

research

VPN in Russia: from blocking services to blocking protocols

НАСТОЯЩИЙ МАТЕРИАЛ (ИНФОРМАЦИЯ) ПРОИЗВЕДЕН И (ИЛИ) РАСПРОСТРАНЕН ИНОСТРАННЫМ АГЕНТОМ «РОСКОМСВОБОДА» ЛИБО КАСАЕТСЯ ДЕЯТЕЛЬНОСТИ ИНОСТРАННОГО АГЕНТА «РОСКОМСВОБОДА». 18+

Роскомсвобода

October 2023

Introduction	3
Methodology	5
Part 1. Technology Overview	6
VPN	10
Protocols	14
Part 2. State of Censorship	16
Blocking Methods	19
Circumvention Tools Blockings	22
Conclusion	25

Introduction

Internet censorship in Russia is emerging daily. According to [Freedom on the Net reports](#), since 2011 Russia has steadily risen several positions per year in the Internet Freedom Index, where the maximum value (100) is the non-free Internet. This trend was ensured, on the one hand, with regular changes in legislation that created a regulatory framework for increased censorship, and on the other hand, with an increase in the number and variety of blocked resources.

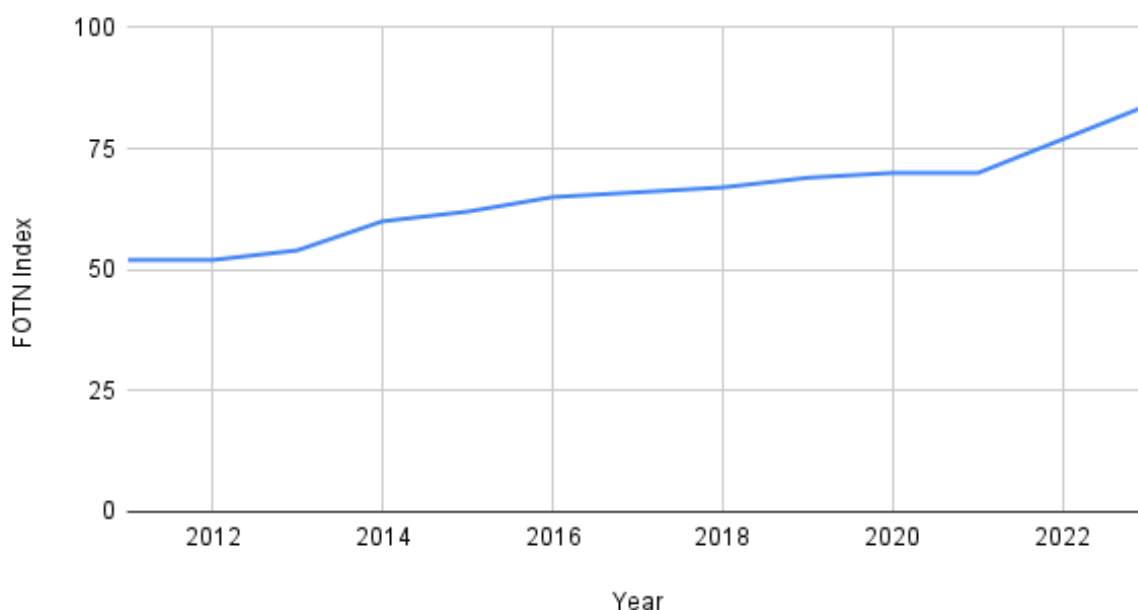


Chart: Russia FOTN index from 2011 to 2023.

Circumvention tools have been actively censored in Russia since 2017 when the [first legislation](#) prohibiting VPN services was created. This legislation was targeting specifically VPN services providing access to the content prohibited by Russian law. According to [Lumen's database](#), since 2017 Google has received more than 2,000 requests from Roskomnadzor related to the removal of links leading to the download of VPN services or information describing their usage. Some of these requests include thousands of individual URLs, so the total amount of content that Russian users couldn't access may exceed hundreds of thousands of resources.

