RKS Global

Witness RC

August 2026 · rks.global

VPNs in Russia: User Adaptation to Censorship

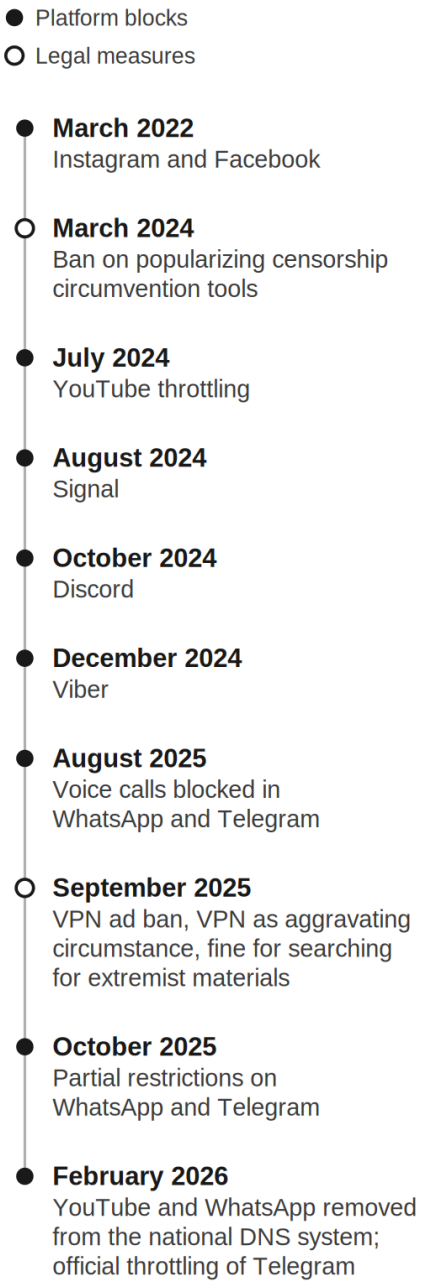
This study examines how users adapt to internet censorship and their experience of using VPNs: how they choose a VPN, what difficulties they encounter while using it, and how they view blocking policy in Russia in general and their own cybersecurity in particular.

The study draws on three focus groups (two made up of ordinary users, one of civic activists), an expert interview with the head of support at Amnezia VPN, and participant observation. The sample of 16 people comprises informants balanced across the age cohorts 18–24, 25–34, 35–45, and 46+, from Moscow, the Moscow region, Yekaterinburg, and Rostov-on-Don.

Context

Over the past 15 years, Russia has shown a rapid decline in the level of internet freedom[1] and has definitively become one of the leading countries in internet censorship, coming to resemble Iran and China. This is a complex of measures consisting of:

- Legal prohibitions on advertising circumvention tools and on searching for banned materials, the recognition of VPN use as an aggravating circumstance when an offense is committed, and measures to deanonymize users
- Throttling of services with or without an official ban, blocking by IP addresses and subnets and by protocol (detecting and suppressing VPN use), removal of domains from the National Domain Name System, the introduction of "whitelists", and complete shutdowns of mobile connectivity



Censorship has become ubiquitous and affects everyone in Russia, because the most popular services have come under attack. In this way, the state provokes a gateway effect[2]— the uptake of circumvention tools that unintentionally expand access to other blocked content as well.

At the same time, the state increasingly crosses the line between selective blocking of services (even the most in-demand ones) and the complete shutdown of mobile connectivity. In some regions the latter has become the new normal, particularly in those close to Ukraine, but shutdowns have already occurred in cities such as Moscow and St. Petersburg. Blocking and internet shutdowns create common

[1] Vesteinsson, K., & Baker, G. (2025). Freedom on the net 2025: An uncertain future for the global internet. Freedom House. https://freedomhouse.org/report/freedom-net/2025/uncertain-future-global-internet
[2] Hobbs, W. R., & Roberts, M. E. (2018). How sudden censorship can increase access to information. American Political Science Review, 112(3), 621–636.

inconvenience, thereby provoking irritation and discontent among broad segments of the population.

