taking into account the description of the functional characteristics of parental control applications, the Commission concludes that the presence of a value in the code "allowSafari-false" is a necessary condition that provides one of the most important functional characteristics of the parental control application for the consumer – disabling content that is undesirable for the child.

MDM Protocol Reference

MDM means "Mobile Device Management". This technology is described in the Apple "MDM Protocol Reference".

As with the Configuration Profile Reference, the MDM Protocol Reference contains the descriptive part, codes, and values for them.

The differences between these two references include that the Configuration Profile Reference in the preamble refers to device configuration, while the MDM Protocol Reference in the preamble refers to device management.

Section 1 "About Mobile Device Management" of the reference states that *"The Mobile Device Management (MDM) protocol provides a way for system administrators to send device management commands to managed iOS devices running iOS4 and later, macOS devices running macOSv10.7 and later, and Apple TV devices running iOS7 (Apple TV software 6.0) and later. Through the MDM service, an IT administrator can inspect, install, or remove profiles; remove passcodes; and begin secure erase on a managed device".*

Further, the same section states: *"To provide MDM service, your IT department needs to deploy an HTTPS server to act as an MDM server, then distribute profiles containing the MDM payload to your managed devices".*

Further, the same section states: *"The MDM payload can be placed within a configuration profile (.mobileconfig) file distributed using email or a webpage, as part of the final configuration profile delivered by an over-the-air enrollment service, or automatically".*

"Structure of MDM Payloads" section of the reference states that MDM *"should define four standard payload keys"*:

Key	**Value**
PayloadType	com.apple.mdm.
PayloadVersion	1.
PayloadIdentifier	A value must be provided.
PayloadUUID	A globally unique value must be provided.

In order to properly review the case, the Commission reclaimed[70] Apple and Kaspersky Lab to explain at what point the iOS device becomes manageable and what the management criteria are.

Apple reported[71] the following:

<...>

Kaspersky Lab reported that[72], <...>

Thus, based on the analysis of the Configuration Profile Reference, MDM Protocol Reference, and responses of Apple and Kaspersky Lab, the Commission concludes that for iOS devices that consumers can purchase from a retailer, MDM technology in an iOS app can only be applied if a set of conditions are met:

1) device connects to a pre-deployed MDM server;
2) MDM technology can only be used as part of the program code contained in the configuration profile created in accordance with the Configuration Profile Reference;
3) configuration profile that is installed on the device should contain four aforementioned payloads, and the "PayloadType" should contain the value "com.apple.mdm".

If the aforementioned conditions are not met, from the point of view of Apple's Configuration Profile Reference and MDM Protocol Reference, the device is not managed, that is, it does not have MDM technology applied, and therefore, there is no such technology in the application.

Having regard to the above, the Plaintiff believes that the KSK application does not have MDM technology, because <...>[73], <...>[74].

It should be noted that <...> the Commission notes that this circumstance does not apply to iOS devices sold at retail and purchased by users for personal needs and is

---

[70] Item 3 of the ruling on postponement No. 3, volume 9, inventory position 28, sheet 126
[71] Item 3 of the response of Apple Inc. No. 200220 of February 20, 2020 (incoming letter No. 31968-ДСП/20 of February 20, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheet 307)
[72] Item 2 of the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701- ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheets 524-526)
[73] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p. 1.10, page 7)
[74] Slides 22-23.4 of the Annex 1 (presentation) to the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheets 466-470)

not essential for the consideration of this case[75].

The Commission notes that Apple provided information in the case file on the proper use of configuration profiles and MDM technology in B2C-applications, as well as on the identity or differences between these technologies.

Whether or not there is a ban on using configuration profiles in Apple's regulatory documents.

The Commission examined Apple's regulatory documents that are used by third-party app developers, for whether or not there is a ban on the use of configuration profiles in B2C-applications, and found the following. The ban on using configuration profiles in B2C-applications as of November 13, 2018 (the date of Apple's first rejection of the KSK application) was not contained in the current versions of the Apple Configuration Profile Reference and MDM Protocol Reference, <...>[76].

The Commission did not ascertain this ban for the specified date in other Apple regulations (all existing versions). At the same time, <...>[77]<...>

Apple added <...>

Therefore, in the absence of proof to the contrary, the Commission concludes that <...>[78].

The ban on using configuration profiles in B2C-applications first emerged on June 3, 2019, <...>[79], in Apple's online documentation "Using configuration profiles", which in the preamble contains: *"Configuration profiles are for enterprise use only. With the exceptions of the APN, VPN, and Wi-Fi profiles, do not use configuration profiles with consumer apps".*

The Commission emphasizes that Apple has not announced that ban on using the configuration profile in B2C-applications was introduced in the Configuration Profile Reference, which is a document that directly regulates the technology of

---

[75] Item 2 of the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheets 525-526); Section 4 of the MDM Protocol Reference "Device Enrollment Program"

[76] Item 4 of the response of Apple Inc. No. 271119 of November 27, 2020 (incoming letter No. 213298-ДСП/19 of February 3, 2020) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 415)

[77] <...>

[78] Item 17 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 398)

[79] https://developer.apple.com/documentation/devicemanagement/using_configuration_profiles https://developer.apple.com/documentation/devicemanagement/configuring_multiple_devices_using_profiles

configuration profiles. In the case file, the most current version of the directory provided by Apple is dated September 12, 2019[80], which does not include this ban.

Thus, based on the case file and available online sources, in the absence of proof to the contrary, the Commission concludes that the online documentation outlined above is the only Apple document (other than the aforementioned <...>, which is not applicable to the circumstances considered in this case) that explicitly prohibits the use of configuration profiles in B2C-applications, except for permission to use APN, VPN and Wi-Fi technologies that are not applicable to this case.

According to Apple[81], <...>

Therefore, the Commission hereby records the contradiction between the specified online documentation and the Configuration Profile Reference in terms of the ban on the use of the configuration profile in B2C-applications, which emerged on June 3, 2019.

Whether or not there is a ban on using MDM technology in Apple's regulatory documents.

The Commission examined the Apple documents that guide app developers for whether there are (or are not) bans on the use of MDM technology in B2C-applications, and found the following.

A direct prohibition on the use of MDM technology in B2C-applications as of November 13, 2018 (the date of Apple's first rejection of the KSK application) has always been contained in the above <...>. However, as the Commission has indicated above, < ... > does not cover the applications created outside of <...>, including the Plaintiff's KSK application, and is not an applicable circumstance for the consideration of this case.