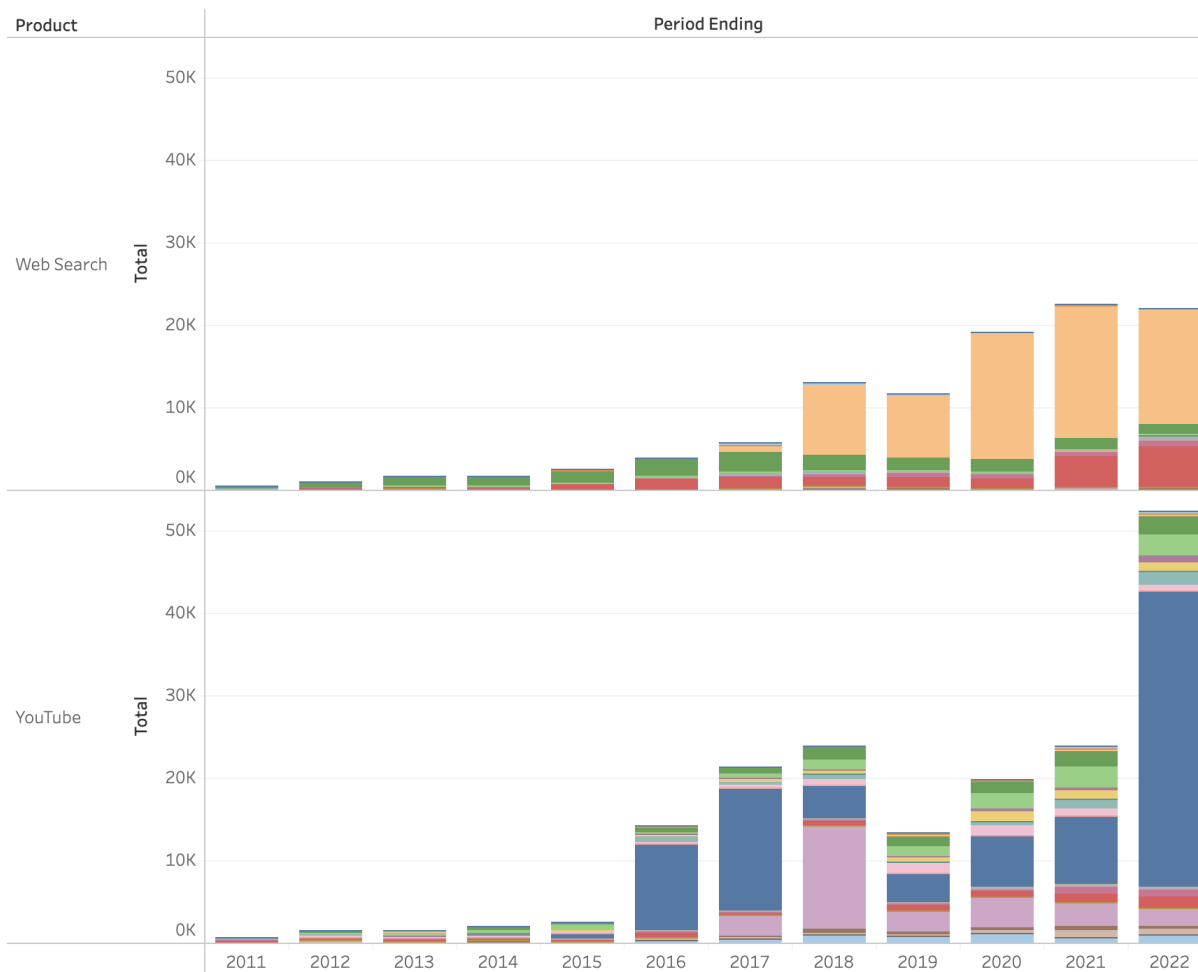


Chart: number of requests for content [removal](#) received by Google from Roskomnadzor from 2011 to 2022. Blue - the reason for the request is "national security", red - "privacy and security", orange - "copyright". The full [list of labels](#).

In 2023, the Ministry of Digital Development proposed a [new law](#) that should allow Roskomnadzor to purposefully block "information about methods of providing access to information resources and (or) information and telecommunications networks, access to which is restricted on the territory of the Russian Federation".

In this study, we tried to understand how Russian users circumvent censorship, which services are the most popular, how users react to the emerging blockings, and how internet censorship affects content consumption and access to information for people based in Russia.

Methodology

This research is based on open data sources, survey conducted by Roskomsvoboda, and short interviews with independent Russian media. Each of the sources has its limitations, but in this study we have tried to use diverse sources in answering all questions in order to be able to compare results and confirm hypotheses, or to highlight inconsistencies.

To determine the list of the most popular circumvention services in the region, we used data from Google Play, Apple Store, Google Trends, and Yandex Search. While the data from each individual source may be unrepresentative due to the limited audience and their dynamic nature (at different times on marketplaces, different applications may be top-ranked), the aggregate of data from all four sources and the survey can give us a general understanding of what services are most popular among Russians.

Based on a survey conducted by Roskomsvoboda (1900 respondents) and a survey conducted by MadBrains (1000 respondents), we tried to describe the most common circumvention tools' user journey in Russia. However, the sample of the Roskomsvoboda's survey was not representative – more than 40% of respondents mentioned that their work is related to IT. We do not know the demography and occupation of the MadBrains' survey respondents, so we cannot argue that the findings of both surveys are ground truth. In the description of the survey results, we provide data from different audiences based on Roskomsvoboda's survey, and show how the behaviour of people with more technical background differs from the average behaviour of less experienced users.

To determine content consumption trends and patterns, we relied on the survey results, on the results of Mediascope and BrandAnalytics research on media consumption in Russia, on the responses of Russian independent media regarding the changes in their traffic since the beginning of the war, and on Google Transparency Report data, which allowed us to look at the amount of traffic of Google Search and YouTube.

To determine the quality of access to VPN services and their effectiveness in bypassing Russian censorship, we used multiple sources: data from the search services (Google Trends, Yandex Search), data from Tor Metrics, data from Proton

Observatory, and data collected by the technology community in Russia through feedback on the effectiveness of circumvention tools in Russia. Each of the sources we used has its own limitations, but we think that by combining the information from these diverse sources allowed us to get an understanding of general context of the state of circumvention tools censorship in Russia.

In the context of websites blocking, in most cases we used data from the Open Observatory of Network Interference (OONI) to determine the accessibility of websites and services. OONI data has limitations on the number of websites tested, so for this study we updated the test lists to include the most popular circumvention tools.

This study is based on a diverse sources that provide an opportunity to analyse the context of the accessibility and usage of circumvention tools in Russia, but it cannot be considered exhaustive without the circumvention tools' own data that would show how specific services were affected by different types of censorship.

Part 1. Technology Overview

The demand for VPN services and other circumvention tools [increased dramatically](#) since the beginning of the war, reaching peak values by mid-March 2022. [According](#) to Atlas VPN, the number of downloads of various VPN services in Russia roughly tripled compared to 2021, from 12,585,576 downloads in 2021 to 33,540,600 downloads in 2022. In 2023, demand dropped sharply, with Russian users downloading VPNs only 3,366,919 times in the first half of 2023.

Similar trend is reflected in statistics of individual VPN services, for example, the number of Proton VPN downloads rose rapidly in March 2022, and by April it had already returned almost to its original values.