Adaptation to these processes follows three scenarios: submission (abandoning the use of banned services in favor of "Max," VK, Yandex.Zen, and others), avoidance (seeking alternatives unconnected to the services promoted by the state — a striking example being the growth of the American messenger Imo from fewer than a million users to 8 million in 2025[3]), and resistance (the subject of our interest, the use of circumvention tools). The ubiquitous search for circumvention not only leads to active downloading of VPN services but also creates new forms of cooperation and communities aimed at countering censorship, even where their motive is consumer-driven rather than political.

[3] Американский мессенджер Imo стал пятым по популярности в России [The American messenger Imo became the fifth most popular in Russia]. (2026, February 4). Forbes.ru. https://www.forbes.ru/tekhnologii/554754-amerikanskij-messendzer-imo-stal-patym-po-populyarnosti-v-rossii

Using a VPN

Drawing on the focus group material, we constructed a user journey covering the search for and choice of a circumvention service, the actual experience of using it and the difficulties involved, and the conditions under which users are willing to give up using a VPN.

Stage	Description of the stage
Trigger	Awareness of the need is tied to a specific blocking event. The triggers are predominantly linked to the blocking of Instagram and YouTube, WhatsApp and Telegram. Censorship measures stimulate VPN downloading, which is also confirmed by the words of the Amnezia VPN support representative.
Free entry	The first free VPNs are taken from the top of the App Store/Google Play rankings and from bloggers' advertising. Users often accumulate interchangeable free apps in order to switch between different options depending on whether they work.
Moving to paid services	A build-up of fatigue with the costs associated with using free apps (advertising, instability, the VPN automatically switching off mid-use) pushes users into the paid segment. The choice of a specific service is made predominantly through personal recommendations; to a lesser extent the sample also shows choices based on recommendations from bloggers and specialized organizations (for example, First Department, though this applies mainly to activists), and, last of all, on reviews in the App Store/Google Play. That is, the situation is the direct opposite to the choice of a free service.
Use and attendant problems	The main experienced problem is not blocking but the breakdown of the coexistence of VPNs and local services: regularly switching the service on and off because of resistance from the state-loyal structures of everyday use (banks, marketplaces, taxis, and others). Regional specifics ("whitelists," mobile

	shutdowns) are in many cases insurmountable (circumventing "whitelists" has not yet become widespread and is perceived as a positive distinguishing feature of particular services). Focus groups often mentioned that when something does not work, informants find it hard to determine whether this is due to blocking by Russia, by the service, to a VPN malfunction, or to connectivity problems in general.
Retention / switching	The primary retention factors are connection stability and the quality of support. For many, paying for a VPN has come to be considered part of a household's necessary expenses, on a par with paying for internet. Within the focus groups, a price range of 100 to 800 rubles a month is called satisfactory. A significant retention factor is fault attribution: informants who explain malfunctions by the censor's actions, rather than by the service's shortcomings, did not change their VPN even with regular connection drops, since they proceeded from the conviction that the service would solve the problem (support plays a large role in this respect). Inertia also retains users separately. The ability to connect several devices turns a subscription into a collective infrastructure and raises the costs of switching services. Users leave in four cases: support failed to cope with a problem or otherwise performed unsatisfactorily (delayed responses, ignoring, using a bot instead of a person); prolonged connection instability with no explanation of the causes; the service disappeared on its own (blocked, removed from the app store, shut down); the service is incompatible with outdated equipment.
Relaying	People who already use a VPN often become distribution nodes: they recommend the service, share keys, add their loved ones to their subscription, and install and configure it for those who cannot manage on their own (predominantly older relatives). The furthest form of relaying in the sample is a consumer cooperative, which one informant built around his own server: each new

	membership fee extends the server rental, and loved ones can be added without fees. The invitation to the cooperative itself is circulated only among personal acquaintances.
Giving up the VPN	In all the focus groups, giving up VPN use is, in the informants' own words, unacceptable. They name only two scenarios in which they might give up circumvention: a sharp tightening of the law (prison terms for VPNs) or the lifting of the blocks as such. That said, it should be noted that for older informants technical complexity can become a cause of involuntary abandonment of VPN use. There are also mentions of cases of switching to unblocked resources owing to fatigue with access problems and the need to stay connected (for work, for example).

