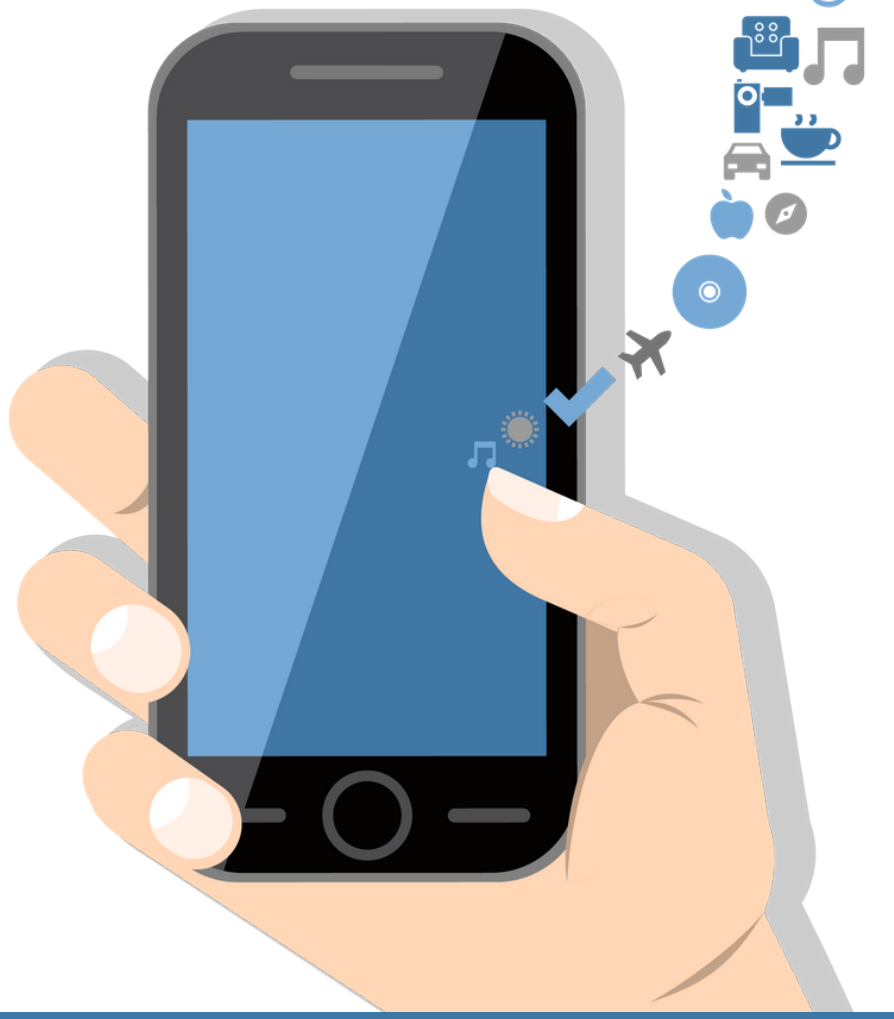
The purpose of the present research is to assess data disclosure policies and practices implemented by four major Russian mobile network operators (Tele2, Beeline, Megafon, MTS). The research also aims to assess the efforts of these companies to safeguard citizens' rights to freedom of expression and privacy, and to comply with standards for protection of human and civil rights in a digital environment.



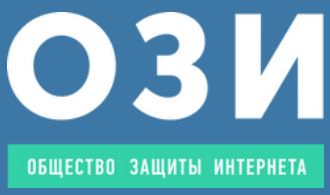
RESEARCH

RANKING TRANSPARENCY OF MOBILE SERVICE PROVIDERS

TELE2 Beeline™ MEGAFON МТС

The research was conducted by independent analysts:

Sarkis Darbinyan
Mikhail Klimarev
Sergei Hovyadinov



The authors of the report are grateful to

ValdikSS (Blockcheck)
Leonid Evdokimov (OONI, The Tor Project)

for their assistance in testing blocking methods and analyzing the collected data.

2018

CONTENTS

INTRODUCTION

Over the last five years, intense regulatory activities in the sphere of Internet governance have introduced into the Russian legislation many new obligations and restrictions for actors which take part in the dissemination and delivery of information over the Internet. These relate not only to Russian users but also to IT, telecom and content markets in general.

When a new digital sovereignty doctrine was rolled out in 2012, information intermediaries were tasked to ensure the implementation of the new requirements in the Russian-speaking segment of the Internet (hereafter, the Runet).

In 2012, the Federal Law "On Information, Information Technologies and Information Protection" was amended to introduce general duties for Internet service providers (ISPs) that obliged them to restrict access to the websites listed in the Unified Register of Domain Names, Internet Website Page Locators, and Network Addresses that Allow to Identify Internet Websites Containing Information Prohibited for Distribution in the Russian Federation ("Unified Register"). The Unified Register is maintained by Federal Service for Supervision of Communications, Information Technology, and Mass Media ("Roskomnadzor").

Subsequently, telecommunications companies got involved in fulfilling more and more functions as part of the implementation of the state information policy, and the scope of their responsibilities has been expanding every year. Over the last five years, eight governmental bodies were entitled to make decisions to regard information as illegal and restrict access to such information upon nine different grounds. According to the Roskomsvoboda data, during five years of enforcement, more than nine million websites and online services were blocked in one way or another due to access restrictions on IP-addresses.

In addition, after the Federal Law of July 6, 2016 No. 374-FZ ("Yarovaya Law") was adopted, communications service providers were tasked to store metadata for three years in the territory of the Russian Federation, as well as to store any messages and content transmitted by subscribers for six months.

However, despite the increasing role of communications service providers in the framework of state control over content distribution and the activities of Runet users, the procedures and practices of cooperation between public authorities and telecommunications companies are not always sufficiently transparent.

The obligation of private companies to respect human rights regardless of the duties imposed upon them by the state is emphasized in the Guiding Principles on Business and Human Rights. The Principles provide for a minimum basic level of corporate transparency in the field of human rights and encourage companies to commit themselves to respecting human rights.

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, also focused on the specific role of private companies in ensuring civil and human rights and freedoms in the digital environment. The Report on the promotion

and protection of the right to freedom of opinion and expression, which was submitted to the UN Human Rights Council, contains a number of recommendations that may seriously encourage the development of soft law norms concerning rights and duties of information intermediaries.

It is pointed out in the recommendations that "when States request corporate involvement in censorship or surveillance, companies should seek to prevent or mitigate the adverse human rights impact of their involvement to the maximum extent allowed by law. In any event, companies should take all necessary and lawful measures to ensure that they do not cause, contribute to or become complicit in human rights abuses."

According to the recommendations, private companies should ensure maximum transparency of their policies, standards and practices concerning freedom of expression and other fundamental rights. Moreover, it is recommended that they include their own obligations to protect freedom of expression in corporate policies, develop products and businesses, train staff and conduct other relevant internal activities aimed at improving protection of human rights.

The penetration of the Internet is becoming more extensive every year. According to the GFK Rus data, at the beginning of 2018, the audience of Internet users age 16+ in Russia was 87 million people, while the audience of the mobile Internet has grown by almost 20% up to 67 million people over the last two years.

The explosive growth of Internet consumption via mobile devices was also confirmed by data provided by the Moscow City Department of Information Technologies. According to the survey, mobile Internet consumption in Moscow has increased five times since 2013.

Taking into account the fact that the Internet consumption has shifted largely to the mobile devices segment, we believe that research on how private companies respect human rights and freedoms should start with the examination of four mobile network operators that share the entire Russian mobile Internet market: *MTS*, *VimpelCom* (brand - "*Beeline*"), *Megafon*, *T2 RTK Holding* (brand - "*Tele2*").

As *AC&M* estimated, there were 254.3 million active SIM-cards at the end of second quarter of 2017. Approximately 31% of them were operated by *MTS*, 30% by *Megafon*, 23% by *VimpelCom*, 16% by *T2 RTK Holding*, and about 1% by other mobile network operators.

The purpose of the present research is to assess data disclosure policies and practices implemented by these operators in the course of their cooperation with governmental authorities and implementation of legal requirements, as well as to assess these companies' efforts to safeguard citizens' rights to freedom of expression and privacy, and to comply with standards for the protection of human and civil rights in the digital environment. It is our understanding that when a user cannot evaluate a company's approach to respecting his/her rights based on publicly available documents before signing a contract with the company, the user is deprived of the opportunity to choose properly an ISP.

We hope that this research becomes the starting point for further regular analysis of policies and practices implemented by both telecom and Internet companies, and that it allows the relevant actors to understand which additional measures need to be implemented to increase the level of respect and protection for human rights in a digital environment. We seek to involve more researchers into further analysis and to popularize its results not only in Russia but also abroad.

METHODOLOGY

In order to conduct this study, we used the methodology of Ranking Digital Rights and localized it to take into an account Russian local context. We used selected indicators and elements from RDR's methodology that were most applicable to the scope of our study, and added several aspects of technical testing (such as looking at companies' "parking pages" etc.) to gain insight into how companies implement their policies in practice.

In order to study companies' policies on human rights we looked at official web resources of all four mobile operators, web resources of their parent companies and corporate groups (e.g., https://veon.com), official blogs of companies (e.g., at https://habrahabr.ru), and other publicly available information.

The subjects studied were grouped into five main categories:
1. The company's stance on respect for human rights.
2. Availability of Terms of Service and Privacy Policy.
3. Protection of users' rights to freedom of information.
4. Protection of users' rights to privacy.
5. Methods of blocking websites.