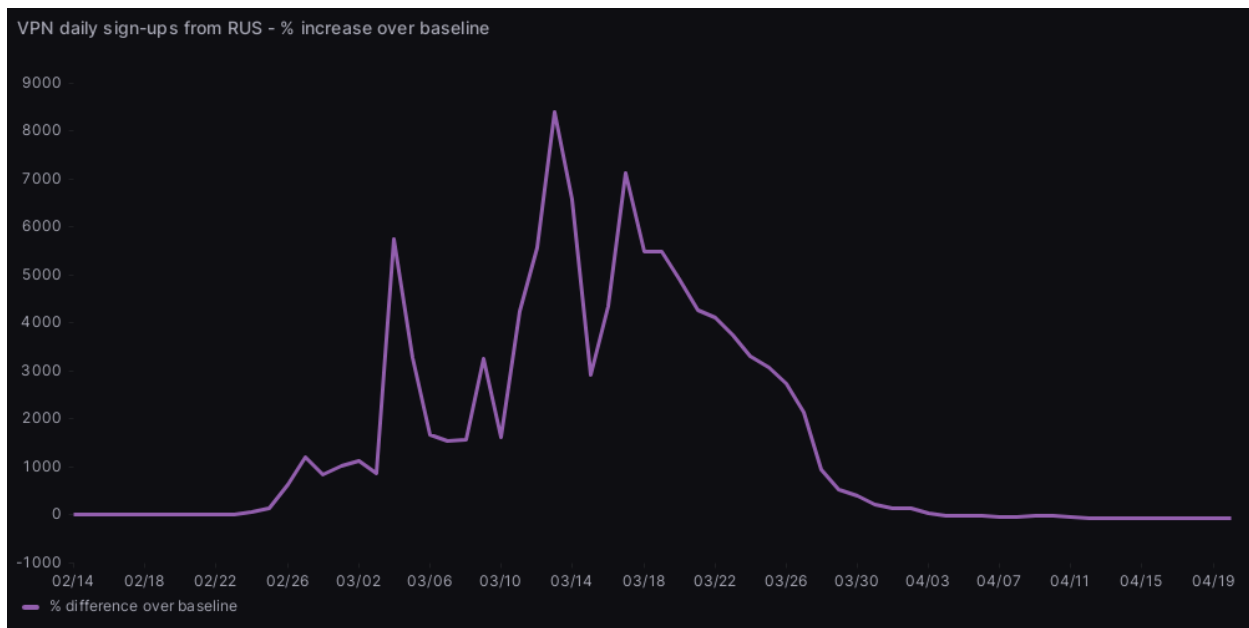


Chart: [Number of daily downloads](#) of Proton VPN application in Russia between 14th February 2022 to 19th April 2022

Since March, smaller peaks occurred in the periods between 29th May to 4th June 2022, and between 6th to 12th August 2023. These periods coincide with the dates of reported blocking of VPN services popular in Russia, for example, reports of blocking of Nord VPN and Proton VPN started on the [1st](#) and [2nd](#) June 2022, respectively.

The peak between 6th to 12th August also correlates [with time](#) when Wireguard and OpenVPN protocols were reported to be blocked in different Russian regions. Access to these protocols was restored on the 8th of August 2023.



Chart: Number of search queries on the topic of VPN services in Google Search from the 1st January 2022 to the 31st August 2023

Yandex Search data shows similar statistics, with the first peak in mid-March and the second in early June 2022.

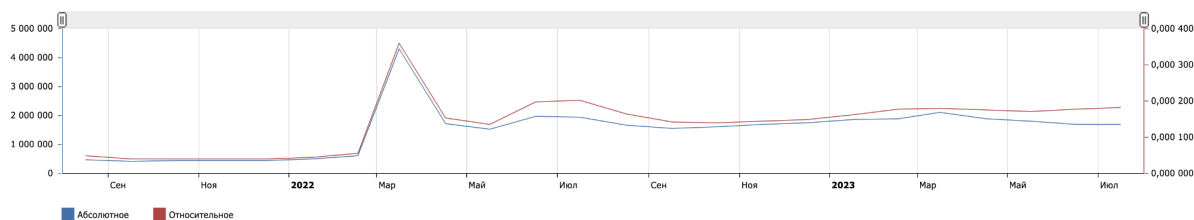


Chart: Number of search queries on the topic of VPN services in Yandex Search from the 1st January 2022 to the 30th July 2023

A similar trend can be seen for the search queries pertaining to Tor browser, with the number of queries peaking between 6th to 12th March, and followed by peaks between 29th May to 4th June and between 25th June to 1st July 2023.



Chart: Number of search queries on the topic of Tor in Google Search from the 1st January 2022 to the 31st August 2023

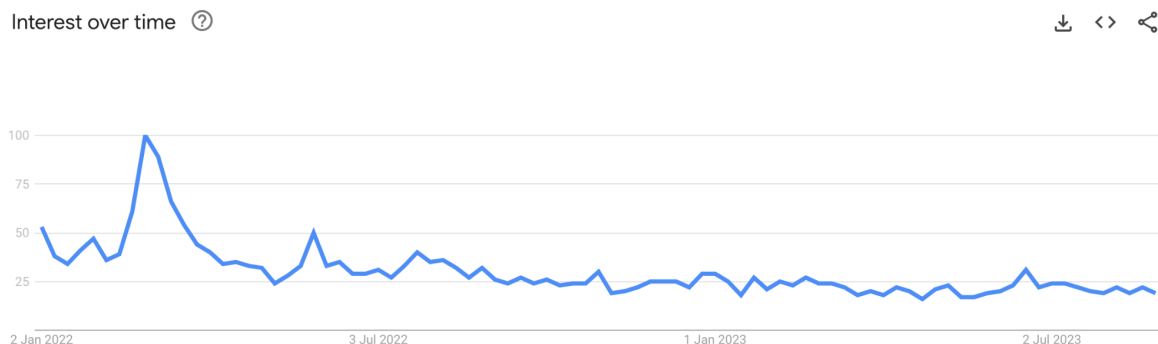


Chart: Number of search queries on the topic of Tor browser in Google Search from the 1st January 2022 to the 31st August 2023

Tor metrics also confirm [several peaks](#) in connections over the past two years. In December 2021, the number of Tor network users in Russia dropped sharply due to the blocking of Tor on 8th December 2021.

The number of connections to the network continued to fall until March 2022, when there was a peak of connections due to mass blocking of various sites and services.

After March, the next peak is in September 2022, most likely it is connected on the one hand with the [unblocking of the Tor](#) website in Russia, on the other hand with the beginning of partial mobilisation. The last peak in the number of connecting users occurred in August 2023, most likely it is related to the blocking of VPN services in early August.

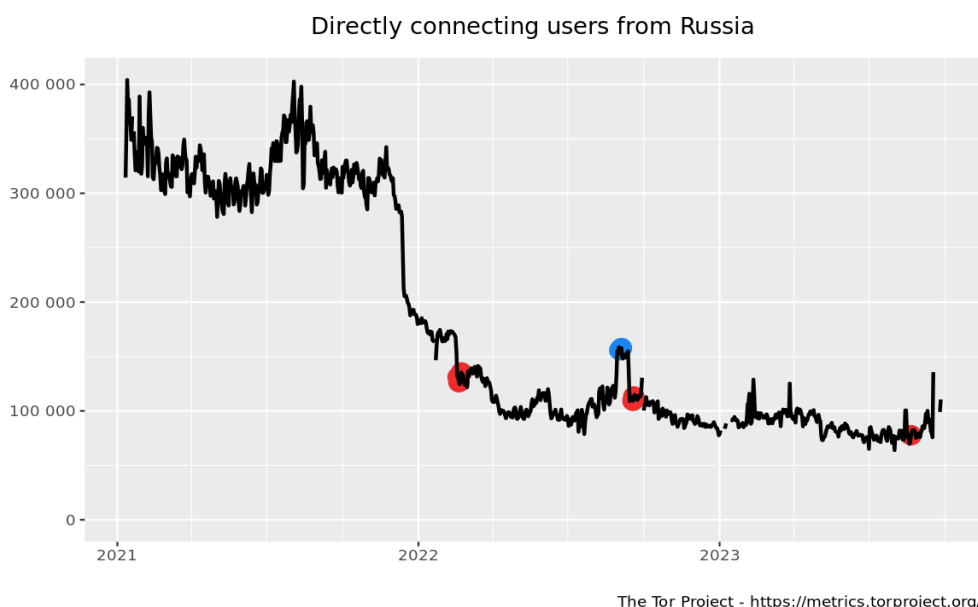


Chart: Statistics of user connections to the Tor network from Russia from 2021 to the end of September 2023.