<...> according to Apple[82], <...> according to Apple[83]:

---

[80] Annex 13 on electronic media to the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 261)

[81] Item 16 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 399)

[82] Item 5 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 415)

[83] Item 3 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 416)

<...>[84] <...>

The Commission finds this wording indirectly prohibiting the use of MDM in B2C-applications.

<...>[85] <...>

Taking the foregoing into consideration, the Commission found that the use of MDM technology in B2C-applications has been banned since the release of the App Store.

Comparing configuration profile and MDM technologies.

Apple claims[86], <...>

The Commission notes, <...>[87] <...>[88] <...>

The Commission also notes that this ban has always been present indirectly in the MDM Protocol Reference. However, Apple <...>

At the same time, Apple claims: <...>

The Commission notes that <...>Apple links <...>

Apple further claims[89], <...>

The Commission notes that <...> and the online documentation "Using Configuration Profiles" incorporated such a ban only on June 3, 2019. Regarding the online documentation "MDM Commands and Queries", the case file does not indicate the date of inclusion of this ban in the given documentation. However, in the absence of proof to the contrary and based on Apple's claim[90] that <...>, as well

[84] Contained in the electronic media to Apple Inc's response No. 161019 of October 16, 2019 (incoming letter No. 182549-ДСП/19 of October 16, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 1, sheet 4)
[85] Item 16 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 399)
[86] Item 12 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 173-174)
[87] Item 14 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheet 171)
[88] Item 14 to the ruling on consideration (volume 9, inventory position 5, sheet 23)
[89] Item 3 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) o the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 416)
[90] Item 16 of the response of Apple Inc. No. 091219 of December 9, 2019 (incoming letter No. 217531-ДСП/19 of December 9, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 8, sheets 429-430)

as Kaspersky Lab's claim[91] that <...>, the Commission believes that the online documentation "MDM Commands and Queries" introduced this ban not earlier than June 3, 2019.

Apple further claims[92], <...>

Apple further claims[93], <...>

Apple further claims[94], <...>[95] <...>

Apple further claims[96], <...>

Therefore, based on Apple's theses, the Commission concludes that <...>

At the same time, Apple claims that <...> [the Configuration Profile Reference provides only five ways to deliver the configuration profile to the device, as mentioned above – the Commission's note].

<...>

Here Apple notes, <...>

Thus, summarizing all of the above Apple statements, the Commission forms the following theses based on these statements:

<...>

The Commission has assessed all Apple's arguments and statements <...> comes to the following conclusions.

Since Apple's position is that <...>, the Commission assesses this argument.

As mentioned above, Apple said that <...>

The Commission reviewed the Configuration Profile Reference and the MDM Protocol Reference and concluded that the key difference between MDM technology

---

[91] Item 7 of the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheet 516)

[92] Item 4 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 415)

[93] Item 5 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 415)

[94] Item 16 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheet 399)

[95] https://developer.apple.com/documentation/devicemanagement/restrictions

[96] Item 15 of the response of Apple Inc. No. 091219 of December 9, 2019 (incoming letter No. 217531-ДСП/19 of December 9, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 8, sheets 434-436)

and configuration profile that does not include MDM payload is the device management (configuration) method:

- in case of MDM, the system administrator can remotely control the device, change its settings or reset it to factory settings without holding it in hands and going through confirmation procedures. In order to make a comparison, the Commission suggests that in this case, the device is a TV, and the MDM server (from which the commands come) is a remote control. To switch channels or change the volume level, you do not need to go to the TV, it is enough to carry out this procedure using the remote control;
- in case of configuration profile without MDM, no one can control the device remotely. Configuration profile contains any settings or limitations set in its code in advance. After installation, these settings or limitations will apply, but they cannot be changed remotely. To change them, you need to create a new configuration profile and re-install it on the device. In this case, setting the configuration profile will always be accompanied by the need to "hold the device in hands". In order to make a comparison, the Commission suggests that in this case the device is a pipe with a tap, and the configuration profile is a valve. To open or close the valve, you need to go to it and do it with an pipe wrench. You cannot do this remotely.

Therefore, the Commission concludes that the device on which applications with the technologies in question are installed can be in two states: in the "managed" state (if MDM-payload is present in the configuration profile) and in the "configurable" state (if MDM-payload is not present). If the device is managed, it is possible to change the settings and operation of the device remotely. If the device is configured, the device should be "picked up" for this change.

The Commission emphasizes that Apple did not provide evidence in the case file that the two states are the same. All Apple's arguments and claims that < ... > are not supported by the evidence and materials of the case.

Besides, the Commission, relying on the principle of reasonableness, is convinced that developers of iOS-applications should be guided (in terms of compliance with Apple requirements) exclusively by Apple regulations (executed both in the form of separate documents and in the form of online documentation), but they cannot and should not guess whether or not there is a ban on the use of any technologies, if such ban does not explicitly follow from the relevant regulations.

Therefore, since no Apple regulations explicitly prohibited the use of configuration profiles (without MDM) in B2C-applications before June 3, 2019, the Commission concludes that such use was allowed before this date, and bans on MDM technologies in B2C-applications did not apply to configuration profiles without MDM-payload.

Regarding Apple's argument <...>, the Commission notes that <...>

Regarding Apple's argument <...>, the Commission finds this argument inconsistent and relying on the principle of presumption of good faith of parties to business transactions, is convinced that developers who send B2C-applications with a configuration profile without MDM-payload to Apple for a review cannot be suspected or accused of illegally implementing a set of measures for integrating MDM-payload into the configuration profile in the future.

Besides, according to Apple's obligatory regulatory documents for developers, the Defendant can detect and prevent unfair actions of developers. For example, according to the Section 1.4 of the App Store Review Guidelines, Apple may reject an app if it behaves in a way that creates a risk of physical harm to the user (in particular, medical apps that may provide incorrect data or information). Thus, the Commission believes that the suppression of unfair actions of developers should be carried out on a case-by-case basis and should not be assumed for each developer.

VI. Apple's rejection of the Kaspersky Safe Kids app

In this section, the Commission examines the details of the circumstances of Apple's rejection of the KSK application and assesses the eligibility of such rejection, taking into account Apple's regulations.