To reach the conclusions, we examined in detail companies' terms for the provision of services (TOS), privacy policies, as well as other public documents. As we examined the documents, we paid attention primarily to the public commitments of the companies related to privacy and the rights of users to search, receive and disseminate information.

Note

Our research is based exclusively on public documents that can be accessed not only by the subscriber but also by anyone through the official Internet resources of the companies. Throughout the report we use the terms "users" and "subscribers" interchangeably to refer to all potential and current users in the market, because we believe that the companies' attitude towards observing fundamental human rights should be available before choosing a mobile service provider.

The research process consisted of the following stages:

1. Compiling an inventory of relevant publicly available documents of each mobile network operator by the first expert;
2. Evaluating each indicator by the first expert;
3. Validating the results by the second and third experts;
4. Requesting additional information from the companies;
5. "Horizontal check": comparing the results of each company between themselves in order to maintain a unified and objective approach;
6. Running tests to assess the methods of blocking implemented by each operator.

Based on the experts' evaluation, the company received one of the scores:

- "1" (yes) - the information found allows us to conclude that the company clearly demonstrates its commitment to the rights to freedom of information and privacy;
- "0.5" (partially) - the company discloses some information but it is not sufficient to award full credit;
- "0" (no) - we found no evidence of the company's commitment to the rights to freedom of information and privacy.

A total score was calculated based on each of the questions for each indicator.

To study the blocking methods implemented by operators, we used two tests: Blockcheck and OONI Probe (The Open Observatory of Network Interference - https://ooni.torproject.org/).

LEGAL FRAMEWORK AND DOCUMENTS

1. The Universal Declaration of Human Rights.
2. The Convention for Protection of Human Rights and Fundamental Freedoms (ETS N 005) (came into force in the Russian Federation on May 5, 1998).
3. The Constitution of the Russian Federation.
4. The Civil Code of the Russian Federation, Part 4.
5. The Federal Law No. 149-FZ “On Information, Information Technologies and the Protection of Information”.
6. The Federal Law No. 126-FZ “On Communications”.
7. The Federal Law No. 152-FZ “On Personal Data”.
8. The Federal Law No. 139-FZ “On the Protection of Children”.
9. The Federal Law No. 398-FZ “On Introducing Amendments to the Federal Law No. 149-FZ” (“Lugovoi Law”).
10. The Federal Law No. 187-FZ “On Introducing Amendments to the Laws of the Russian Federation Concerning the Protection of Intellectual Rights on the Internet” (“Anti-piracy Law ver. 1.0”).
11. The Federal Law No. 364-FZ “On Introducing Amendments to the Federal Law No. 149-FZ and the Civil Procedure Code of the Russian Federation” (“Anti-piracy Law ver. 2.0”).
12. The Federal Law No. 97-FZ “On Introducing Amendments to the Federal Law No. 149-FZ and to Separate Laws of the Russian Federation in Relation to Streamlining of Information Exchange Over the Internet” (“Law on Bloggers and Providers of Information Dissemination”).
13. The Federal Law No. 242-FZ “On Introducing Amendments to Separate Laws of the Russian Federation on Detailing the Rules of the Personal Data Processing on the Internet” (“Law on Personal Data Localization”).
14. The Federal Law No. 374-FZ “On Introducing Amendments to the Federal Law on Counteracting Terrorism and to Separate Laws of the Russian Federation in Part of Establishing Additional Measures on Counteracting Terrorism and Ensuring Public Safety” (“Yarovaya Law”).
15. The Order of the State Committee of Russia for Communications and Information No. 79 of April 20, 1999 “On Technical Requirements for the System of Technical Facilities Enabling the Conduct of Operational-Search Activities Using Telecommunications Networks of the Russian Federation”.
16. The Guiding Principles on Business and Human Rights.
17. The Report of the Special UN Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38 (2016).
18. Perspectives on Internet Content Blocking: Overview. Internet Society.

GENERAL CONCLUSIONS

1. The surveillance and data interception system created in Russia within the operational investigative activities framework (SORM) is being still actively debated, especially in the light of the adoption of the "Yarovaya Law." No controls or efficient safeguards against the misuse of the SORM system when connecting the FSB to the equipment of communications service providers have yet been created. In *Roman Zakharov v Russia* case, the European Court of Human Rights ruled that "Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret service and the police have direct access, by technical means, to all mobile telephone communications."

However, we discovered that none of the service providers informs its subscribers about such significant risks of violation of their constitutional rights or reveals any information on possible traffic interception by security agencies via the SORM system. Companies' documents which set out the terms for rendering communications services do not contain any information about the fact that ISPs' equipment is connected to the FSB terminal which "mirrors" all the traffic transmitted to/from subscribers. None of the examined mobile communications companies clarifies the way the SORM system functions in their terms of service or privacy policies. Communications service providers do not reveal the number of connections and cases of the SORM system application within operational investigative activities at all.

2. Apart from traffic interception, which requires investigators to follow the formality of getting a court order, requests for subscribers' data, including registration data, geolocation data of devices and information on connection session, are made directly to ISPs quite often. Despite the fact that law enforcement agencies commonly request users' data, no telecom operator publishes information on how such requests are reviewed or how many requests are made. The lack of transparency of Russian companies is very different from the practices of mobile operators in Europe (for example, Telia Company) or in the US (for example, AT&T), which regularly publish information on law enforcement agencies' requests.

3. In 2012, new legal requirements regulating the blocking of access to websites containing illegal information were introduced. The number of state bodies authorized to decide on website blocking, as well as the number of grounds for such blocking, have been increasing every year. Currently, eight different state bodies are entitled to rule on the legality of online content. At the same time, the list of grounds for website blocking is non-exhaustive. Communications service providers are obliged to restrict access to websites listed in the Unified Register of Roskomnadzor under the threat of administrative penalty.

Despite their key role in filtering web applications and content, none of the mobile operators publishes the procedures by which decisions are made to restrict access to certain online resources, the procedures by which one might appeal such decisions, or the number of websites that have blocked.

4. Neither federal legislation, which regulates the dissemenation of digital content on the Internet and stipulates the procedures for restricting access to websites containing illegal information, nor regulatory acts adopted within the relevant framework, establish any

requirements for the “parking pages” - web-pages shown to users when they try to access blocked content. Therefore, mobile network operators are free to decide themselves on the design and content of those pages. In the course of our research, we identified that the nature and scope of information displayed on “parking pages” varied from ISP to ISP.

5. We note that all the examined mobile network operators place their terms of service and privacy policies on collecting, storing and transmitting personal data on their official websites, so that those documents are available to the public. Nevertheless, our experts discovered that the information was presented in legal jargon and contained large amounts of information that was difficult to comprehend. In some cases, it was also problematic to find relevant documents on the companies’ websites.

6. It is worth emphasizing the positive trends in the companies’ willingness to fight spam and fraud, as well as to educate their subscribers on how to protect themselves against cyberthreats on the Internet.

7. Due to the large size of subscriber base and the need to apply the system of “deep packet inspection” (or DPI), the mobile network operators tend to restrict access precisely to the content, which is listed in the Unified Register. In general, we have not found examples of excessive blocking.[1]

8. At the same time, the operators implement different approaches to content blocking. *Tele2* and *Beeline* use “common DPI systems” that do not analyze users’ traffic at non-standard ports. Megafon and MTS apply “full DPI systems” that classify the traffic regardless of the IP address or port and thus are capable of blocking websites even when proxy servers are used or non-standard ports are used to access a website.

9. Examples of “unethical blocking” were detected only in the case of Tele2, which replaced DNS responses for the purpose of blocking and interfered with user traffic.

10. MTS’s blocking system has signs of attempts to substitute SSL-certificates for the blocked resources (an application of MITM). Apparently, such attempts were made to facilitate URL-based content filtering at those websites that were protected by security certificates.

11. Almost all service providers use “parking pages” to advertise their own fee-based services or other third-party services. MTS’s “parking pages” are the most “loaded” with advertisements and web analytics systems.

12. MTS notifies its subscribers of the reasons for blocking in the best way: the reason for website blocking is indicated on the “parking pages” so a subscriber does not need to visit any other resources or enter additional data, which was assessed as good practice.

[1] *See Appendix 2 for more details on the procedures and techniques of content blocking, used by the mobile operarators.*

FINAL RESULT

(from the highest possible)

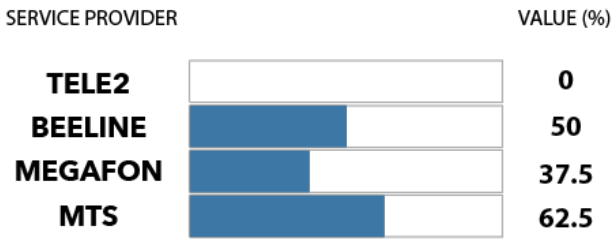
28.2%

27.4%

25.8%

23.4%

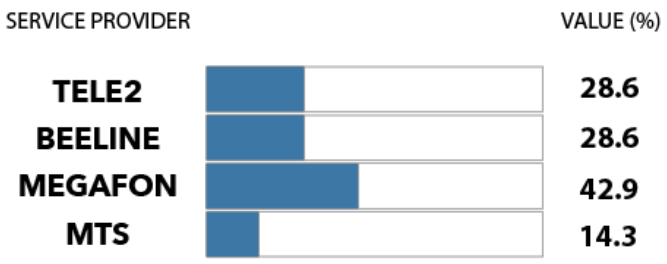
1. Stance on respect for human rights



Adoption of new legal acts in the sphere of content circulation and increasing regulation in terms of storage, communication and dissemination of information, significantly affect existing business models and the interaction between telecom companies, government agencies and law enforcement agencies. During the discussion of new legislative initiatives or at the stage of the adoption of draft laws, the representatives of mobile network operators have the opportunity to state publicly their stand on drafts of normative documents, commenting on their compliance with generally accepted standards in the sphere of human rights such as freedom of information and privacy (including rights to the protection of personal data). Such statements can be expressed in the form of press releases, publications on their own websites, transmission of the stance through professional associations or unions whose members (or founders) are the companies, as well as public comments on the stance of the company and its key employees in response to media requests. This assessment takes into account any corporate activity that announces the attitude of the companies towards current draft laws and laws that directly affect digital human rights, participation in associations that focus on respecting the rights and freedoms of users, and publicly posted information from the companies' policies aimed at respecting these rights, and guaranteeing respect for them.