It is important to note that Tor services are about 10 times less popular than VPN services in Russia. While people search for VPN tools approximately 2.1 million times per month, only 200 thousand searches are related to Tor services (Yandex Wordstat).

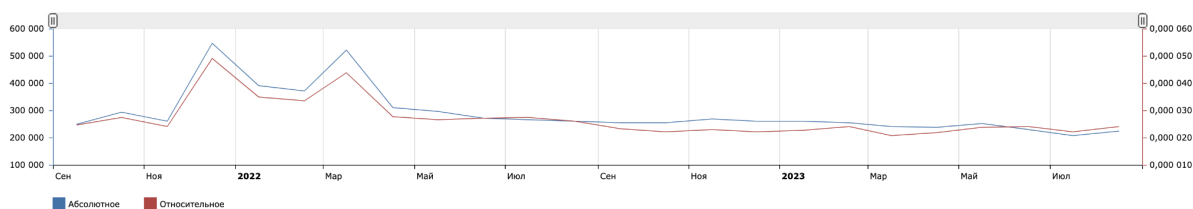


Chart: Number of queries related to Tor in Yandex Search from the end of 2021 to 31st August 2023. At the same time, among the users surveyed by Roskomsvoboda, Tor services (Tor Browser, Orbot) were the most popular among other circumvention tools, and

slightly less than half of the respondents mentioned that they had used Tor services at least once in the past year.

In addition to VPN services and Tor services, we included several tools that help to bypass censorship but are not classic VPNs, e.g. Lantern and AntiZapret, and also briefly described how media outlets help users to access their content without using circumvention tools.

VPN

The most popular VPN-services in Russia can be considered:



AdGuard VPN



Express VPN



Proton VPN



Turbo VPN



VPN Planet



VPN Proxy Speed



VPN Master

These services are at the top of Google Play and AppStore applications, and have the biggest number of related queries to Google Search and Yandex Search services, and are the leaders in the number of downloads in the country.

Less popular services can be considered Hola VPN, Nord VPN, Secure VPN, Tomato VPN, VPN - fast, secure, no limits, VPN Super Unlimited Proxy - these are services popular among users of at least one of the search engines and one of the marketplaces.

From the 13 most popular VPNs in Russia, 9 are present in the [VPN Overview ranking](#), and only 4 of these 9 are considered safe and effective enough (AdGuard VPN,





Express VPN, Proton VPN, Nord VPN). Among the four VPNs which are not included in the VPN Overview ranking, some don't even have a website where you could find information about the service, for example the 'VPN Proxy Speed - Super VPN' website on Google Play - <https://www.supershell.me/>, results in a blank page. 'VPN - fast, secure, no limits' has no website link at all and the only documents available are [Privacy Policy](#) and [Terms of Service](#).












Thus, we can say that out of the 13 most popular VPN services in marketplaces and search engines, only 4 can be considered conditionally safe, and only three of these four services have passed a formal external audit: Express VPN, Proton VPN, Nord VPN.

According to the results of the survey conducted by Roskomsvoboda, the most popular services mentioned by the respondents were AdGuard VPN, Proton VPN, Express VPN, Amnezia VPN, Planet VPN, Lantern VPN, Psiphon VPN, Outline VPN, Turbo VPN.

This list partially coincides with the statistics of the search queries and app downloads, the differences between the statistics of search queries and the survey results may be due to the limitations of the audience that was surveyed.

Based on the most popular services in terms of the number of search queries and app downloads, and on the results of the Roskomsvoboda's survey, we have compiled the following list of 15 popular services, which we further used for analysis:

- 1  AdGuard VPN
- 2  Express VPN
- 3  Proton VPN
- 4  Turbo VPN

- 5  VPN Planet
- 6  VPN Proxy Master
- 7  Amnezia VPN
- 8  Lantern VPN
- 9  Psiphon VPN
- 10  Outline VPN
- 11  Secure VPN
- 12  Nord VPN
- 13  RedShield
- 14  Hola VPN
- 15  AntiZapret

In order to determine the availability of basic information about these 15 services, we checked the accessibility of the websites of these services in Russia.

According to OONI data, domains of 8 of the 15 most popular services are being blocked in Russia.

AdGuard VPN, AntiZapret, Hola, NordVPN, Psiphon, RedShield, TurboVPN and VPN Proxy Master are either completely inaccessible for Russian users or are available only on certain networks.