Assessment of the Paragraph 2.5.1 of the App Store Review Guidelines

Kaspersky Lab provided <...>[97] <...> as part of the application

The Commission, having examined <...>

Kaspersky Lab provided <...>[98] <...> as part of the application

The Commission, having examined <...>

Thus, the Commission found that <...>

In the process of case consideration, Apple stated[99], <...>

Paragraph 2.5.1 of the App Store Review Guidelines contains the following: *"Apps may only use public APIs and must run on the currently shipping OS. Learn more about public APIs. Keep your apps up-to-date and make sure you phase out any*

[97] Annexes 11, 12 to the application of Kaspersky Lab of March 19, 2019 No. 3-5-2019/39 (incoming letter No. 45492-ДСП/19 of March 19, 2019) (volume 1-ДСП, inventory position 1, sheets 30-92, second copy of the application – volume 2-ДСП, inventory position 1, sheets 19-53)
[98] Annexes 11, 13 to the application of Kaspersky Lab of March 19, 2019 No. 3-5-2019/39 (incoming letter No. 45492-ДСП/19 of March 19, 2019) (volume 1-ДСП, inventory position 1, sheets 21-29, second copy of the application – volume 2-ДСП, inventory position 1, sheets 19-53)
[99] Item 12 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 dated October 21, 2019) to the ruling on consideration (volume 10- ДСП, inventory position 2, sheets 172-173)

deprecated features, frameworks or technologies that will no longer be supported in future versions of an OS. Apps should use APIs and frameworks for their intended purposes and indicate that integration in their app description. For example, the HomeKit framework should provide home automation services; and HealthKit should be used for health and fitness purposes and integrate with the Health app."

This statement was present in the guidelines at the time of the first rejection of the KSK <...> and is present now. The key proposal in this statement is: *"Apps should use APIs and frameworks for their intended purposes and indicate that integration in their app description."* Apple stated[100] <...>

The Commission concluded that Apple, <...>

The Commission assessed the circumstances and concluded that Apple rejected the KSK beyond the requirements of the Paragraph 2.5.1 of the App Store Review Guidelines, because, as previously established, configuration profile becomes a part of MDM technology only when its code contains MDM-payload. The KSK app configuration profile does not contain MDM-payload, which is confirmed by <...>

Thus, the configuration profile without MDM-payload was used in the KSK app for its intended purpose due to the absence of a ban on its use in B2C-applications, and the KSK app did not violate the Paragraph 2.5.1 of the App Store Review Guidelines.

Rejection of the KSK app based on the Paragraph 2.5.2 of the App Store Review Guidelines

Apple said[101], <...>[102] <...>

Commission by examining <...>

In Kaspersky Lab's statement on the circumstances of the case[103], Kaspersky Lab stated that it has never received a refusal from Apple to publish any version of the KSK in the App Store based on the Paragraph 2.5.2 of the App Store Review Guidelines. Kaspersky Lab also pointed out[104] that the KSK app complies with the Paragraph 2.5.2 of the App Store Review Guidelines, since (1) the KSK does not

---

[100] Item 15 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 169-170)

[101] Item 15 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheet 169)

[102] Item 15 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheet 169)

[103] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p.1.11, page 8)

[104] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p.1.12, pages 9-10)

"read or write data outside the designated container area" as all the KSK parameters are stored either within the KSK container area locally on an iOS device or on a remote My Kaspersky server, local saving of the configuration profile created by the KSK is also performed within the KSK container area, (2) the KSK does not "download, install, or execute code, which introduces or changes features or functionality of the app, including other apps" as the KSK code does not change from the moment when the KSK is installed until the KSK is updated or removed, (3) using the configuration profile functionality to set restrictions for a child to access web pages with unsuitable content through hiding the Safari browser and to access adult apps cannot be considered a change to the features or functionality of the Safari browser and third-party adult apps installed on an iOS device. Firstly, the configuration profile is applied by parent, not by the KSK app, which only creates the configuration profile. Secondly, restrictions imposed by the configuration profile do not change the functions or functionality of Safari and third-party apps, but only set restrictions on access to them by child.

In this regard, the Commission finds Apple's argument <...> inconsistent and not relevant to the case, since <...>

Paragraph 2.5.2 of the App Store Review Guidelines requires apps to be self-contained in their bundles and not to download, install, or execute code, which introduces or changes features or functionality of the app, including other app.

However, Apple's "MDM Protocol Reference" and "Configuration Profile Reference" provide for loading, installing, and executing code outside the scope of the corresponding app by applying configuration profiles (with/without MDM-payload), since in this case the code is contained not only in the app, but also in the configuration profile, which is a separate file.

These References provide such functionality for configuration profiles (with/without MDM-payload), in which the functionality and characteristics of other apps can be changed, for example, the value "false" of the payload code "allowSafari" leads to disabling the Safari browser and hiding the icon from the device's desktop. That means that using this code, firstly, the app is not self-contained (the code is loaded from the configuration profile, which is a separate file), and, secondly, the functionality of another app (the Safari browser) changes.

Thus, for app developers with a configuration profile (with/without MDM-payload), the requirement of the Paragraph 2.5.2 of the App Store Review Guidelines may become technologically unrealizable or lead to a significant loss of functionality of parental control apps, as well as similar apps.

The Commission also notes that the Paragraph 2.5.2 of the App Store Review Guidelines was in effect until the first rejection of the KSK app <...>

Having regard to the above, the Commission concludes that <...>

VII. Consequences of Apple's actions

In this section, the Commission examines the circumstances relating to Apple's actions with regard to parental control apps and assesses the consequences resulting from these actions, described in chronological order.

iOS 12 release

On September 17, 2018, Apple released the iOS 12 operating system, which includes the built-in Screen Time feature (pre-installed app). This feature has program functionality similar to the parental control app.

Thus, the Commission concludes that the Screen Time feature is a competitor for third-party parental control iOS apps.

The KSK rejection after iOS 12 release

Shortly after the release of iOS 12, Apple rejected another version of the KSK app containing similar Screen Time functionality, which it had repeatedly approved before the release of iOS 12, citing misuse of MDM technology and configuration profiles.

As described above, the Commission found that the KSK always used configuration profiles and at the time of rejection, its use in B2C-applications was not prohibited, but never used the MDM technology that is prohibited in B2C-applications.

<...>[105] <...>

Since support for configuration profiles was deleted from the KSK app version 1.26, the app lost important functionality: hiding the Safari browser from the desktop and setting age restrictions on using (launching/installing) other apps.

It stems from the fact that such functions were implemented in the configuration profile: Safari was hidden using the value "false" in the payload code "allowSafari" and age restrictions were applied using the corresponding values in the payload code "ratingApps" (according to the Configuration Profile Reference, the value = age: 0 = no restrictions, 100 = 4+, 200 = 9+, 300 = 12+, 600 = 17+, 1000 = all). Otherwise, except using a configuration profile, it is technologically impossible to implement such restrictions in iOS apps.