Attitudes toward blocking and cybersecurity

The study's second focus of interest was attitudes toward blocking, as well as the perception of VPNs in the context of personal cybersecurity. The corresponding block of questions was aimed at clarifying awareness of cybersecurity, the protective tools used, and the perception of threats.

First of all, it should be noted that blocking is universally perceived negatively — it provokes irritation, fatigue, and a sense of the digital environment degrading. None of the informants spoke of it in a positive light. The official state discourse concerning the protection of children, extremism, or sovereignty was not reproduced either in criticism or in attempts to explain the reasons for blocking. In this respect no successes of propaganda are observed within the study, which allows us to suppose that it is not believed.

Some informants find it hard to give themselves any explanation for such a policy at all, noting its futility with references to historical experience (drawing a comparison with Prohibition and the ban on abortion). Those who do offer an explanation treat blocking as state protectionism to support domestic platforms, and as a means of carrying out

surveillance and control over citizens' actions in the digital environment. Informants see behind this policy nothing but the interests of the state, which conflict with their own interests — free access to information and the preservation of privacy on the internet.

All the more telling, then, that a VPN is almost never endowed with a protective function. Informants see it first and foremost as a means of accessing familiar services (and two informants even regard a VPN as an additional source of threat, fearing the theft of their data). With respect to cybersecurity, most users declare indifference. Half of the activist informants, by contrast, express a well-grounded interest in cybersecurity. Ordinary users say that they have "nothing to hide" and that "however much you protect yourself, everything is ultimately accessible," yet when asked about the security measures they use, they recall two-factor authentication, antidetect browsers, disk encryption, and other technical means of protecting their data (up to running "Max" on a virtual machine when they need to use it).

Thus, informants' self-reflection does not coincide with the practices they actually carry out; basic security measures are applied by many.

Awareness in the field of cybersecurity predominantly correlates with awareness in the field of IT. It is important to note that the very word "cybersecurity" sounds to informants like something specialized rather than everyday, which is probably where the gap between reflection and practice arises. A lack of knowledge does not prevent the use of software aimed at ensuring the user's security.

Category	Activists	Ordinary users	Total
Declared indifference to cybersecurity	3 of 6 informants	7 of 10 informants	10 of 16 informants
Technical means (software)	4 of 6 informants	5 of 10 informants	9 of 16 informants
Precautionary measures	5 of 6 informants	8 of 10 informants	13 of 16 informants

The precautionary measures that informants recall when they speak of their own security deserve separate mention. The main sources of threat named in this context were the state and fraud. Precautionary measures connected with fraud are aimed mainly at protection from phishing and in this sense also belong to the sphere of cybersecurity, but they are of no substantial interest to us in the context of the study. As for the state, fears, for example, push users toward avoiding the installation of the imposed messenger "Max" (including under the declared stance "I have nothing to hide") or of Russian apps in general. The attitude toward "Max" looks like the attitude toward communicating over mobile phone lines: it is unsafe, and the Russian user perceives the risk of being wiretapped as inevitable (political topics are "not a phone conversation"). The only difference is that "Max" collects far more information than could be said over the phone.

Fears of the state, meanwhile, are rarely correlated with any legal norms; informants are not inclined to recall them. This applies to a lesser degree to activists, who are better acquainted with the law. It is of interest that one informant, who explained installing a VPN precisely by fear of the law, cited a law that was never passed but was vigorously discussed on social media (namely the news about a possible charge for foreign traffic). At the same time, according to Amnezia support's data, there is a widespread misconception that paying for a VPN may be a crime.

This demonstrates that there is a kind of intimidation among users, who do not follow legislation and may have a false idea of the laws that exist.