Web Connectivity Test

Russia

OK Confirmed Anomaly Failure

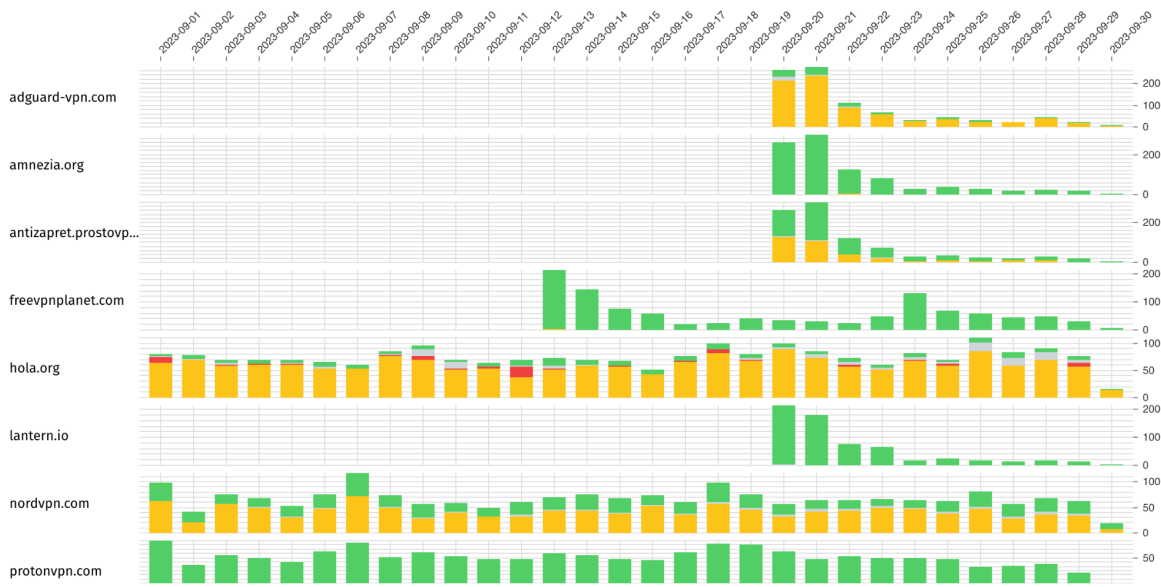


Chart: [OONI measurements](#) collected on the territory of the Russian Federation from 1st September 2023 to 30th September 2023

Web Connectivity Test

Russia

OK Confirmed Anomaly Failure

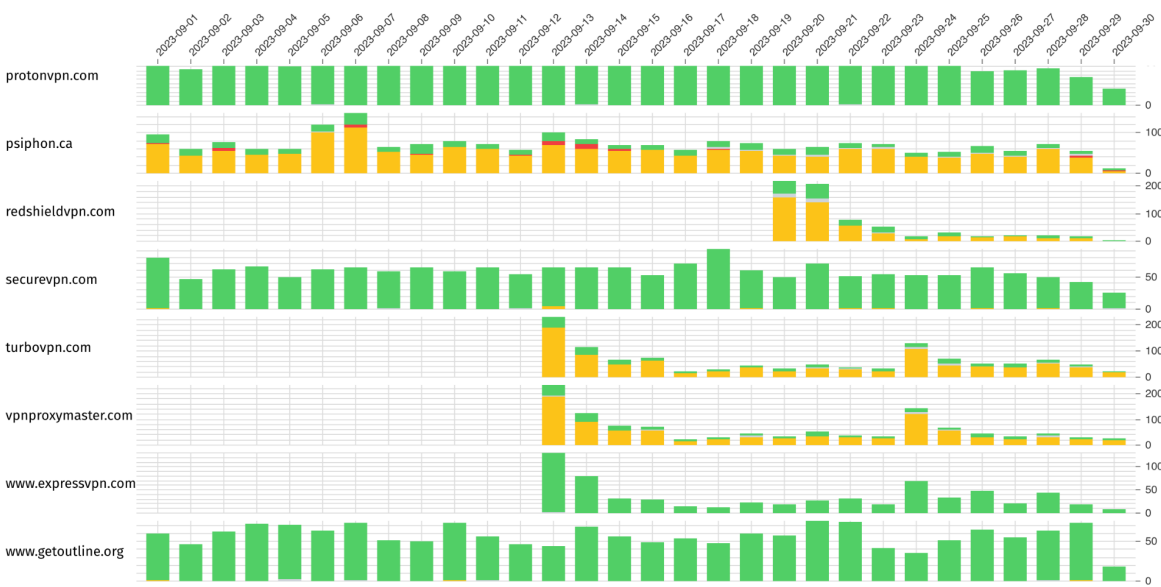


Chart: [OONI measurements](#) collected on the territory of the Russian Federation from 1st September 2023 to 30th September 2023

Thus, despite the popularity of these services, the number of their users may be affected by the blockings and possibly redistributed among other services that have not yet been blocked.

For new users who do not yet use circumvention tools, it may be more difficult to find information about the services whose websites are already blocked in Russia.

Roskomsvoboda has its own [VPN Love](#) rating, compiled by infosecurity experts and digital advocates.

This is a list of reliable vpn services that meet the requirements of security, anonymity and have a low cost. Experts monitor the market of vpn-services, analyze their characteristics, security policies, track incidents, analyze the reputation of founders. The function of secure payment for blocking circumvention services from Russian cards and cryptocurrency on [VPNPay](#) is implemented.

Protocols

The main protocols used by the 15 services we highlighted in the previous article are:

- OpenVPN,
- Wireguard,
- Shadowsocks,
- IKEv2,
- V2Ray.

Four of the 15 services use only OpenVPN protocol or their own protocol based on OpenVPN, two more services use Wireguard in addition to OpenVPN. Only two services out of fifteen use the Shadowsocks protocol: Amnezia VPN and Outline VPN.

OpenVPN is considered one of the most vulnerable protocols to blocking. In a 2022 study, CensoredPlanet was able to identify 85% of traffic going through OpenVPN as part of the research experiment.¹

This protocol is [also favoured](#) by Russian banks and commercial companies using VPNs.

Only six of the fifteen services have a built-in obfuscator. ExpressVPN offers Camouflage developed by Surfshark, Proton VPN offers their own obfuscator (Proton VPN Stealth), Nord VPN uses an obfuscator developed by Tor (obfsproxy), Amnezia offers cloak.

In the same Censored Planet study, researchers demonstrated that one of the most popular obfuscators, the [XOR](#) patch, is also easily identified and was detected in 70% of the cases. The same results were achieved for obfuscation with TLS, SSL, obfs2/3, TCP obfuscation.

Only five services offer inbuilt anonymity tools: AdGuard VPN offers SOCKS5 proxy, Nord VPN and AntiZapret offer Onion proxies, Nord VPN and RedShield offer an option to connect via Double VPN.

Thus, when the OpenVPN and Wireguard protocols started to be [targeted by censors](#) in August 2023, at least 6 out of 15 services started experiencing network access problems. Depending on the efficiency of obfuscation of the remaining services and user awareness of the existence of such a setting, users of at least three more services (Express VPN, Nord VPN, Proton VPN) may have experienced problems with access to the Internet.

For example, OONI data shows that blocking in August 2023 affected Psiphon, which uses the L2TP/IPsec and Shadowsocks protocols, but the service remained available to most users. The same thing happened during the mid-September blocking wave.

¹ Xue, Diwen, Reethika Ramesh, Arham Jain, Michalis Kallitsis, J Alex Halderman, Jedidiah R Crandall, and Roya Ensafi. 'OpenVPN Is Open to VPN Fingerprinting', n.d.