[105] Annexes 11, 13 to the application of Kaspersky Lab of March 19, 2019 No. 3-5-2019/39 (incoming letter No. 45492-ДСП/19 of March 19, 2019) (volume 1-ДСП, inventory position 1, sheets 21-92, second copy of the application – volume 2-ДСП, inventory position 1, sheets 13-29)

Apple specified[106], <...>Kaspersky Lab explained[107], <...>

Configuration profiles may contain other restrictions that apply to parental control functionality. <...>

Thus, due to Apple's actions (rejecting the KSK app and approving it only after configuration profiles were deleted) the KSK app was subjected to a significant functional deterioration and became less competitive, since it lost the important parental control functionality, which exists in the Screen Time.

Further, <...>

From the release of iOS 12 until June 3, 2019, Apple did not make any changes to the app developer regulations that are relevant to the circumstances of this case. There are no changes to the iOS operating system.

Changes to Apple regulations after the release of iOS 12

On June 3, 2019, Apple made changes to the regulations for app developers:

<...>

- App Store Review Guidelines, Paragraph 5.5: *"Mobile Device Management Apps that offer Mobile Device Management (MDM) services must request this capability from Apple. Such apps may only be offered by commercial enterprises (such as business organizations, educational institutions, or government agencies), and in limited cases, companies using MDM for parental control services or device security. You must make a clear declaration of what user data will be collected and how it will be used on an app screen prior to any user action to purchase or otherwise use the service. MDM apps must not violate any applicable laws. Apps offering MDM services may not sell, use, or disclose to third parties any data for any purpose, and must commit to this in their privacy policy. Apps that do not comply with this guideline will be removed from the App Store and you may be removed from the Apple Developer Program"*;
- Apple online documentation "Using configuration profiles"[108], preamble: *"Configuration profiles are for enterprise use only. With the exceptions of the*

[106] Item 18 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheet 165)
[107] Item 5 of the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheet 522)
[108] https://developer.apple.com/documentation/devicemanagement/configuring_multiple_devices_using_profiles

APN, VPN, and Wi-Fi profiles, do not use configuration profiles with consumer apps".

Starting from June 3, 2019, Apple established in the regulations ban on the use of configuration profiles in B2C-applications, possibility of using MDM technology only with the written permission of Apple only for B2B-applications and, as an exception, only for parental control B2C-applications, as well as banned MDM apps from selling, using or disclosing any data to third parties for any purpose.

Apple explained[109], <...>[110]

Kaspersky Lab reported that <...>[111]. On December 21, 2019, Apple granted Kaspersky Lab permission to use MDM technology in the KSK for a period of 1 year[112].

<...> Kaspersky Lab explained[113] the following: <...>

Apple < ...> explained[114] the following: <...>

Thus, based on the analysis of the abovementioned explanations by Apple and Kaspersky Lab, as well as the versions of the App Store Review Guidelines of June 3, 2019 and September 12, 2019 (regarding the provisions on the use of analytical tools), the Commission comes to the following conclusions.

In the version of App Store Review Guidelines of June 3, 2019, Apple completely prohibited the use of analytical tools in any apps that use MDM technology.

---

[109] Item 6.3 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 185-187); Item 11 of the response of Apple Inc. No. 271119 of November 27, 2019 (incoming letter No. 213298-ДСП/19 of February 3, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 5, sheets 405-407)

[110] Item 4 of the response of Kaspersky Lab No. 3-5-2019/103 of August 22, 2019 (incoming letter No. 150042-ДСП/19 of August 26, 2019) to the ruling on consideration (volume 2-ДСП, inventory position 2, sheet 386); Annex 3 to this response (sheets 281-305); Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p.1.14, pages 10-11)

[111] Letter of Kaspersky Lab No. 3-5-2020/25 of February 25, 2020 (incoming letter No. 34010-ДСП/20 of February 25, 2020), volume 12-ДСП, sheet 21; Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p. 1.14, pages 12-13)

[112] Annex 4 to the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheet 362); Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p. 1.14, page 13); Taking into account position of Apple on the statement on the circumstances of the case (item "a", p. 3.4, pages 32-33)

[113] Item 1.4 of the response of Kaspersky Lab No. 3-5-2019/103 of August 22, 2019 (incoming letter No. 150042-ДСП/19 of August 26, 2019) to the ruling on consideration (volume 2-ДСП, inventory position 2, sheets 392-393)

[114] Item 6.3 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 185-187)

In the next version of App Store Review Guidelines of September 12, 2019, Apple added two provisions:

- Paragraph 5.1.4: *"Apps intended primarily for kids should not include third-party analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics and third-party advertising may be permitted provided that the services adhere to the same terms set forth in Guideline 1.3"*;
- Paragraph 1.3: *"Kids Category apps may not send personally identifiable information or device information to third parties. Apps in the Kids Category should not include third-party analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics may be permitted provided that the services do not collect or transmit the IDFA or any identifiable information about children (such as name, date of birth, email address), their location, or their devices"*.

However, Paragraph 5.5 of the App Store Review Guidelines of September 12, 2019 remains unchanged and bans the use of analytical tools in any apps containing MDM technology.

Therefore, analytical tools can only be used in parent control apps that do not have MDM technology. You cannot use these tools in any MDM apps.

The Commission previously established that important consumer security features (hiding the Safari browser, age restrictions that prohibit the use of certain apps, etc.) in parental control apps, in particular in the KSK app, can only be implemented using a configuration profile. Without a configuration profile, such security features cannot be implemented technologically.

However, as mentioned above, since June 3, 2019, Apple has prohibited the use of configuration profiles in B2C-applications in the developer regulations, with the exception of parental control apps that use a configuration profile with MDM-payload, i.e. containing MDM technology.

Thus, the only one way to implement appropriate security features in parental control apps is to use configuration profiles with MDM technology, having received written permission from Apple, which prohibits the use of analytical tools.

Consequently, by the given actions, Apple has effectively prohibited developers of parental control apps from using analytical tools, since such an app will either not use the configuration profile and thus become unattractive to the consumer (functionally useless, uncompetitive with the Screen Time), or will use a configuration profile that only contains MDM-payload, and thus will be subject to a ban on using analytical tools.

Kaspersky Lab reported[115], <...>[116]

<...>

The Commission notes that on June 3, 2019, Apple banned the use of such tools in the regulations for developers of parental control apps, while such tools are critical for the development of apps, and their absence may negatively affect the subsequent operation and, as a result, the further competitiveness of the app.