Out of the four companies examined, Beeline and MTS declare their commitment to respect for human rights in a more outspoken way than Tele2 and Megafon. This can be explained by the participation of their holding companies Veon (for Beeline) and JSFC "Sistema" (for MTS) in the UN Global Compact which requires participants to make commitments to comply with its principles. Unfortunately, at the level of local operating companies, public obligations to respect human rights, and especially the right to freedom of information, are much less clearly articulated or nonexistent.

2. Availability of Terms of Service and Privacy Policy

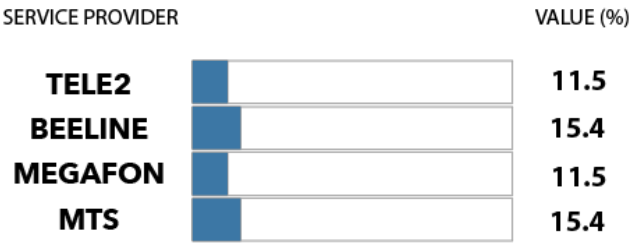


Terms of Service ("TOS"), which lays out rules for the provision of services, is the main document that defines all conditions of the provision of Internet access services, the rights and obligations of the consumer and of the company itself, as well as the responsibilities of the parties and other important conditions. Privacy policy ("Privacy Policy") is a document that contains procedures for obtaining and processing the personal data of users, the purpose of the data collection, the terms of disclosure and transmission of data to third parties and other provisions relating to the privacy of the subscribers.

We determined for each mobile operator how easily TOS and Privacy Policy can be found, how clearly they are written for an ordinary user, and the level of detail in the descriptions of the procedures of making changes to such documents and notifying users about them.

All mobile operators that we reviewed post their own TOS and Privacy Policy on their official websites with public access for a wide range of people. However, our experts noted that the information is presented in a rather complicated format. Publicly available documents are often written in the language of legal officialdom; they are very long and hard to understand. In some cases, these documents are difficult to find on the website and hard to obtain in a convenient form.

3. Protection of users' rights to freedom of information

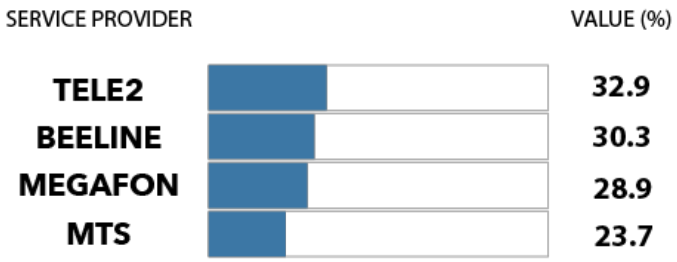


The right to disseminate and receive information is an integral part of the right to freedom of information. In the digital age, access to sites and services on the Internet is a fundamental component of this right. Based on the obligations imposed on telecommunication companies by law, mobile operators play a key role in giving users access to information on the Internet, as they are the ones to implement state policy regarding the dissemination of information online. In this regard, we examined the transparency of companies in terms of whether they publish information on the reasons for restricting access to certain websites and pages, the number of requests to restrict access, and the decision-making procedure for restricting access to web resources. To understand how operators inform their users about the reasons for the inaccessibility of blocked sites, we examined their "parking pages" (web-pages shown to users when they try to access blocked content).

Despite their key role in filtering web applications and content, none of the mobile operators publishes the procedures by which decisions are made to restrict access to certain online resources, the procedures by which one might appeal such decisions, or the number of websites that have blocked.

In the absence of legal requirements for the order of blocking access to websites with illegal information and the content of the "parking page" displayed to the end user trying to access the blocked site, mobile operators independently determine the text they display on these pages. This study identified that the "parking pages" of mobile operators differ significantly in terms of the amount of information that is provided to users when websites and web applications are blocked.

4. Protection of users' rights to privacy



The questions in this category assess whether companies' policies, commitments and practices demonstrate their commitment to respecting users' right to privacy, as well as to protecting their digital security, as provided by the Universal Declaration of Human Rights and other international human rights documents. We considered companies' public declarations regarding how much of users' personal data was collected, its use, and how it is stored and disposed of. Special attention was paid to internal procedures for controlling access to users' data and its provision upon the request of government agencies.

The study found that none of the operators notifies the subscribers about the risks of limiting their constitutional rights and does not disclose information about the possibilities that users' traffic will be monitored by law enforcement agencies using the SORM system. In the basic documents that define the operation of the service, there is no sign that the operator's equipment is connected to the Federal Security Service control panel, through which all user traffic can be "mirrored". None of the mobile network operators include in TOS or in Privacy Policy any explanation of SORM operating procedure. No information is provided about in how many cases the SORM procedure has been applied for the purposes of investigative activity.

Despite the fact that law enforcement agencies commonly request users' data, no telecom operator publishes information on how such requests are reviewed or how many requests are made. In this respect, the lack of transparency of Russian companies is very different from the practices of mobile operators in Europe (for example, Telia Company) or in the US (for example, AT&T), which regularly publish information on law enforcement agencies' requests.

5. Methods of blocking websites

According to the Federal Law of July 28, 2012, No. 139-FZ, which introduced amendments to the Federal Law No. 149-FZ "On Information, Information Technologies and the Protection of Information", Russia-based communications service providers are obliged to apply technical measures to block "illegal websites."

Websites that contain information prohibited for dissemination in Russia are listed in Unified Register. Federal government agencies and courts have the authority to classify information as illegal depending on the type of content. The Unified Register is operated by Roskomnadzor according to the Decree of the Government of the Russian Federation of October 26, 2012, No. 1101.

According to the ISOC analysis,[2] there are 5 types of content blocking:

1. IP and Protocol-based blocking;
2. Deep Packet Inspection-based blocking;
3. URL-based blocking;
4. Platform-based blocking (especially search engines);
5. DNS-based blocking.

Content blocking may occur at the:

1. National level;
2. Carrier and ISP level;
3. Local network level;
4. End-point level.

If the blocking is required by law (as in Russia), general content blocking measures are applied at two levels (*i.e.*, at the state level, within the sphere of responsibility of telecommunications service providers, and at the level of local ISPs). There are different ways to block undesirable and illegal content, and each technique has different consequences. For this reason, the experts specifically focused on the technical measures used for content blocking by the examined companies.

The process of content blocking executed by the examined companies is carried out as follows:

1. Data on websites that contain information which is prohibited for dissemination in Russia is listed in the Unified Register.
2. Mobile network operators are obliged to refer to the Unified Register several times per day, and to download the database in order to execute content blocking. If a service

[2] https://www.internetsociety.org/wp-content/uploads/2017/03/ISOC-ContentBlockingOverview_ru.pdf

provider fails to refer to the Unified Register on a regular basis, it may be found administratively liable. Operators are identified by their digital signatures.

3. All the websites listed in the Unified Register must be blocked by ISPs. Currently, there is no legal requirement for how content should be blocked, so service providers use their discretion in choosing different methods.
4. At the same time, Roskomnadzor oversees the actual content blocking by operators via a "hardware and software complex" called "Revizor." The complex is operated by the Federal State Unitary Enterprise "State Radio Frequency Center" and managed through special probes that are installed on the ISPs' premises. The Revizor monitors access to the prohibited content, and if it is not blocked, Roskomnadzor files a court notice seeking to impose administrative liability on the service provider.