Psiphon Test

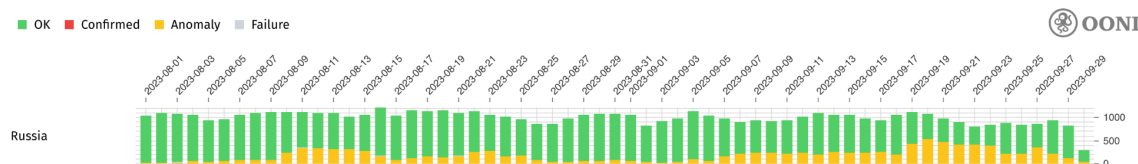


Chart: [OONI measurements](#) pertaining to Psiphon VPN between 1st August to 30th September 2023

In October 2023, Amnezia VPN [announced its AmneziaWG](#) protocol, designed for countries with strict censorship.

This is a fork based on the standard WireGuard, which adds garbage and randoms to the packets to prevent DPI systems from blocking WireGuard habitually. In this way it is possible to achieve high speeds like WireGuard, but be protected from protocol blocking.

Part 2. State of Censorship

Internet censorship in Russia in 2023 has taken [unprecedented scale](#). In the middle of 2023, Roskomnadzor reported an 85% increase in the number of blockings compared to 2022. At the same time, in 2022, most independent media websites were already blocked, mirrors of independent media, human rights projects websites and political organizations websites were actively blocked. [According to OONI](#), censorship in Russia has affected virtually all types of content - from commercial businesses to environmental and educational projects.

Along with the volume of censorship, the procedure required to block different services has also changed. Since 2022 more governmental entities acquired the legal force to request blocking of resources without court orders: for example, in 2022, the Prosecutor General's Office was given the opportunity to include resources into Roskomnadzor's registry without a court decision.

In 2022 only, 34 thousand resources were included in the registry "anonymously" without specifying the governmental entity responsible for blocking.

Before 2022, there were approximately three hundred anonymous blocking decisions in the last 10 years. None of the resources which were added "anonymously" were unblocked.

Roskomsvoboda continues to track the number of resources blocked as part of military censorship, this number exceeds 15 thousand at the moment of the publication.

Entity	01.2022 — 09.2023		11.2012 — 09.2023		Actual stat on 09.2023
	Blocked	Unblocked	Blocked	Unblocked	Blocked now
Genprokuratura	21 569	1156	174 199	105 250	68 949
State body not specified (presumably the Prosecutor General's Office)	34 028	295	34352	295	34 057
MIA (Ministry of Internal Affairs)	16 074	29 647	81 967	62 516	19 451
Ministry of Communication	17 479	1	49 028	11	49 107
Ministry of Digital Development	3 663	0	5 779	0	5 779
Ministry of Justice	6	0	6	0	6
Moscow City Court	27 455	33 430	211 226	153 028	58 198
Rosalkoregulirovanie	2 032	2 998	15 427	12 188	3 239
Roszhdravnadzor	5 564	7 120	24 209	13 909	10 300
Roskomnadzor	23 738	9 319	93 732	49 485	42 297
Rosmolodezh	266	255	769	375	394
Rospotrebnadzor	966	555	6 270	4 810	1 460
Rosselkhoznadzor	22	84	106	84	22
Federal Tax Service	50 420	176 830	429 277	265 126	164 151
Federal Drug Control Service	173	154	27 592	27 127	465
Central Election Commission (CEC)	1	0	1	0	1
Court	28 238	155 021	365 048	306 335	58 713
TOTAL	231 694	416 865	1 518 988	1 000 539	516 589

Table: Number of blocked and unblocked websites from the beginning of 2022 to the end of September 2023 according to [Roskomsvoboda registry](#)

In 2022, a number of legislative projects were adopted to expand the capacity of Roskomnadzor to implement the blockings, to expand the number of content categories to be censored, and to strengthen the responsibility of ISPs (Internet Service Providers) for the successful implementation of censorship.

Thus, the Ministry of Internal Affairs [developed](#) a mechanism for blocking websites containing personal data of people under state protection. Roskomnadzor was recognized as an entity responsible for adding such websites to the registry of banned websites, Roskomnadzor now is obliged to make a corresponding entry to the registry within 24 hours of receiving a decision to ban the information and an order to restrict access to it.

In March 2022, a law on penalties of up to 15 years of imprisonment for publishing fake news about the Russian army came into force. Courts are now beginning to hand down the first sentences with real terms of more than 5 years in prison.

In July 2022, Putin [signed](#) a law that introduces fines for Telecom Operators who fail to install TSPU on their networks. The authorities explain the need to use this equipment by the presence of "information threats to Russian citizens."

In August 2022, the Ministry of Digital Development [published](#) documents where it proposed to give Roskomnadzor the authority to block mirrors of previously blocked websites. The resolution came into force on March 1, 2023 and will be valid for 6 years.

In December 2022, the law [banning](#) LGBT propaganda came into force. Now this type of content [should be included](#) in the registry of banned content by decision of Roskomnadzor. The website "Nuntiare et Recreare", dedicated to LGBT believers of different confessions, and the website of the Museum of LGBT History in Russia were blocked.

In September 2023, the Ministry of Digital Development [published](#) for public discussion a draft decree of the Cabinet of Ministers, which covers Roskomnadzor's efforts to maintain a registry of banned information. This decree also expands the capacity of Roskomnadzor to [block](#) "information on ways, methods of providing access to information resources and (or) information and telecommunication networks, access to which is restricted on the territory of the Russian Federation."

From March 2024 onwards, marketplaces working in Russia will have [to remove](#) VPN services applications from their stores at the request of Roskomnadzor. Next year, it may start blocking VPN services that provide access to websites blocked in Russia. First of all, the blocking will affect services hosted in the applications marketplaces.

Earlier, in July 2023, Law No. 406-FZ was signed. The law prohibits advertising of circumvention tools, and criteria for blocking information about circumventing tools, namely:

- Presence of a description of actions that allow users to access blocked resources;
- Presence of information that gives an idea of how to access blocked resources;
- Presence of information aimed at convincing users of the effectiveness of circumvention tools;
- Information that substantiates the merits of circumvention tools, and that gives a positive evaluation or endorsement of circumvention tools;
- Offers to purchase access to circumvention tools;
- Presence of information that provides the capacity to access blocked resources

Restrictions will [not apply](#) to scientific, and statistical information on circumvention tools and methods.