Conclusion

Before the mass blockings, a VPN was a tool of the professional milieu; it was censorship that turned it into an everyday technology. Each wave of VPN uptake begins with the blocking of some popular service whose audience sees no alternatives in the Russian-language segment of the internet (as in the case of YouTube, the quantity and quality of whose content are incomparable with RuTube or VK Video) or does not wish to use them (as in the case of "Max," whose installation many avoid, or whose risks they contain by using a separate phone for it).

The qualities of the VPN services themselves are responsible for retaining users, but nothing promotes their downloading as much as the actions of the state. At the same time, on the basis of the focus group material, we can assert that the Russian authorities are not succeeding in suppressing circumvention tools (isolated cases of abandoning circumvention tools have been recorded, but they are too few), and the deterioration of one service or another leads not to giving up the VPN as such, but only to a redistribution of users among services. A closed circle forms: the blocking of a popular service creates mass everyday inconvenience, the inconvenience converts into the installation of circumvention tools, the growth of circumvention provokes a new round of tightening, and this, in turn, recruits the next wave.

In seeking control over the consumption of information, the state itself expands the audience of anti-censorship tools. Moreover, people do not seek circumvention routes individually; they form a multitude of small and large mutual-aid networks: from sharing keys with relatives and loved ones to creating whole cooperatives of dozens of people. Affecting loyalists, oppositionists, and apolitical citizens in equal measure, blocking becomes an unusual source of solidarity, since it acts as a shared problem at the everyday level and forms a routine practice of noncompliance.

Thus, the policy of blocking is, if not counterproductive, then at the very least extremely ambiguous in its results. On the one hand, the loss of a share of users is inevitable when a service is blocked. On the other, the mass uptake of circumvention tools for the sake of a single service — whose absence prompted the user to install a VPN — opens access to the entire array of blocked resources and makes the exercise of censorship more difficult. That is, the solution of a particular problem has as its consequence the overcoming of the existing restrictions as a whole.

Users' fears, meanwhile, are aimed past the actual risks: in the expert's words, the most persistent misconception is that paying for a VPN is illegal, whereas the real legal innovations of the fall of 2025 (liability for the deliberate search for extremist materials and the recognition of VPN use as an aggravating circumstance) are rarely recalled in the focus groups. In the meantime, shifting punishability from the dissemination of banned information to its consumption returns the VPN to its original purpose — namely, concealing network activity from the provider and the state — yet users do not notice this shift (at least not yet).

Despite the conviction that prevails among informants that blocking is useless, this appears true only up to a certain limit. Filtering — that is, restricting access to specific services — is not the limit of the state's capabilities. There exists a further rung of escalation: the infrastructural restriction of connectivity — "whitelists" and the complete shutdown of mobile internet. In some regions, including Rostov-on-Don, such restrictions have become part of everyday life, but they have not yet touched home internet.

"Whitelists" can be circumvented, but this is technically more difficult and depends heavily on the intermediate permitted servers used for circumvention, the blocking of which, in the expert's words, is unlikely but nonetheless possible. Against a complete shutdown of connectivity there is nothing to set at the everyday consumer level. Even as mesh-network technologies using Bluetooth and local Wi-Fi become better known and capable of countering a connectivity shutdown, their use runs up against the problem of scaling (since a network's coverage depends directly on the density of active users). That said, as a study of the practice of shutdowns in India shows, such connectivity restrictions, when applied in the course of protests, make them more unpredictable and violent[4]. This is not especially relevant now, since no large protests are taking place, but it is important for understanding the prospects for how the situation in Russia will develop and for assessing the possible consequences of applying restrictions harsher than filtering.

[4] Rydzak, Jan, Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India (February 7, 2019). Available at SSRN: https://ssrn.com/abstract=3330413

Forecasting

1. Blanket protocol analysis exceeds the capacity of TSPU, while user retention rests on attributing failures to the censor. At the level of filtering, circumvention cannot be suppressed: the censor's capabilities and the services' ability to adapt will maintain a wavering stalemate in which users flow between services rather than abandoning circumvention, and only a shift to a regime where "only permitted resources work" can break this (whitelists, connectivity shutdown). The next frontier of blocking is home internet, which restrictions have not yet touched. It should be expected that home internet will not be filtered but completely shut down when necessary. The testing ground, in all likelihood, will again be the southern border regions.