We ran "open tests" using Blockcheck and OONI Probe and analyzed the blocking of both web-sites and individual web-pages that use http and https protocols. The results are presented below:

	TELE2	BEELINE	MEGAFON	MTS
DNS responses substitution	●	○	○	○
Redirecting third party DNS-servers to servers of service provider	○	○	○	○
Blocking of third party DNS-servers	○	○	○	○
Blocking of an entire zone of blocked domain name (subdomains)	○	○	○	○
URL filtering at specific IP addresses and ports ("Common DPI")	●	●	○	○
URL filtering at all IP addresses and/or ports ("Full DPI")	○	○	●	●
Blocking of https-connections	●	●	●	●
Substitution of SSL (HTTPS) certificate	○	○	○	●
IP-based blocking	●	●	●	●

Appendix 1: Questions, assessments and comments on respect for human rights

1. Stance on respect for human rights

	Tele2		Beeline		Megafon		MTS	
	Freedom of expression	Privacy	Freedom of expression	Privacy	Freedom of expression	Privacy	Freedom of expression	Privacy
G1.1[3] Does the company make an explicit, clearly articulated policy commitment to human rights, including freedom of expression and privacy?	0	0	0.5	0.5	0.5	1	0.5	1

[3] *The numbering of questions corresponds to the numbering used in the Ranking Digital Rights index*

	No information found	No information found	Since 2013, Veon (a corporate group of which Beeline is also a part) has been a participant in the UN Global Compact and has formally reaffirmed its commitment to the ten principles of the Global Compact, including the respect for human rights and the prohibition of their violation. Commitment to the respect for human rights was confirmed in a letter sent to the UN in 2015, in Corporate Social Responsibility Report for 2016 and in Corporate Responsibility Report for 2015. Due to the fact that human rights obligations were voiced at an international level on behalf of the controlling	Since 2013, Veon (a corporate group of which Beeline is also a part) has been a participant in the UN Global Compact and has formally reaffirmed its commitment to the ten principles of the Global Compact, including the respect for human rights and the prohibition of their violation. Commitment to the respect for human rights was confirmed in a letter sent to the UN in 2015, in Corporate Social Responsibility Report for 2016 and in Corporate Responsibility Report for 2015. Due to the fact that human rights obligations were voiced at an international level on behalf of the controlling	Megafon points at a common commitment to respect for human rights ("We adhere to generally accepted moral and ethical standards, endorse business transparency, respect human rights and support environmental initiatives. Our sustainability activities are guided by international regulations and standards, including the United Nations Global Compact and the Social Charter of Russian Business. Our reporting on sustainability is part of the Company's annual report and takes into account international	In its annual report for 2016, Megafon points at a commitment to the generally accepted moral and ethical norms and observance of international rights and standards, including the UN Global Compact (not formally its participant). Also the company marked the ensuring of security of information and protection of personal data of users as one of the priorities in order to comply with their rights.	In its Corporate Social Responsibility Strategy for 2017-2020 the company MTS points at the observance of human rights as one of the priorities ("We respect human rights and recognise their importance and the necessity for their blanket distribution. We respect and, where possible, promote the rights provided for by the International Bill of Human Rights, respect the global nature of such rights and take measures to comply with human rights. In situations where the legislation or its application does not ensure adequate protection of human rights, we	In its Corporate Social Responsibility Strategy for 2017-2020 the company MTS points at the observance of human rights as one of the priorities ("We respect human rights and recognise their importance and the necessity for their blanket distribution. We respect and, where possible, promote the rights provided for by the International Bill of Human Rights, respect the global nature of such rights and take measures to comply with human rights. In situations where the legislation or its application does not ensure adequate protection of human rights, we

			company Veon, and the level of obligations voiced for the Russian market and in Russian language is much weaker or nonexistent, Beeline gets partial credit.	company Veon, and the level of obligations voiced for the Russian market and in Russian language is much weaker or nonexistent, Beeline gets partial credit.	standards: the Guidelines on Social Responsibility (ISO 26000) and the Global Reporting Initiative (GRI) Guidelines for sustainability reporting"). Due to the fact that the obligation to protect users' rights to freedom of expression is not mentioned separately, Megafon gets partial credit.		follow the principle of compliance with international norms of behaviour.") Also, a controlling company JSFC "Sistema" is a participant in the UN Global Compact and it has expressed its commitment to the ten principles of the Agreement, including respect for human rights. Since the obligation to protect the rights of users to freedom of expression is not mentioned separately, the company MTS gets partial credit.	follow the principle of compliance with international norms of behaviour.") Also, a controlling company JSFC "Sistema" is a participant in the UN Global Compact and it has expressed its commitment to the ten principles of the Agreement, including respect for human rights. In the 2016 Sustainable Development Report MTS pointed at the protection of confidential information as one of its priorities ("We pay great attention to the protection of confidential data of our clients. When processing the personal data, the Company

								protects them in accordance with the international and Russian laws.")

G5.1: Is the company a member of a multi-stakeholder initiative whose focus includes a commitment to uphold freedom of expression and privacy based on international human rights principles?	0	0	0.5	0.5	0	0	0.5	0.5

	No information found	No information found	Since 2013, Veon (a corporate group of which Beeline is also a part) has been a participant in the UN Global Compact and has formally reaffirmed its commitment to the ten principles of the Global Compact, including the respect for human rights and the prohibition of their violation. Commitment to the respect for human rights was confirmed in a letter sent to the UN in 2015, in Corporate Social Responsibility Report for 2016 and in Corporate Responsibility Report for 2015. Due to the fact that human rights obligations were voiced at an international level on behalf of the controlling	Since 2013, Veon (a corporate group of which Beeline is also a part) has been a participant in the UN Global Compact and has formally reaffirmed its commitment to the ten principles of the Global Compact, including the respect for human rights and the prohibition of their violation. Commitment to the respect for human rights was confirmed in a letter sent to the UN in 2015, in Corporate Social Responsibility Report for 2016 and in Corporate Responsibility Report for 2015. Due to the fact that human rights obligations were voiced at an international level on behalf of the controlling	No information found	No information found	In its Corporate Social Responsibility Strategy for 2017-2020 the company MTS points at the observance of human rights as one of the priorities ("We respect human rights and recognise their importance and the necessity for their blanket distribution. We respect and, where possible, promote the rights provided for by the International Bill of Human Rights, respect the global nature of such rights and take measures to comply with human rights. In situations where the legislation or its application does not ensure adequate protection of human rights, we	In its Corporate Social Responsibility Strategy for 2017-2020 the company MTS points at the observance of human rights as one of the priorities ("We respect human rights and recognise their importance and the necessity for their blanket distribution. We respect and, where possible, promote the rights provided for by the International Bill of Human Rights, respect the global nature of such rights and take measures to comply with human rights. In situations where the legislation or its application does not ensure adequate protection of human rights, we

			company Veon, and the level of obligations voiced for the Russian market and in Russian language is much weaker or nonexistent, Beeline gets partial credit.	company Veon, and the level of obligations voiced for the Russian market and in Russian language is much weaker or nonexistent, Beeline gets partial credit.			follow the principle of compliance with international norms of behaviour.") Also, a controlling company JSFC "Sistema" is a participant in the UN Global Compact and it has expressed its commitment to the ten principles of the Agreement, including respect for human rights. In the 2016 Sustainable Development Report MTS pointed at the protection of confidential information as one of its priorities ("We pay great attention to the protection of confidential data of our clients. When processing the personal data, the Company	follow the principle of compliance with international norms of behaviour.") Also, a controlling company JSFC "Sistema" is a participant in the UN Global Compact and it has expressed its commitment to the ten principles of the Agreement, including respect for human rights. In the 2016 Sustainable Development Report MTS pointed at the protection of confidential information as one of its priorities ("We pay great attention to the protection of confidential data of our clients. When processing the personal data, the Company

							protects them in accordance with the international and Russian laws.")	protects them in accordance with the international and Russian laws.")

G5.2: If the company is not a member of a multi-stakeholder initiative, is the company a member of an organization that engages systematically and on a regular basis with non-industry and non-governmental stakeholders on freedom of expression and privacy?	0	0	0	0	0	0	0	0
	No information found	No information found	No information found	No information found	No information found	No information found	No information found	No information found

G5.3: If the company is not a member of one of these organizations, does the company disclose that it initiates or participates in meetings with stakeholders that represent, advocate on behalf of, or are people whose freedom of expression and privacy are directly impacted by the company's business?	0	0	0	0	0	0	0	0
	No information found	No information found	No information found	No information found	No information found	No information found	No information found	No information found

2. The availability of Terms of Service and Privacy policy

	Tele2	Beeline	Megafon	MTS
F1.1: Are the company's terms of service (ToS) easy to find?	1	0	1	0.5
	The TOS are posted in the section "Blanks and Documents" and are easily accessible via a link on the main page of Tele 2 (https://msk.tele2.ru/)	The TOS can not be found through the company's main page. We could find them only by using the Internet serch	The TOS provided by Megafon are easily accessible (2 clicks from the main page)	Although TOS are available in 2 clicks from the company's home page, it is quite difficult to find them. In addition, on the page of the application for transfer with your user number to MTS you are asked to agree on the terms of service, but there is no link to the text of the conditions itself. The company gets partial credit
F1.3: Are the ToS presented in an understandable manner?	0	0	0	0

	The TOS, in our opinion, are set out in a complex format, written in the language of legal officialdom, are characterized by a large volume and difficulty of perception	The TOS, in our opinion, are set out in a complex format, written in the language of legal officialdom, are characterized by a large volume and difficulty of perception	The TOS, in our opinion, are set out in a complex format, written in the language of legal officialdom, are characterized by a large volume and difficulty of perception	The TOS provided by MTS, in our opinion, are set out in a complex format, written in the language of legal officialdom, are characterized by a large volume and difficulty of perception
P1.1: Are the company's privacy policies easy to find?	0.5	0.5	1	0
	Privacy Policy ("Policy of processing and protecting personal data in the Tele2 Group of Companies") is within two clicks from the company's homepage, but it is located in the "For business" section which, in our opinion, may disorientate subscribers - individuals. In this regard the company gets partial credit.	Privacy Policy ("Policy of processing personal data") it is not easy to find (it is located in the "Disclosure" section which in our opinion is not quite intuitively understandable for users). In this regard, the company gets partial credit.	Privacy policy of Megafon is within two clicks from Home Page.	Privacy Policy ("Policy of processing personal data in PJSC MTS") is difficult to find. It is located within four clicks from the home page ("About the Company" -> "Investor relations" -> "Corporate Governance" -> "PJSC MTS Documents"). For this, the company does not receive any credit.
P1.3: Are the policies presented in an understandable manner?	0.5	1	1	0.5