The Commission finds Apple's security arguments in favor of such a prohibition inconsistent, since Apple could have provided for such measures in the regulations, so that developers of parental control apps (regardless of whether or not the app has a configuration profile or MDM technology) could use analytical tools with certain conditions (for example, approval of tools when submitting the app to Apple for a review or otherwise approving them with Apple), but Apple has established an absolute prohibition, thus depriving developers of such apps of critical tools for app development.

At the same time, Apple uses analytical tools to develop, support, and improve its own apps.

The Commission reviewed Apple's Privacy Policy[117] (updated on December 31, 2019), which states the following:

"Collection and Use of Personal Information

We also collect data in a form that does not, on its own, permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

We may collect information such as occupation, language, zip code, area code, unique device identifier, referrer URL, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.

We may collect information regarding customer activities on our website, iCloud services, our iTunes Store, App Store, Mac App Store, App Store for Apple TV and iBooks Stores and from our other products and services. This information is aggregated and used to help us provide more useful information to our customers and to understand which parts of our website, products, and services are of most

---

[115] Annex 4 to the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheet 366)

[116] Taking into account position of Kaspersky Lab on the statement on the circumstances of the case (p. 1.16, pages 15-16)

[117] https://www.apple.com/legal/privacy/en-ww/

interest. Aggregated data is considered non-personal information for the purposes of this Privacy Policy.

We may collect and store details of how you use our services, including search queries. This information may be used to improve the relevancy of results provided by our services. Except in limited instances to ensure quality of our services over the Internet, such information will not be associated with your IP address.

With your explicit consent, we may collect data about how you use your device and applications in order to help app developers improve their apps.

If we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined."

Apple has also announced <…>[118]

Taking the foregoing into consideration, the Commission concludes that Apple collects various kinds of information (technical, consumer, etc.) that may help to improve its services, including Screen Time, but Apple has deprived third-party parental control applications developers of this opportunity. The Commission believes such actions create a competitive advantage for Screen Time as Apple has the vast amount of information it needs to develop it.

Moving further, <…>

Until September 19, 2019, no changes were made to the iOS 12 operating system related to the circumstances of the present case. There were no other adjustments apart from the changes in the Paragraphs 1.3 and 5.1.4 of the App Store Review Guidelines mentioned above.

iOS 13 release

On September 19, 2019, Apple has released iOS 13, which included changes related to the circumstances of the present case, namely, certain payload codes for configuration profiles now only work on devices that are put into supervised mode.

Apple has also mentioned[119] <…>

Thus, the Commission concludes that the iOS device supervised mode is a special mode (similar to root-access[120] on other operating systems), in which the device's

[118] Item 17 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheets 165-166)

[119] Items 1-2 of the response of Apple Inc. No. 310320 of March 31, 2020 (incoming letter No. 60019-ЭП/20 of April 1, 2020) to the ruling on postponement No. 4 (volume 12-ДСП, inventory position 5, sheets 146-148)

[120] According to the well-known information, root or superuser is a special account, the owner of which has the right to perform all operations without exception

functionality is expanded and can be used by application developers to add such functions that will not be available on a device not set to this mode.

In order to put device in the supervised mode, the consumer should perform a number of actions that require special knowledge and imply the possession of certain products: in particular, it is necessary to use a special program "Apple Configurator 2", available only on Mac PCs. A consumer who does not have a Mac computer cannot, by acceptable means, put an iOS device in a supervised mode.

According to the data gathered by Apple[121], <...>

In practice, this means that the KSK application, using a configuration profile for its operation, cannot hide Safari browser or App Store on the child's device, and child can delete the configuration profile from his device (in the device settings) because the parent cannot set a password to delete the configuration profile. It stems from the fact that required configuration profile codes for "allowSafari" and "RemovalPassword" do not work on an unsupervised device, and putting the device into supervised mode is a difficult (sometimes even impossible) task for the user.

Thus, in addition to hiding Safari browser, which is important for the KSK consumer, all other security features (including those available on an unsupervised iOS 13 device) set by a parent can be easily canceled by a child through deleting the configuration profile.

Along with Kaspersky Lab, other developers of parental control applications that use a configuration profile cannot provide users with password protection against deleting a configuration profile. In particular, the developer of the application for parental control Minder.Expert sent an application to the FAS Russia (attached to the case file[122]). The application indicates <...>

In this regard, the Commission concludes that Apple’s actions of releasing the iOS 13 on September 19, 2019 with the indicated changes, led to an even greater deterioration in the functionality of the KSK application and other parental control applications with configuration profiles, up to a state of their complete ineffectiveness (child can freely delete the configuration profile), which negatively affected competitiveness of the KSK application and similar parental control applications in relation to the Screen Time, where all specified security features are available.

---

[121] Item 3 of the response of Apple Inc. No. 310320 of March 31, 2020 (incoming letter No. 60019-ЭП/20 of April 1, 2020) to the ruling on postponement No. 4 (volume 12-ДСП, inventory position 5, sheets 142-143)

[122] Appeal of the Minder. Expert (incoming letters No. 210172-ЭП/19 of November 27, 2019 and No. 212590-ДСП/19 of December 2, 2019), volume 10-ДСП, inventory position 5, sheets 242-246

Thus, the Commission concludes that actions of Apple in this case were committed not only in relation to the KSK application, but also in relation to similar applications of other developers. This is also confirmed by the fact that, according to media reports of April 29, 2019[123], Apple has removed or restricted at least 11 out of the 17 most downloaded screen time and parental control apps.

In addition, Kaspersky Lab reported, <...>[124]

It actually means that if parent turns on the "always allow" function for the KSK application to determine the location of the device, then the child, having seen the corresponding notification on the device, may accidentally or deliberately press the disable (deny) button, thereby preventing the KSK application from determining the location of the device.

When this happens, the "Secure Perimeter" function, which provides parent with the ability to monitor the location of the child, will stop working in the KSK application.

The Commission notes that the ability of a child to disable the device's location significantly impairs the functionality of the parental control application.

Apple regulations affecting application review

The Commission has reviewed the App Store Review Guidelines and found out that <...> the document contains the following (in all existing editions <...>):

<...>

Thus, Apple has set itself <...> the right to reject an application (refuse publication in the App Store) sent by a developer for any reason, even if this application meets all the requirements.

The Commission believes that the above mentioned provision (<...>) neutralizes the efforts of developers to comply with all the requirements when developing an iOS application, since Apple may still reject the application and may prevent, restrict or eliminate competition in the distribution market for applications on iOS mobile devices (including parental control applications), and creates an uncertain environment for application developers, who cannot be confident that they will be able to distribute their application by complying with Apple's requirements.