2. The state has almost no leverage against the foreign platforms that have departed, so its response to the removal of VK-ecosystem services and the "Max" messenger from the App Store will probably put pressure on users inside Russia. As of today, the use of a VPN is not in itself punishable, but after the September elections there are grounds to expect a further tightening of the law around VPNs and their criminalization. There are enough rumors for some users to be overestimating their risks already (the example of the informant who believed in a law that was never passed). A demonstrative criminal or administrative case could serve as a factor of intimidation for users, which would be a significant contribution to censorship[5].

3. The effective means of countering VPN use is becoming not the fight against it, but the creation of obstacles for VPN users in the main everyday services that drop the connection when a VPN is in use (such as food delivery, taxis, marketplaces). These measures are additionally reinforced by the imposition of VK's infrastructure and the "Max" messenger (foreign messengers are banned for state bodies, banks, and marketplaces under Federal Law No. 41-FZ; linking a "Max" account to "Gosuslugi" is imposed even without "Max" installed, and this messenger is among the apps that must be preinstalled on phones sold in Russia). There are grounds to expect a growth in the number of users who will be forced to migrate to domestic platforms. At the same time, a significant stratum of society will continue to resist internet censorship — the use of circumvention

[5] Roberts, M. E. (2018). Censored: Distraction and diversion inside China's Great Firewall. Princeton University Press.

tools and blocked services may take on a more politicized character. Thus, with a stable 36% using a VPN (there being, moreover, a supposition that the figure is understated owing to survey respondents' fear of answering honestly), awareness of circumvention tools is noticeably higher among those who disapprove of the president (51%) and those who do not support the military actions in Ukraine (55%)[6],[7], and the departure of conformists to domestic platforms will only strengthen this selection.

4. As free mass-market apps cease to be effective, circumvention may further become more of a collective practice than an individual one. The cascading distribution of VPNs (to relatives and friends) and cooperatives realize one of the key resources of resilience to censorship: a broad personal social network. They convert awareness into collective resistance to the restrictions. A fragmented, small-scale infrastructure that admits only acquaintances is, in addition, harder to suppress than mass-market services.

5. Possible risk factors are Article 13.29.2 of the Code of Administrative Offenses[8] and Article 274.5 of the Criminal Code[9]. 13.29.2 is an anti-fraud provision with an exception for transferring access with consent for the purposes of lawful use, under which the sharing of keys does not currently fall. For now, circumvention remains legal, but the exception within the article rests on the word "lawful." In the case of Article 274.5 of the Criminal Code, the activity of a cooperative engaged in such practices may be deemed criminal, and its participants held liable under paragraph 2 of that same article. A post-election tightening of the law around VPNs could turn the sharing of keys into an administrative or criminal offense.

---

[6] Levada Center. (2026, April 14). Пользование интернетом и социальными сетями в марте 2026 года [Internet and social media use in March 2026] [Press release]. https://www.levada.ru/2026/04/14/internet-i-sotsseti-v-marte-2026-goda/

[7] Levada Center. (2026, March 31). Проблемы с мобильным интернетом и блокировка иностранных мессенджеров (март 2026) [Problems with mobile internet and the blocking of foreign messengers (March 2026)] [Press release]. https://www.levada.ru/2026/03/31/problemy-s-mobilnym-internetom-i-blokirovka-inostrannyh-messendzherov-mart-2026/

[8] The transfer of information necessary for the registration and (or) authorization of a user of the information and telecommunications network "Internet" in order to gain access to the functional capabilities of an information resource.

[9] The organization of activity to transfer to other persons information necessary for the registration and (or) authorization of a user of the "Internet" network in order to gain access to the functional capabilities of an information resource, where these acts are committed out of mercenary interest or for the purpose of committing another crime.