	Privacy Policy is presented as an internal document of Tele 2 and is set out in a way that is difficult for average users to understand	Privacy Policy is presented as an internal document of the company and set out in a way that, in our opinion, is more understandable for an average user than the documents of Tele 2 and MTS	Privacy Policy is presented as an internal document of the company and set out in a way that, in our opinion, is more understandable for an average user than the documents of Tele 2 and MTS	Privacy Policy is presented as an internal document of MTS and is set out in a way that is difficult for average users to understand
P2.1: Does the company clearly disclose that it notifies users about changes to its privacy policies?	0	0.5	0	0
	Changes to Privacy Policy are introduced by the company Director General's order without mentioning anything about the notification of users	Changes to the Privacy Policy are approved by the President of the company and come into force starting from the moment of its publication on the company's website. Since the notification of subscribers is not directly mentioned, the company gets partial credit.	Privacy Policy of Megafon does not include the mentioning of the users' notification about the changes	Privacy Policy does not include the mentioning of the users' notification about the changes
P2.3 Does the company clearly disclose the timeframe within which it provides notification prior to changes coming into effect?	0	0	0	0

	Privacy Policy does not contain provisions on prior notification of users in the case of the introduction of changes to the document	Privacy Policy of Beeline (clause 11.1) indicates that all changes to the Policy come into effect from the moment of their publication on the company's website, which does not imply prior notification of users	Privacy Policy of Megafon does not contain provisions on prior notification of users in the case of the introduction of changes to the Document	Privacy Policy does not contain provisions on prior notification of users in the case of the introduction of changes to the Document
P2.4: Does the company maintain a public archive or change log?	0	0	0	0
	No information found	No information found	No information found	No information found

3. Protection of users' rights to information

	Tele2	Beeline	Megafon	MTS
F6.5: Does the company list the number of requests that come from different legal authorities?	0	0	0	0
	No information found	No information found	No information found	No information found
F7.5: Does the company describe the types of parties from which it gets requests?	0	0	0	0
	No information found	No information found	No information found	No information found
F7.6: Does the company list the number of requests on the restriction of information including the once it complied with?	0	0	0	0
	No information found	No information found	No information found	No information found

F6.8: Does the company publish the original requests or disclose that it provides copies to a public third-party archive?	0	0	0	0
	No information found	No information found	No information found	No information found
F6.9: Does the company report this data at least once a year?	0	0	0	0
	No information found	No information found	No information found	No information found
F5.7: Does the company clearly disclose that it carries out due diligence on government requests before deciding how to respond?	0	0	0	0
	No information found	No information found	No information found	No information found
F5.8: Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?	0	0	0	0

	No information found	No information found	No information found	No information found
F5.9: Does the company commit to push back on inappropriate or overbroad requests made by governments?	0	0	0	0
	No information found	No information found	No information found	No information found
F5.10: Does the company commit to push back on inappropriate or overbroad private requests?	0	0	0	0
	No information found	No information found	No information found	No information found
F8.2: Does the company clearly disclose that it notifies users who attempt to access content that has been restricted?	1	1	1	1

	Tele2 notifies its users of the blocking. Example of notification is given here.	Beeline notifies its users of the blocking. Example of notification is given here.	Megafon notifies its users of the blocking. Example of notification is given here.	MTS notifies its users of the blocking. Example of notification is given here.
F8.3: In its notification, does the company clearly provide a reason for the content restriction (legal or otherwise)?	0.5	1	0.5	1
	Notification of Tele2 contains general information, without indicating the reasons for the blocking ("This resource is blocked by a decision of government bodies of the Russian Federation"). For this company gets a partial credit.	Notification on the blocking leads to a search page, where, by entering the address of the resource, you can see the reason for the blocking, the number and the date of the decision of the state authority.	As in the case of Tele2, notification of Megafon contains general information, without indicating the reasons for the blocking. For this the company gets partial credit.	Notification on blocking of MTS contains the name of the authority, the number and the date of the decision, on the basis of which access to the resource is blocked.
F9.1: Does the company clearly disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network?	0	0	0	0

	No information found	No information found	No information found	No information found
F9.2: If the company does engage in these practices, does it clearly disclose its purpose for doing so?	0	0	0	0
	No information found	No information found	No information found	No information found

4. Protection of users' rights to privacy

	Tele2	Beeline	Megafon	MTS
F6.5: Does the company list the number of requests that come from different legal authorities?	0	0	0	0
	No information found	No information found	No information found	No information found
F7.5: Does the company describe the types of parties from which it gets requests?	0	0	0	0
	No information found	No information found	No information found	No information found
F7.6: Does the company list the number of requests on the restriction of information including the once it complied with?	0	0	0	0

	No information found	No information found	No information found	No information found
F6.8: Does the company publish the original requests or disclose that it provides copies to a public third-party archive?	0	0	0	0
	No information found	No information found	No information found	No information found
F6.9: Does the company report this data at least once a year?	0	0	0	0
	No information found	No information found	No information found	No information found
F5.7: Does the company clearly disclose that it carries out due diligence on government requests before deciding how to respond?	0	0	0	0

	No information found	No information found	No information found	No information found
F5.8: Does the company clearly disclose that it carries out due diligence on private requests before deciding how to respond?	0	0	0	0
	No information found	No information found	No information found	No information found
F5.9: Does the company commit to push back on inappropriate or overbroad requests made by governments?	0	0	0	0
	No information found	No information found	No information found	No information found
F5.10: Does the company commit to push back on inappropriate or overbroad private requests?	0	0	0	0

	No information found	No information found	No information found	No information found
F8.2: Does the company clearly disclose that it notifies users who attempt to access content that has been restricted?	1	1	1	1
	Tele2 notifies its users of the blocking. Example of notification is given here.	Beeline notifies its users of the blocking. Example of notification is given here.	Megafon notifies its users of the blocking. Example of notification is given here.	MTS notifies its users of the blocking. Example of notification is given here.
F8.3: In its notification, does the company clearly provide a reason for the content restriction (legal or otherwise)?	0.5	1	0.5	1

	Notification of Tele2 contains general information, without indicating the reasons for the blocking ("This resource is blocked by a decision of government bodies of the Russian Federation"). For this company receives partial credit.	Notification on the blocking of Beeline goes to the search page, where, by entering the address of the resource, you can see the reason for the blocking, the number and the date of the decision of the state authority.	As in the case of Tele2, notification of Megafon contains general information, without indicating the reasons for the blocking. For this company receives partial credit.	Notification on blocking of MTS contains the name of the authority, the number and the date of the decision, on the basis of which access to the resource is blocked.
F9.1: Does the company clearly disclose that it does not prioritize, block, or delay certain types of traffic, applications, protocols, or content for reasons beyond assuring quality of service and reliability of the network?	0	0	0	0
	No information found	No information found	No information found	No information found

F9.2: If the company does engage in these practices, does it clearly disclose its purpose for doing so?	0	0	0	0
	No information found	No information found	No information found	No information found

Appendix 2: Description of blocking methods, samples of “parking pages”

Replacement of DNS-responses

DNS replacing (or DNS Spoofing) is one of the most unethical method of blocking implemented by service providers. This method of content blocking works as follows:

DNS (Domain Name System) resolves alphabetical domain names like www.test.com into respective IP addresses like 192.168.0.1, and vice versa. This content blocking method involves communicating false responses to DNS requests of a user. The title of DNS-protocol package has an identification space which is used to match requests and responses. The aim of DNS ID spoofing is to send fake response to a DNS request before proper DNS server responds. In order to do that one needs to predict identificator of the request. Locally, it may be done via a mere network traffic interception, which is performed with the equipment installed at the service provider’s premises.

Such content blocking method is dangerous because it resembles “hacker attacks”, when a user gets redirected to malicious websites like fishing websites where he/she may insert sensitive data, e.g. login, password, pin-code, etc.

We discovered that among four examined service providers only Tele2 used DNS spoofing for content blocking.

Redirecting third party DNS-servers to servers of service providers

Redirecting third party DNS-servers to servers of service providers is similar to DNS-based blocking. But unlike the first blocking method, this one involves forcing user’s DNS requests to the servers of service providers, which makes impossible the use of third party DNS-services or public services like DNS.Yandex (https://dns.yandex.ru/) or Google Public DNS (https://developers.google.com/speed/public-dns/).

The open testing showed that none of the examined service providers used this type of content blocking method.

Blocking of third party DNS-servers

Blocking of third party DNS-servers makes sense while the previous method is implemented and is applied via redirecting. This would make it impossible for subscribers to use third party DNS-services.

Our testing demonstrated that none of the examined service providers used this type of content blocking method.

Blocking of the whole domain name zone (including subdomain names)

Websites names generally contain first-level domains (TLD - e.g., ".ru" zone or ".com" zone) and second-level domains that are separated by a dot (for example, wikipedia.org). Sometimes website owners use third- or higher level domains like in the example "ru.wikipedia.org" where "ru" is a third-level domain.

Some filtering systems block all domains starting from the second-level domains, although the websites of third-level domains may not be related to second-level domains.