---

[123] https://www.theverge.com/2019/4/27/18519888/apple-screen-time-app-tracking-parental-controls-report

[124] Item 5 of the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheet 521)

Apple declared[125], <...> Kaspersky Lab specified[126], <...>

Technological features of the Screen Time

For the purpose of substantive due process, the Commission has requested Apple to clarify which technological capabilities of the iOS operating system Screen Time[127] uses, whether third-party application developers can use these functions[128], and whether Screen Time uses configuration profiles and associated payload codes (such as "allowSafari", etc.)[129].

Apple reported that <...> [130] <...>.[131]

Thus, the Commission concludes that the Screen Time App, including parental control functionality (security features, etc.), uses the technological capabilities of the iOS operating system, which Apple does not provide for third-party developers.

The Commission believes that as such the above actions of Apple lead (may lead) to giving the Screen Time a competitive advantage over third-party parental control applications, since application developers cannot use the specified technological capabilities <...>, as well as configuration profiles in the proper form (it is allowed to use configuration profiles with MDM-payload for B2C-applications only for parental control applications, while the payload codes that are important for the functionality of such an application cannot be used on an unsupervised device, leading to the ineffectiveness of such an application for the consumer).

In addition to that, since the iOS is the only operating system for Apple mobile devices, Apple is forcing the consumer to buy this application bundled with an iOS device. Even if Apple does not charge a separate price for the pre-installed applications, the consumer still pays for it, since its cost is included in the price of

---

[125] Item 24 of the response of Apple Inc. No. 091219 of December 9, 2019 (incoming letter No. 217531-ДСП/19 of December 9, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 8, sheet 428)

[126] Item 3 of the response of Kaspersky Lab No. 3-5-2019/140 of November 27, 2019 (incoming letter No. 211080-ДСП/19 of November 28, 2019) to the ruling on postponement No. 2 (volume 10-ДСП, inventory position 3, sheets 230-232)

[127] Sub-item 16 of item 5 of the ruling on consideration (volume 9, inventory position 5, sheet 23); Sub-item 16 of item 5 of the ruling on postponement No. 2 (volume 9, inventory position 18, sheets 78-79)

[128] Sub-item 1 of item 5 of the ruling on postponement No. 3 (volume 9, inventory position 28, sheet 126)

[129] Sub-item 4 of item 4 of the ruling on postponement No. 4 (volume 9, inventory position 39, sheet 422)

[130] Item 1 of the response of Apple Inc. No. 200220 of February 20, 2020 (incoming letter No. 31968-ДСП/20 of February 20, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2, sheet 308)

[131] Item 4 of the response of Apple Inc. No. 310320 of March 31, 2020 (incoming letter No. 60019-ЭП/20 of April 1, 2020) to the ruling on postponement No. 4 (volume 12-ДСП, inventory position 5, sheet 141)

the entire bundle purchased. The Commission notes that the Screen Time can be considered as a free one by the users, which further reduces the propensity of consumers to switch through the existence of a "zero price effect" (giving consumers comparatively more value to free goods). In addition to that, switching costs may be higher due to the initial integration of the pre-installed application with the operating system and other applications.

Security issues of user (personal) data and confidential information

The Defendant in the case materials refers to the need to ensure the security of user (personal) data and confidential information.

Thus, the Defendant indicates[132], <...>

Further, in position of Apple on the statement on the circumstances of the case, the Defendant states[133]: *"Introduction by the Defendant of restrictions on the use of corporate MDM technology, including configuration profiles in B2C-applications, is associated with the security issues of user data. The Defendant's own functionality Screen Time, which has the function of hiding the Safari browser, as well as the configuration profile technology, through which such function is available under certain circumstances, are fundamentally different in nature. The Screen Time App is a part of the operating system and does not pose a security risk to user data, while configuration profiles can be created by anyone and distributed outside the App Store, including for malicious purposes".*

On June 3, 2019, the Apple amended the App Store Review Guidelines and added Paragraph 5.5: *"Mobile Device Management Apps that offer Mobile Device Management (MDM) services must request this capability from Apple. Such apps may only be offered by commercial enterprises (such as business organizations, educational institutions, or government agencies), and in limited cases, companies using MDM for parental control services or device security. You must make a clear declaration of* ***what user data will be collected and how it will be used*** *on an app screen prior to any user action to purchase or otherwise use the service.* ***MDM apps must not violate any applicable laws. Apps offering MDM services may not sell, use, or disclose to third parties any data for any purpose, and must commit to this in their privacy policy.*** *Apps that do not comply with this guideline will be removed from the App Store and you may be removed from the Apple Developer Program."*

In the next version of the App Store Review Guidelines of September 12, 2019, Apple added two principles:

---

[132] Item 6.3 of the response of Apple Inc. No. 211019 of October 21, 2019 (incoming letter No. 185297-ДСП/19 of October 21, 2019) to the ruling on consideration (volume 10-ДСП, inventory position 2, sheet 187)

[133] Position of Apple on the statement on the circumstances of the case (Paragraph 2.4, page 26)

- Paragraph 5.1.4: *"Apps intended primarily for kids should not include third-party analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics and third-party advertising may be permitted provided that the services adhere to the same terms set forth in Guideline 1.3"*;
- Paragraph 1.3: *"Kids Category apps may not send personally identifiable information or device information to third parties. Apps in the Kids Category should not include third-party analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics may be permitted provided that the services do not collect or transmit the IDFA or any identifiable information about children (such as name, date of birth, email address), their location, or their devices"*.

Thus, the Commission concludes that in 2019 Apple allowed developers of parental control applications to use MDM technology for B2C-applications (non-corporate segment), while banning them from disclosing any data to third parties for any purpose, leading to inability of using analytical tools. However, later Apple has allowed such usage in limited circumstances.

However, an analysis of Apple's regulations and technical documents that developers should be guided by has shown that before the changes and prior to this case, they provided the necessary tools to ensure the security of confidential information and user data.

Thus, <...> contained <...>

in the same version <...>

App Store Review Guidelines of September 19, 2017, also contained a number of provisions related to the security of confidential information and user data, particularly the Paragraph 5.1.1: *"Apps that collect user or usage data must have a privacy policy and secure user consent for the collection"*.