Blocking Methods

When considering the topic of blocking tools, you need to understand the types of website and media blocking. The technical implementation of censorship in Russia has long been highly decentralized: each provider was responsible for implementing blocking on its networks, and could use [any blocking methods](#). As a result, the data collected by network measurement projects [shows](#) the same resources are blocked in different ways on different networks, and sometimes even within the same network different blocking methods can be used.

Such methods could include^{2 3}:

- Unencrypted data packages filtering by key words
- HTTP packet filtering in outgoing and incoming requests and responses
- TCP/IP blocking with terminating sessions with all unwanted hosts or returning a block page
- DNS tampering resulting in returning false domain names or redirecting to a block page
- SNI-filtering of encrypted traffic with subsequent interference in TLS handshake (connection reset, RST packet enabling, session time out)

After the adoption of Law 90-FZ (on the "Sovereign Runet") in 2019, all Russian operators had to install TSPU, the Russian version of DPI (Deep Packet Inspection). In 2021, the [first known case](#) of using TSPU occurred when Twitter was slowed down (trotted) on many networks at the same time. In contrast to previous inconsistent blocking, the trotting was implemented at the same time on different networks by different providers; later Roskomnadzor [confirmed](#) that the blocking was implemented with the help of TSPU.

At the same time, in 2021 it was known that the devices were not installed by all providers on all networks, and a lot of collateral damage was done during the Twitter trotting. Users reported problems with access to government websites, the Russian Post and other services. The [research](#) from 2022 discovered more than 6,000 devices on more than 650 networks.

In the same study, the authors sought to understand what types of traffic TSPU can detect and what types of traffic trigger its activity. Through a series of experiments, the researchers determined that TSPU responds to different types of traffic, both SNI-based, IP-based, and QUIC. TSPU blocks only connection attempts coming from the territory of the Russian Federation, and monitors mainly connections to information resources: blogs, news media, social networks. Despite the fact that some resources are already included in Roskomnadzor's registry, TSPU still continues to monitor connections to these resources.

² Xynou, Maria, and Arturo Filastò 2022-03-07. 'New Blocks Emerge in Russia amid War in Ukraine: An OONI Network Measurement Analysis', 7 March 2022.

<https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/>.

³ D. Xue, R. Ramesh, ValdikSS, L. Evdokimov, A. Viktorov, A. Jain, E. Wustrow, S. Basso, and R. Ensafi. Throttling twitter: An emerging censorship technique in russia. In Proceedings of the 21st ACM Internet Measurement Conference, IMC '21, page 435–443, New York, NY, USA, 2021. Association for Computing Machinery.

TSPU-based blockings can still be circumvented, and the authors of the publication propose several different solutions. However, at this stage it is not entirely clear how exactly TSPU blocking methods will develop further, while the speed of implementation of the entire system and the scale of its impact makes us assume pessimistic scenarios. For comparison, it took decades to build Great Firewall in China, while the implementation of TSPU took less than three years since the adoption of the 90-FZ law.

It is important to note that blocking of the websites and services can have great collateral damage not only in regards to the access to information, but also for the work of independent media in general. Some media outlets have noted that the work of their reporters directly depends on the accessibility of the media's website, as many interviewees refuse to communicate with journalists if they see that the resource is blocked.

On the other hand, blocking media websites leads to their inability to accept donations from Russia, so many media outlets have started using separate crowdfunding platforms which are still available in Russia. Unfortunately, the accessibility of crowdfunding platforms does not guarantee their availability for independent media, for example, the Boosty platform [reported](#) the closure and "lifetime blocking" of Novaya Gazeta's account. Many platforms used by media and bloggers to create content were also censored. For example, the website builder Tilda [blocked](#) and then completely removed the DOXA website from their platform in March 2022, and Mave, the platform for podcast creators, [blocked](#) access to the "To Be Continued" project in October 2023. Thus, censorship affects not only the accessibility of the existing content, but also the production of new material, limiting the ability of projects to collect donations and restricting access to the services that projects use to create content.

It is important to note that in addition to the circumvention tools, there are other ways to access blocked content. For example, many media outlets are redistributing content across different platforms that are not yet blocked in Russia: Telegram, YouTube. Also, many independent media continue to release mirrors and create automated systems for their publication, thus far outpacing Roskomnadzor's efforts to automatically block new mirrors. Most of the interviewed media noted that the speed of mirrors blocking has varied over the past two years depending on the general context. For example, at the time of the campaign of PMC Wagner, the speed of blocking for the new mirrors for the largest media outlets could reach 1.5 minutes.

Circumvention Tools Blockings

VPN services in Russia have been blocked on a different scale since 2017, when the [law](#) banning the use of VPN services and anonymizers came into force. In 2019, Roskomnadzor requested VPN services operating in Russia to connect to the Federal State Information System (FGIS), the [requests](#) to connect were sent to Nord VPN, Hola! VPN, and ExpressVPN. [In June](#) 2021 VyprVPN and Opera VPN were blocked, [in September](#) 2021 Hola! VPN, ExpressVPN, KeepSolid VPN Unlimited, Nord VPN, Speedify VPN and IPVanish VPN were blocked.

In 2021, the first reports of protocol-level censorship appeared. For example, in September, [Rostelecom](#) and [Beeline mobile](#) networks users were reporting problems with the connection through the Wireguard protocol. It seems that this was an attempt to implement blocking using the TSPU, but it was not very successful, as individual users reported collateral damage, [including blocking](#) of one of the biggest Russian marketplace, Avito, Twitch and some other streaming services.

In May 2022, Windscribe users [reported](#) problems with the service, in June 2022, users of Proton VPN and NordVPN started reporting problems with access to their services. Roskomnadzor later [confirmed](#) that it had restricted access to Proton VPN, and according to some [media reports](#), it was also planned to restrict access to Proxy Master VPN, Browsec VPN, vpn-super unlimited proxy, Melon VPN, Windscribe VPN, and RedCat secure unlimited VPN. In 2022, there have been attempts to block services using TSPUs, through blocking domains and IP addresses associated with VPN services. For example, in the [case of Proton](#), the API host `api.protonvpn.ch` was blocked, and in the case of Windscribe, the IP addresses of the service's servers were blocked. At the same time, users also reported blocking of some protocols: in the regions of western Siberia and southern Russia IPsec and IKEv2 protocols were [unavailable](#) on corporate networks.