Our testing did not reveal any evidence of application of this method of content blocking.

URL-based filtering at specific IP-addresses and ports ("Common DPI")

In accordance with the Federal Law No. 139-FZ, websites may be blocked using the following identificators:

- IP-address - any request directed to a specific IP-address gets blocked regardless of the requested domain name or communications protocol;
- Domain name - the blocking shall be implemented in relation to a specific domain name;
- Specific URL of a webpage with a full identificator of network address (Uniform Resource Locator).

For example, when a full network address, like http://devil.com/restricted-info.html, is listed in the "Unified Register", the logic of content blocking should involve restriction of access to this specific network address. Yet, if the subscriber would use a different protocol (e.g., https instead of http), there should be no access restriction.

Such a method of content blocking is called "common DPI" among service providers, where DPI stands for deep packet inspection. This means that communications service provider should be capable of restricting access strictly to a specific URL.

"Common DPI" is a system that filters certain type of traffic only at ports which are the most common for a respective type of traffic. For example, "common DPI" detects and blocks forbidden HTTP traffic only at the port 80, HTTPS traffic - at the port 443. This type of DPI does not track illegal content in cases where the request with the blocked URL is sent to an IP which is not blocked or to a non-standard port.

The testing revealed that Tele2 and Beeline use "common DPI" content filtering.

URL filtering at all IP addresses and/or ports (“Full DPI”)

Unlike “common DPI”, this type of DPI allows to classify the traffic regardless of the IP address and port. Thus, the blocked websites will not be accessible even if a proxy server at a completely different port and unblocked IP address is used.

The use of “full DPI” was detected in the practice of MTS and Megafon.

Https connections blocking

The main problem of blocking https websites is that it is impossible to restrict access to specific content based on URL. Therefore, service providers block entire https websites based on domain name or IP address.

All the examined service providers block https traffic by restricting access to entire websites even when only URL filtering is required according to the Unified Register.

Replacing SSL (HTTPS) certificate (HTTPS traffic interception)

Some service providers attempt to monitor inter alia encrypted traffic for the purpose of blocking by using the technique of “SSL substitution”. The technical side of the problem is that when a subscriber tries to access a blocked website via HTTPS protocol, a service provider can merely detect the fact of such connection by identifying SNI (Server Name Indication) in the request. SNI - is a TLS protocol extension which allows to transmit during the “handshake” information on the specific host to which a client is connected (there is one IP address, but several hosts). So this name is transmitted openly due to which the DPI system can block only the traffic of an entire domain name which contains URL address listed in the Unified Register.

However, there is another side of the problem: when a subscriber requests a blocked https website, the blocking system of a service provider can not display so called “parking page” (notification about a website being blocked) because the user’s browser requests specific address on the network, as well as SSL certificate of conformity. Since the data received by the browser (parking page) differs from data of the certificate, the browser normally simply closes the connection and displays a notification like “the website can not be accessed”.

The testing by OONI probes revealed the following:

- Tele2: the connection to the blocked HTTPS websites gets broken. OONI: the connection gets broken because the stub server does not respond through https, certificate substitution does not occur.
- Beeline: the service provider restricts access to entire HTTPS websites listed in the Unified Register. OONI: the connection gets broken (a bit differently within different experiments), but no substitution of SSL certificate occur.
- Megafon: the service provider restricts access to entire HTTPS websites listed in the Unified Register. OONI: the connection gets broken, but no substitution of SSL certificate occur.

- MTS: Requests to specific blocked URLs get redirected to “parking page” blocked.mts.ru, including HTTPS requests accompanied with certificate substitution. OONI: substitution of a certificate takes place. However, it remains unknown whether the link is monitored or not.

IP-based blocking

IP-based blocking is the most widespread and simple method of content blocking. In this case, service provider merely breaks any traffic exchange with IP addresses listed in the Unified Register without any analysis of the traffic type and requests to DNS.

At the same time the examined service providers have some differences at applying the IP-based method of content blocking:

- Tele2: Yes, the service provider applies IP-based blocking when an entry in the Unified Register contains only IP address, and displays “parking page” in such cases (http://88.208.38.202). OONI: redirection to “parking page” is performed at "Server": "Ericsson Web Redirect".
- Beeline: Yes, the service provider applies IP-based blocking when an entry in the Unified Register contains only IP address.
- Megafon: Yes, the service provider applies IP-based blocking when an entry in the Unified Register contains only IP address.
- MTS: Yes, the service provider blocks IP addresses. HTTP requests to the blocked IP addresses also get redirected to the stud.

Features of methods of content blocking of various providers

In order to obtain full picture of blocking techniques, we collected screenshots of “parking pages” of the examined service providers.

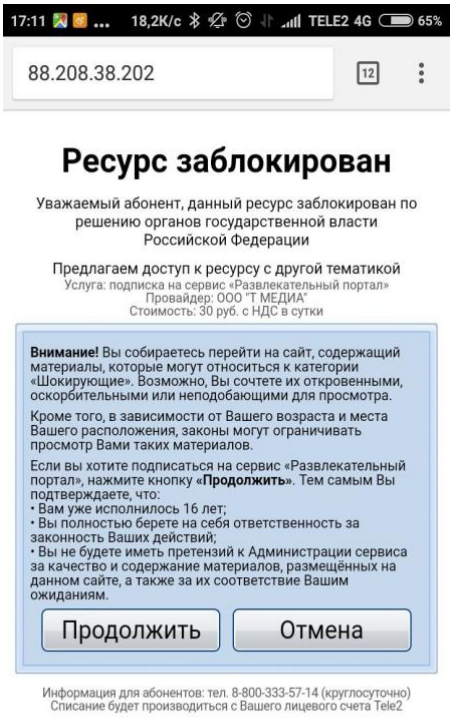
TELE2

Addresses of pages of blocking:

- http://88.208.38.202 (response from outside of a service provider’s network - 403);
- http://t2blocked.com/ (response from outside of network - 403).

The service provider applies several blocking systems in various regions. “Parking pages” are normally quite brief. The reason of access restriction is not displayed - there is a link at the bottom of the page which leads to “Universal service of verification of access restriction of websites and/or URLs on the Internet” operated by the Roskomnadzor.

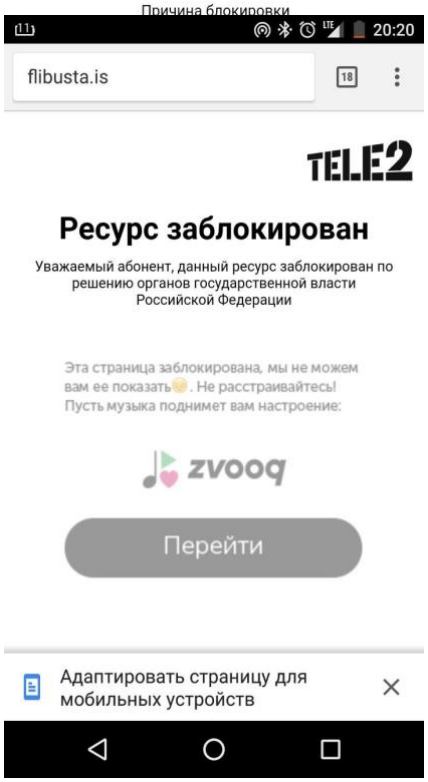
The “parking page” contains advertisement of services offered by the service provider or its partners. Since “parking pages” are not accessible from outside of the network of this service provider, the experts could not conduct a detailed examination of **such** pages.



Translation:
The website is blocked
Dear subscriber, this website is blocked upon a decision of government authorities of the Russian Federation. We would suggest you to visit a website related to other topic. Service: subscription to the service "Entertainment portal". Provider: T Media, LLc. Fee: 30 ru, including VAT, per day. Warning! You are going to visit a website containing the content, which may be categorized as "Shocking". You may consider its content frivolous, offensive or inappropriate. Moreover, depending on your age and location, the law may restrict viewing of such content. If you are willing to subscribe for the service "Entertainment portal", click "Continue". By doing so you confirm that:
- you are 16+;
- you are fully responsible for legality of your own deeds;
- you would not address any complaints to the Administration of the service related to quality and contents of materials displayed at the website, as well as to meeting your expectations.

CONTINUE – CANCEL

Hotline for subscribers 8-800-333-57-14 (24/7). You will be charged from your Tele2 account.
The reason of blocking.



Translation:
The website is blocked.
Dear subscriber, this website is blocked upon a decision of governmental bodies of the Russian Federation. This web page is blocked, we can show you the page. Don't get upset! Let the music cheer you up: svooq

Visit

Translation:
The website is blocked. Dear subscriber, this website is blocked upon a decision of governmental bodies of the Russian Federation.

New cartoons at kids portal. 1 day free of charge. 8 rubles per day.

The reason of blocking.