The Paragraph 5.1.4 of the same version contained the following principle: *"Apps in the Kids Category or those that collect, transmit, or have the capability to share personal information (e.g. name, address, email, location, photos, videos, drawings, the ability to chat, other personal data, or persistent identifiers used in combination with any of the above) from a minor* ***must include a privacy policy and must comply with all applicable children's privacy statutes****"*.

The Commission notes that the list of requirements and restrictions related to the protection of the user data and confidentiality of information is not limited to the examples mentioned above and is contained in the case file as part of the regulatory and technical documents provided by Apple that are mandatory for developers of iOS applications.

In the meantime, the above provisions indicate that Apple had the necessary data security monitoring tools and established appropriate requirements to ensure the security of user data and confidentiality of information, including in relation to applications related to children, long before the circumstances of this case.

At the same time, the above regulatory and technical changes introduced by Apple in 2019 are of a clarification nature and do not increase the scope of requirements for ensuring the security of user data and confidentiality of information to the extent that the security of this data and information was not previously provided.

The Commission is convinced that Apple's initial requirements for the developers of iOS applications to comply with legislation on the protection of confidential information and personal data comprehensively provide for all issues related to the security of such data and information. Subsequent adjustments and technical details of such requirements do not fundamentally affect the nature of their content, as earlier documentation stipulated conditions for rejecting applications and their inadmissibility in the App Store when applications did not comply with Apple regulatory and technical documents.

In terms of the usage of MDM technology and configuration profiles authorized by the Apple in B2C parental control applications subject to its written consent on June 3, 2019, the Commission notes that such authorization does not introduce any technological difference from the use described in the MDM Protocol Reference and Configuration Profile Reference. The differences are only contained in those additional requirements, which are imposed on such applications and related to the collection and transfer of data to third parties.

Taking into account the position of Apple outlined above <...> the Commission states that Apple's actions <...> and Apple's position regarding security are contradictory. <...>

Thus, according to Apple's position, <...>

In this regard, the Commission concludes that the changes made by Apple in the regulatory and technical documents are not justified by strengthening the security level of user (personal) data and confidential information.

In terms of the changes in iOS 13, after which certain keys for configuration profiles (including those that allow hiding Safari browser icon and setting a password for deleting the configuration profile) stopped working on devices that are not in supervised mode, the Commission believes that these changes are not related to security, since such features do not include transferring user data to third parties, but may negatively affect the functionality of third-party parental control applications, including the KSK application.

In this regard, the Commission concludes that Apple's argument <...> is inconsistent, <...>

At the same time, Apple did not provide evidence in the case file that the KSK application or parental control applications of other developers ever violated the requirements of the legislation in the field of protection of confidential information and personal data, including in relation to children, contained components or features that violated such requirements in the functionality or the software code of any version of the KSK, and that Apple has ever rejected the KSK for the reason of violating such requirements.

At the same time, the Plaintiff indicated[134], <...>

Based on the foregoing, the Commission concludes that Apple's arguments that the actions of Apple, which are the subject of this case, are aimed at ensuring the security of user (personal) data and confidential information are inconsistent and not supported by the materials of the case.

Applicability of the Law on Protection of Competition to the circumstances of the case considered by the Commission.

Apple stated that Apple's actions fall within the exemption set out in the Part 4 of the Article 10 of the Law on Protection of Competition, which excepted actions that exercise exclusive rights to intellectual property and equivalent means of personalization of a legal entity, means of individualization of products, works or services.

According to the position of the Defendant [135], <...>

With regard to the application of the provisions of the Part 4 of the Article 10 of the Law on Protection of Competition to the circumstances under consideration, the Commission notes the following.

In accordance with the Article 1225 of the Civil Code of the Russian Federation (hereinafter – Civil Code), the results of intellectual activity, which are granted legal protection (intellectual property), include, among other things, programs for electronic computers (computer software).

According to the Paragraph 1 of the Article 1259 of the Civil Code, objects of copyright also include computer software that is protected as literary compositions.

---

[134] Appendix 5 to the response of Kaspersky Lab No. 3-5-2020/13 of February 20, 2020 (incoming letter No. 32701-ДСП/20 of February 21, 2020) to the ruling on postponement No. 3 (volume 11-ДСП, inventory position 2)

[135] Item V.3. of the position of Apple Inc. No. 070620 of June 7, 2020 (No. 99824-ЭП/20 of June 8, 2020) (volume 14-ДСП, inventory position 1, sheets 1-291)

General provisions on the exercise of exclusive rights to the results of intellectual activity are contained in the Article 1229 of the Civil Code. According to the Part 1 of which a person who has the exclusive right to a result of intellectual activity or to the means of individualization (right holder) has the right to use such a result or such means at his own discretion. The right holder may use the exclusive right to the result of intellectual activity or to the means of individualization (Article 1233), unless otherwise provided by the Civil Code.

Further, in accordance with the Paragraph 1 of the Article 1270 of the Civil Code, the author of a work or other right holder has the exclusive right to use this work in accordance with the Article 1229 of the Civil Code in any form and in any way that does not contradict the law (exclusive right to a work).

Thus, the exercise of exclusive rights to computer software is action to use a computer software or action to dispose of exclusive rights to a computer software.

According to the Commission's notes and confirmed by the materials of the case, when distributing applications for iOS devices, developers do not use, reproduce, distribute, process the App Store, as well as API systems provided by Apple for developing their own applications, which means that the developers do not use the work within the nature of the Article 1270 of the Civil Code.

As determined by the Commission, Apple provides app distribution services to developers for iOS devices, for which Apple, rather than app developers, reviews and publishes third-party apps in the App Store, and provides tools to ensure that these apps are compatible with Apple programs by providing program codes, etc. without affecting Apple programs, including without the ability to modify Apple programs.

The Commission notes that the exemption provided for in the Part 4 of the Article 10 of the Law on Protection of Competition does not apply to actions that go beyond the exercise of exclusive rights.

As indicated by the Constitutional Court in the Resolution No. 8-П of February 13, 2018 "In the case concerning the review of the constitutionality of provisions of Paragraph 4 of the Article 1252, Article 1487 and Paragraphs 1, 2 and 4 of the Article 1515 of the Civil Code in connection with the complaint of PAG LLC", according to the Articles 8 (Part 1), 17 (Part 3), 34 (Part 2), 35 (Parts 1 and 2) and 55 (Part 3) of the Constitution of the Russian Federation, rights and freedoms in the field of entrepreneurial and other economic activities prohibited by law should not be carried out in violation of the rights and freedoms of others and endanger constitutionally protected values.