In January 2023 new reports of access problems while connecting through IKEv2 and OpenVPN protocols appeared. On January 23rd the Telegram channel [Tech Talk](#) reported that in the eastern regions of Russia (Altai, Biysk, Omsk, Novosibirsk and others) IKEv2 and OpenVPN protocols were blocked, while IP addresses of VPN servers remained available. On February 1st, this wave of blocking scaled to other regions, including: Perm, Orsk, Novocheboksarsk, Togliatti, Yakutsk, Kazan, Elabuga, Ufa, Cheboksary, and Nizhny Novgorod.

The next protocol blocking attempt was [launched](#) on May 30th 2023 with partial blocking of OpenVPN, IKEv2 and IPSec protocols. At that time the blocking was reported by users of MTS (mobile networks Moscow, landline Chelyabinsk), Beeline (landline and mobile networks in Moscow, Kazan, Krasnodar, Novosibirsk), Megafon, MirTelecom, Yota, Tele2, Tatttelecom, Wifire (Netbynet), Dom.Ru and other providers. Within a day this wave of blocking ended, and in the evening of May 31 all services became available again.

At the beginning of August 2023, users started reporting access problems while using OpenVPN and Wireguard protocols again. Both protocols, as we wrote above, are very popular and are used by many VPN services to establish a connection. Planet VPN also reported IKEv2 blocking, some users reported IPSec blocking.

The scale of the blockings covered a significant number of regions, the project "Na Svyazi" mapped the messages they received during the wave of blocking in August. Unfortunately, we have no reliable information on how much blocking occurred in each region and how it affected local VPN services users. The maps below are based on reports from individual users and cannot be considered representative, but we provide them to illustrate the potential scale of the blockings.

One of the members of the ntc.party forum, the author of GoodbyeDPI, ran some tests to understand what exactly happens when there is an attempt to connect through one of the protocols and discovered the following:

"For all VPN protocols except L2TP, protocol discovery is performed first, followed by protocol "verification" (response checking or monitoring multiple packets in a TCP/UDP session), followed by session termination (TCP) or blocking traffic from passing through the srcip-srcport-dstip-dstport (UDP) bundle.

Tele2 mobile networks in Saint Petersburg:

- L2TP (UDP 1701, no IPsec): L2TP Control Message packets (the very first packets of the session) do not reach the server on port 1701
- IPsec (UDP 500/4500): UDP packets are blocked after several packets are transmitted during session establishment.
- PPTP (TCP 1723): TCP connection is broken after server sends Start-Control-Connection-Reply response to the first packet in Start-Control-Connection-Request session, does not reach GRE tunnel establishment.

- OpenVPN UDP: UDP packets are blocked after several transmitted DATA packets after session setup
- OpenVPN TCP: TCP connection is dropped after a few DATA packets are transmitted after session setup
- WireGuard: UDP packets are blocked after 5 received Transport Data packets from the server.

Landline MTS Kuzbass:

- Only OpenVPN UDP/TCP, L2TP, WireGuard are blocked, but not PPTP and IPsec
- L2TP delivers packets to the server, but server responses are blocked
- WireGuard: UDP packets are blocked after the first Transport Data packet from the server.

These blockings are different from those used for commercial VPN services (like ProtonVPN, Windscribe): they are filtered from the very first packet, not allowing the session to establish itself."

On the evening of August 8th, the availability of all services was restored. Many VPNs promised to consider using other protocols and find ways to connect despite the blockings.

On September 29th, the project "Na Svyazi" started receiving new reports of blocking, this time users mostly reported the issues with the Wireguard protocol. The scale of the blocking was much smaller this time, and according to the Agency's information, affected mainly the central part of Russia, but covered users of both large and regional providers: MTS, Beeline, Megafon, Tele2, Yota, Tritec, Skynet, Akado, R-Telecom.

The only major protocol that has not yet been blocked on a large scale is Shadowsocks, which is harder to detect by design, but there is no guarantee that services using Shadowsocks will not be affected with the next wave of blockings. Obfuscation services are also not blocked yet, but as we mentioned above, some of the obfuscation services do not work efficiently and can also be detected by DPI.

Since blocking by means of the TSPU is not always carried out by court order or through the Roskomnadzor registry, some services have been able to file a lawsuit against Roskomnadzor demanding that the blocking be lifted. It is still unknown how this [litigation process](#) will end, but this case may become a good precedent in Russian legal practice.

Conclusion

Censorship in Russia is steadily growing every year, both in terms of the number and diversity of blocked services. While earlier blockings were often inconsistent and the same resources could be blocked in different ways by different providers on different networks, in 2021 Russia for the first time used TCSPs for blocking. In 2022, researchers showed that DPI devices can be used to relatively easily detect connections made using one of the most common OpenVPN protocols even when obfuscation is used. In 2023, we see TSPU being used in Russia to block individual VPN protocols, and how these blockings can occur in a coordinated manner, at the same time across different providers and networks in different regions. This speed of development of blocking mechanisms together with the new legislation makes us fear of attempts to completely block existing VPN services in the Russian Federation.

Despite the fact that most Russian users are aware of the existence of Internet censorship and blockings, and are active VPN users, many of them are not sufficiently aware of how exactly circumvention tools work. Such ignorance on the one hand leads to the fact that people choose unreliable, or even fishy, services preferring cheaper or free applications. And on the other hand, in case of blocking of certain protocols they do not have enough knowledge and skills to customize the used service and bypass the blocking.

Censorship in Russia is implemented not only at the network level, but also at the level of individual services, including social networks and search platforms. Such censorship is much more difficult to track, and we have to rely heavily on transparency reports from individual services. The sources that we were able to find and analyze in the framework of this research show that even though services such as YouTube and Google are available, we cannot claim that their users have full access to independent sources of information through these platforms.

As part of this research, we have identified several gaps, to which we would like to draw the attention of the human rights, technology and research communities.

First of all, this is a study of how TSPU's work - at the moment there are only a few academic studies published on how many Russian TSPU's are currently installed and how they filter Russian users' traffic. Since TSPU's are a key element of Russian censorship that allows it to be strengthened through centralization, we believe that the technology and research community needs to collaborate more to study this topic.

The second topic we would like to outline is user awareness of the mechanisms of VPN services and obfuscation, as well as the dangers of using unaudited and unverified services. The current user strategy of scouring VPN services in search of a working application can be a major vulnerability when blocking major popular protocols.

We will continue to monitor the availability of VPN services and protocols, analyze the situation and keep you informed [on the site](#), [in Telegram](#) and update the [VPN-Love rating](#).