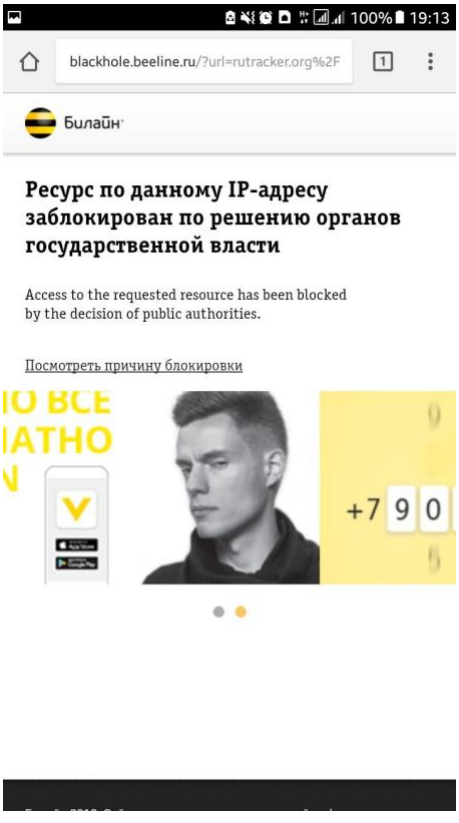
Beeline™

The “parking pages” are displayed in response to requests from networks of any service provider http://blackhole.beeline.ru/.
The reason of blocking of a specific web page may be checked at the “clients support resource” - different regions are assigned with separate addresses. For example, the address for customers from Moscow city region is the following: https://moskva.beeline.ru/customers/help/safe-beeline/ugrozy-v-internete/zablokirovannye-resursy/.

Apparently for the purpose of collecting statistical data, the Google tag-manager and html-code of Piwik advertisement network (http://st.rol.ru/) are installed on the “parking page”.

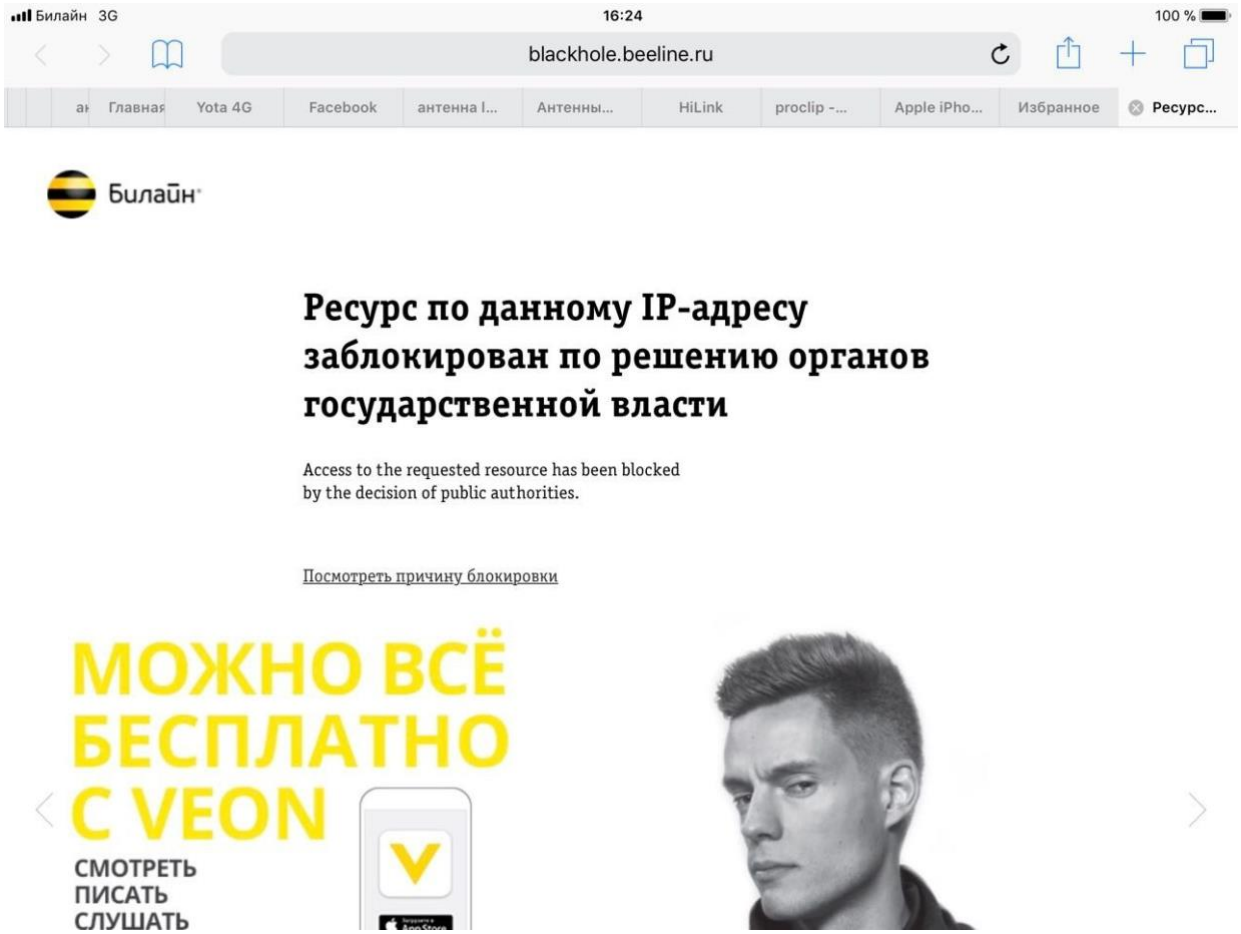
Translation:
The website located at this IP address was blocked upon the decision of government authorities.

Find out the reason of blocking



Translation:
The website located at this IP address was blocked upon the decision of government authorities.

Find out the reason of blocking



Translation:
The website located at this IP address was blocked upon the decision of government authorities.

Find out the reason of blocking.

Everything is possible for free with Veon. Watch, write, listen.

MEGAFON

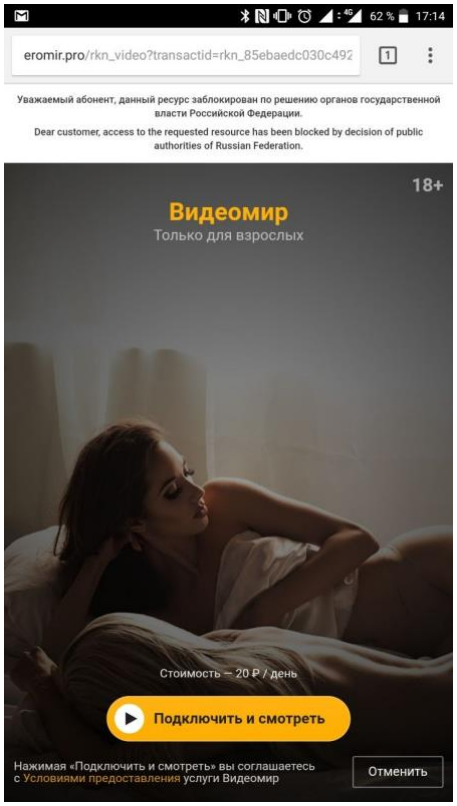
The addresses of “parking pages” are the following:

- https://lp.megafon.tv/rkn - when accessed from the third party network, the request is redirected to the website https://megafon.tv/. The Google tag-manager is installed on the page for the purpose of statistical data collection;
- http://eromir.pro/rkn_video or http://eromir.pro/rkn_foto - these pages are accessible from the third party networks. These pages contain ads of “18+ content” and paid services of *Megafon*.

The “parking page” does not contain any explanation of content blocking reasons or links to online services of verification of access restriction.

Translation:
Watch the package "18+" for 15 rubles per day.

Watch. You will be charged from the telephone number +...