As indicated in the Resolution of the Constitutional Court of the Russian Federation No. 10-П of July 18, 2008, by virtue of the constitutional principle of justice, manifested in the need to balance the rights and obligations of all participants in

market interaction, the freedom recognized for persons engaged in entrepreneurial and other not prohibited by law economic activity, and the protection guaranteed to them, should be balanced by the requirement of a responsible attitude to the rights and freedoms of those affected by their economic activity addressed to these persons.

The constitutional requirement to act in good faith and not abuse one's rights is equally addressed to all participants in civil relations. Based on this, the Civil Code names the following among the basic principles of civil legislation: when establishing, exercising and protecting civil rights and performing civil duties, participants in civil legal relations must act in good faith (Paragraph 3 of the Article 1); no one has the right to take advantage of his illegal or dishonest behavior (Paragraph 4 of the Article 1); any deliberately unfair exercise of civil rights (abuse of law), use of civil rights in order to restrict competition, as well as abuse of a dominant position in the market are not allowed (Paragraph 1 of the Article 10).

The Constitutional Court concludes that the provisions of the antimonopoly legislation, in particular Article 10 of the Law on Protection of Competition, according to which the established requirements do not apply to actions to exercise exclusive rights to the results of intellectual activity and the means of individualization of products, works or services equated to them (Part 4), cannot be interpreted and applied as completely removing conflict of interests of the right holders and other participants in legal relations with respect to the goods on which the corresponding rights are placed, and the related possibility of assessing the behavior of the parties as unfair due to the action of the mechanisms to ensure a balance of constitutionally significant values.

The Commission, guided by the necessity to comply with constitutional principles and guarantees, basics of the civil law, considers it necessary and legally qualified to assess Apple's actions to establish conditions for the distribution of applications for compliance with the requirements of the Law on Protection of Competition.

Matter at issue of this case is not Apple's actions to provide or dispose its own computer software, including the iOS operating system, the App Store and other computer programs, but Apple's behavior in the commodity market in relation to the developers of competing applications that prevents such distribution.

In the circumstances considered by the Commission, Apple defining the functionality of third-party applications goes beyond the exercise of exclusive rights to Apple's computer software.

In accordance with the Paragraph 1 of the Article 10 of the Civil Code, such actions that go beyond the exercise of civil (including exclusive) rights are not subject to legal protection. Such actions cannot be considered as actions to exercise exclusive rights within the legal limits of the enforcement of the right.

In connection with the foregoing, the Commission rejects the Defendant's argument about the need to apply the exemptions established by the Part 4 of the Article 10 of the Law on Protection of Competition, considering it as not based on the materials of the case and not complying with the legislation of the Russian Federation.

On this issue, Kaspersky Lab believes that abuse does not fall under the exclusive right. Apple's actions violate the basic principles laid down in the Constitution of the Russian Federation, in particular, they violate the principles set forth in the Article 34 of the Constitution of the Russian Federation, which prohibit economic activities aimed at monopolization and unfair competition, principles that support competition, set out in the Articles 8 and 2 of the Constitution of the Russian Federation, and basic principles of the Law on the Protection of Competition, namely restricting competition, which is the engine of progress and a source of benefits for consumers. In the Plaintiff's view, Apple's actions under consideration in this case are not actions to exercise exclusive rights.

Taking into account the abovementioned, the Commission comes to the following conclusions:

1) inclusion in <...>, on the basis of which Apple may reject and prevent any third-party application from the App Store for any reason, indicates the creation of conditions of uncertainty on the part of Apple in relation to developers of applications for the iOS operating system and may lead to limited competition in the markets for applications for the iOS operating system;

2) a set of actions by Apple in the period from November 13, 2018 to the present of a technological, regulatory and behavioral nature, which led to a significant difficulty in the implementation of activities for developers of iOS parental control applications, deterioration of the functionality of competing applications, by

    - unjustified rejection and non-admission of parental control applications to the App Store;
    - admission of the parental control application to the App Store only if the developer removes certain technological components from the application, as a result of which the application has lost functionality that is important to the consumer (up to a state of their complete ineffectiveness) and has become unattractive to the consumer, and therefore uncompetitive;
    - technological change of the iOS operating system from version 13 in such a way that the functionality of the third-party parental control application, important for the consumer, stopped working (up to a state of their complete ineffectiveness), while in the Screen Time service such functionality remains in the proper state;

- prohibiting the use of analytical tools in parental control applications by third-party developers, information collected about the operation of the application necessary for the proper development of the application by the developer, while Apple collects and uses such information to improve the Screen Time service;
- Screen Time service uses technological components of the iOS operating system that are not available to third-party application developers;
- inclusion of provisions with double-natured, ambiguous or contradictory interpretation in the technical and legal documentation, which is mandatory for developers,

leads (may lead) to restriction of competition in the market for distribution of parental control applications for the iOS operating system.

According to the Part 1 of the Article 10 of the Law on Protection of Competition, actions (inaction) of an economic entity occupying a dominant position, which result or can result in prevention, restriction or elimination of competition and (or) infringement of the interests of other persons (economic entities) in the sphere of entrepreneurship activity or indefinite range of consumers are prohibited.

The Commission found that Apple, which has a dominant position in the market for distribution of applications for iOS mobile devices, has taken actions that lead (may lead) to restriction of competition.

The Commission, guided by the Article 23, Part 1 of the Article 39, Parts 1-4 of the Article 41, Article 48, Part 1 of the Article 49 of the Law on Protection of Competition,

DECIDED:

1. Acknowledge the following actions of Apple Inc. (1 Infinite Loop, Cupertino, CA 95014, USA):

- inclusion in <...> mandatory for B2C-application developers <...>, on the basis of which Apple may reject and prevent any third-party application from being published in the App Store for any reason;
- a set of actions by Apple during the period from November 13, 2018 to the present of a technological, regulatory and behavioral nature, which led to a significant deterioration in the functionality of third-party parental control applications,

which led (may lead) to the inadmissibility, restriction and elimination of competition among developers of mobile parental control applications for the iOS operating system,

as violation of the Part 1 of the Article 10 of the Federal Law No. 135-FZ of July 26, 2006 "On Protection of Competition".

2. Issue Apple Inc. an order with conditions (remedies) to stop the abuse of dominant position and to take actions aimed at ensuring competition.

Chairman of the Commission <...>

Members of the Commission: <...>

The ruling can be appealed within three months from the date of its adoption in the arbitration court.

Note. In case of failure to comply with the legal ruling of the antimonopoly authority within the prescribed period, the responsibility is established under the Article 19.5 of the Code of Administrative Offences of the Russian Federation.