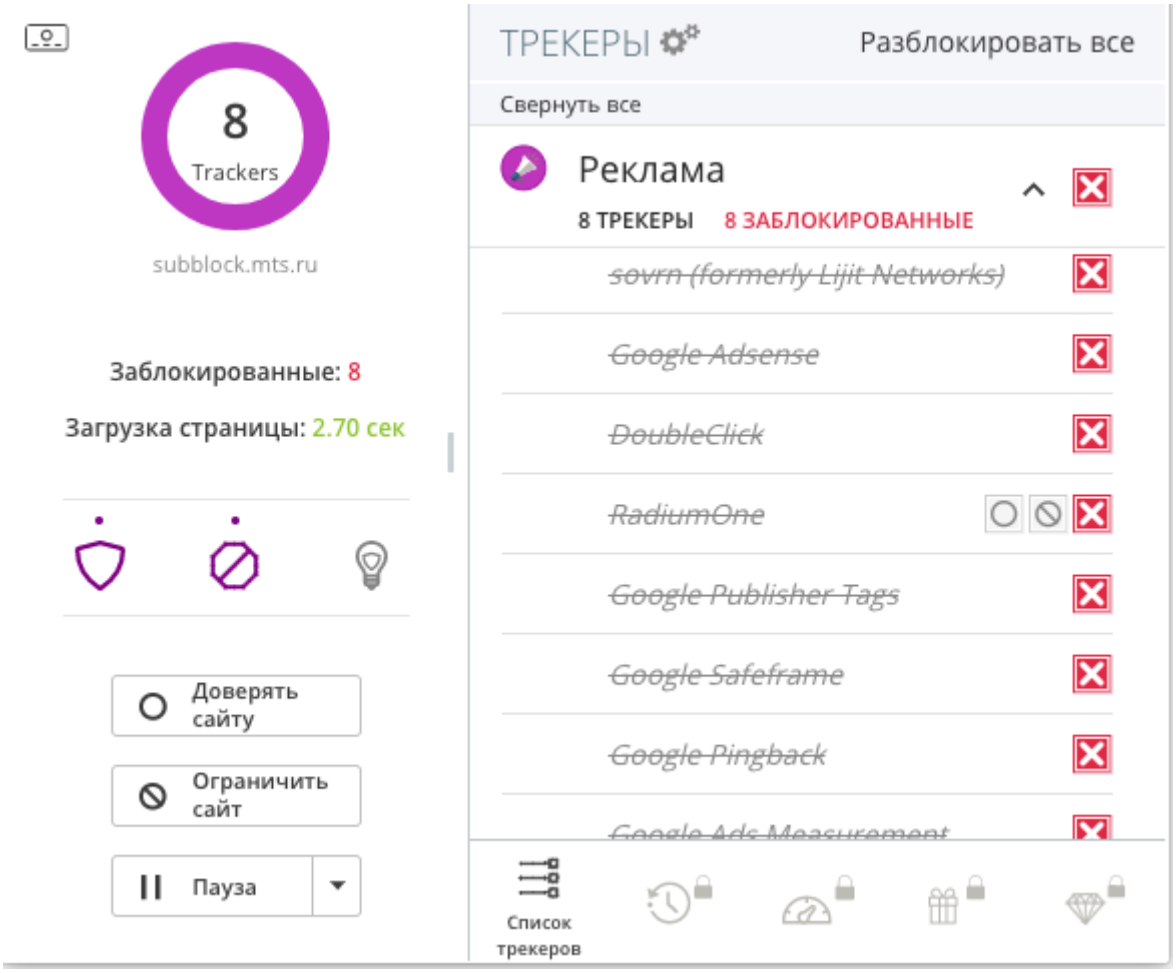


Translation:
Video World.
Only for adults.
Fee - 20 RU / day.

Subscribe and watch. By clicking "Subscribe and watch" you accept the Terms of service of Video World. Cancel. Photo World. Only for adults. Fee - 10 RU / day. Subscribe and watch. By clicking "Subscribe and watch" you accept the Terms of service of Photo World.

Cancel

The “parking page” is located at: http://blocked.mts.ru/ (unaccessible from third party networks). The *MTS* “parking page” contains the record number of various Internet analytics and advertising networks trackers:



Translation:
Left side:Blocked: 8. Time of a web page loading: 2.70 seconds. Trust this site. Block this site. Pause

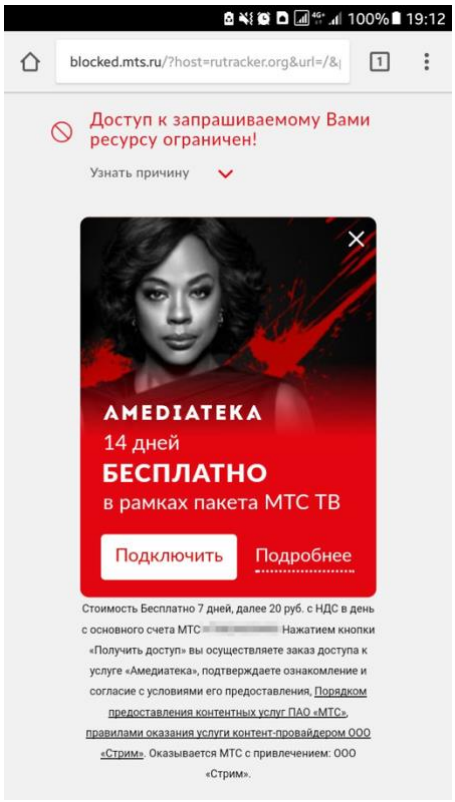
Right side: Trackers. Unblock all sites. Hide everything. Advertisement. 8 trackers, 8 blocked. The list of trackers

The advertisement displayed at “parking pages” originates from both own paid services of the company (mostly “18+ content”) and third party advertisers.

The reason of the website blocking may be discovered directly on the “parking page” without any need to visit other websites, but the respective notification is covered by “design features”, which make it not that obvious requiring a user to click the “down arrow” located near the button “Find out the reason”.

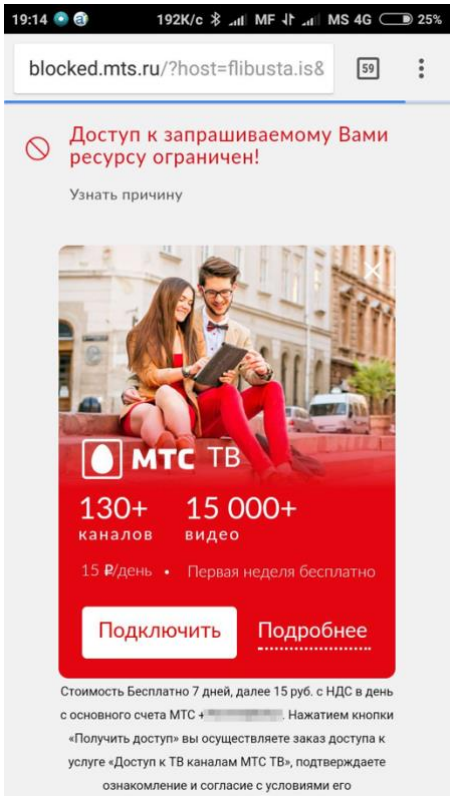
As a result, full information of reasons of blocking gets indicated (see the last screenshot):

- address of the blocked website;
- number and date of the decision on access restriction;
- government authorities which issued the blocking decision.



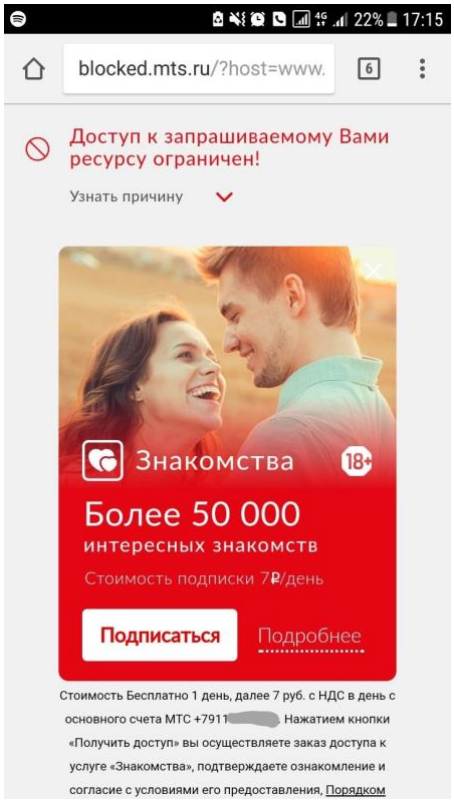
Translation:
Access to the website you are trying to reach is restricted.
Find out the reason.

Amediateka. 14 days. Free of charge within the package MTS TV. Subscribe. More details. Price Free of charge for 7 days, longer - 20 ru, including VAT, per day. which will be charged from the account of our mobile number +... By clicking "Get access" you make an order of access to the service of Mediateka, confirm that you reviewed and agreed with terms of service, Terms of content service provision by MTS, Rules of content service provider Strim. The services are rendered by MTS with assistance of Strim



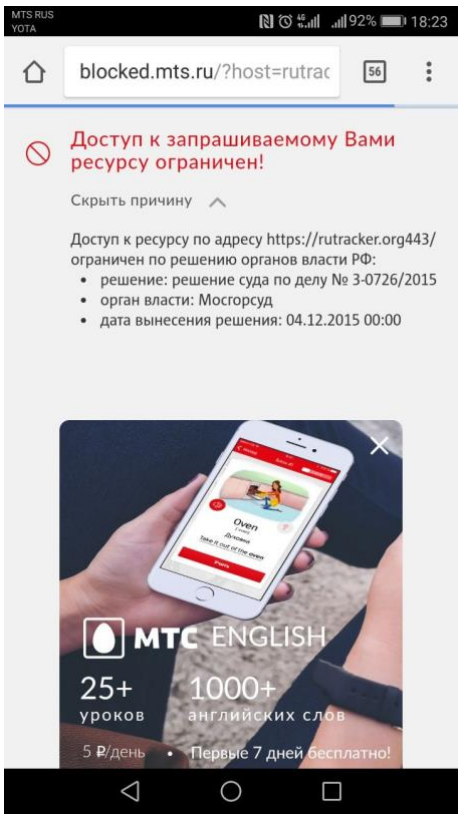
Translation:
Access to the website you requested is restricted.
Find out the reason.

MTS TV. 130+ channels 15 000+ videos. 15 Ru/day - First week for free. Subscribe. More details. Price: 7 days for free, longer - 15 Ru, including VAT, per day, which will be charged from your mobile number +.... By clicking "Get access" you order access to the service "Access to TV channels of MTS TV"



Translation:
Access to the website you requested is restricted.
Find out the reason.

Dating. Over 50 000 of interesting dates. Subscription price 7 Ru per day. Subscribe. More details. Price: 1 day for free, longer - 7 Ru, including VAT, per day, which will be charged from your mobile number +.... By clicking "Get access" you order access to the service "Dating"



Translation:
Access to the website you requested is restricted.
Hide the reason:

Access to the website https://rutracker.org443/ is restricted upon a decision of authority bodies of the Russian Federation:
- decision: court decision on case Np.3-0726/2015;
- authority body: Moscow city court;
- decision date: 04.12.2015.

MTS English. 25+ lessons 1000+ of English words. 5 Ru/day - First week for free

CONTACTS

ROSKOMSVOBODA

roskomsvoboda.org

ОЗИ

ОБЩЕСТВО ЗАЩИТЫ ИНТЕРНЕТА

ozi-ru.org