The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Western Tech Companies Are Capitulating to Russian Censors. Here's How Russians Can Fight Back.

By Sarkis Darbinyan

June 24, 2025

Privecstasy / unsplash

How Russian authorities are pressuring Western corporations to make life easier for Kremlin censorship by removing VPNs from their platforms. But thankfully, there are some measures users can take to circumvent these restrictions.

As of May 29, Google has received 2,729 requests from the Kremlin state communication agency Roskomnadzor to remove resources related to VPNs.

The first was sent in February 2018, the last on Thursday, May 29, 2025. These could be articles ranking VPNs, information about the software, VPN app sites and apps directly, and requests to hide search results. Each request to remove search results could include to several thousand URLs. In May 2024, Roskomnadzor requested that almost 100,000 links be hidden

from users. Not satisfied, they ordered another 478,000 to be removed in early June.

Roskomnadzor only took over applications in Google Play in March 2024, just after the ban on any information about VPNs came into force. The agency stepped up its campaign in a year later, demanding the removal of 86 VPNs. In the first five months of this year, it sent one and a half times more requests to remove VPNs than in the whole of 2024.

Embed:

Despite Roskomnadzor's pestering, Google only removed six VPN services out of a possible 212 in March 2025.

Apple users were less lucky. Between April 2022 and October 2024, the company blocked at least 108 VPN applications for Russians. According to AppleCensorship, Russia is second only to China in the number of blocked apps overall, but leads in the number of remote VPN apps. As of June 2, 2025, 113 apps with the VPN tag were inaccessible in the Russian App Store, 111 in the Chinese version, 32 in the Belarusian and 14 in the Turkish version.

Embed:

Usually, developers try to publicize what happened when they learn their VPN has been removed. They demand that corporations state the reasons behind the removal and point out the incompatibility of doing so with human rights and their company's values. They may also appeal to human rights activists at Access Now, Reporters Without Borders and Roskomsvoboda. Although international organizations like these have traditionally focused more on the actions of states, questions are increasingly being raised about corporate responsibility for complicity in human rights abuses, particularly the enforcement of repressive legislation.

If a VPN is installed on a user's device, it will continue to work even if it is removed from the App Store or Google Play. The problem will be attracting new users, as well as repelling further state attacks. As soon as a VPN starts to fail, dissatisfied users quickly leave, and with each new onslaught from Roskomnadzor, fewer people will use the software.

Related article: Poland Arrests German Man Over Alleged Export of Dual-Use Technology to Russia

While the law is being decided, users should be empowered to become less dependent on centralized platforms. Thankfully, there are ways Russians can circumvent restrictions on VPNs, with varying degrees of convenience and reliability.

Some developers make copies of applications. After the App Store removed Amnezia VPN at the request of Russian authorities, Amnezia released another app. It worked with the same keys and subscriptions as the removed one, so Russian users could make the switch seamlessly. In addition, the well-known provider Free VPN Planet has at least five daughter apps: France VPN, Private and Fast, Free VPN Proxy by Planet VPN, Mexico VPN, Turbo Fast

Proxy and so on.

But this tactic can be quite costly and ineffective since Google Play and App Store algorithms will be able to recognize the clone's similarity.

Users should be aware that fraudsters who want to capitalize on the reputation of legitimate VPNs can also clone apps.

A more labor-intensive but slightly better option is using a VPN based on a distributed network. Many VPNs have only a small number of connection points which allow further access to the free internet, making them fairly easy to block. With distributed VPNs, such as VPN Generator, the entry points are distributed by the network administrators, i.e. the users themselves. Each administrator has a number of sponsored users, usually their friends, to whom they have distributed login keys. Because web traffic flows over multiple hosts on the network, such VPN connections are difficult to trace and block.

A fairly efficient method is to use a Telegram bot to deliver settings and instructions for a VPN. This is what many independent projects and media do — through GenVPN, The Ins VPN Bot, Kovcheg VPN, etc. you can buy a VPN key using stars (in-app currency), create configuration files (files with settings and instructions) through the same bot and set up client applications for your own VPN. More about this further on. In Telegram, you can also make a VPN mini-application with a user interface, service settings, and payment.

Users also have options to access uncensored resources independently. One of the most affordable options is to set up your own VPN server or provide one for an existing product. To do this, you need to rent a virtual server (VPS) such as Amnezia VPN or Outline for about $5 per month, copy its settings, then download and install a VPN wrapper before entering the copied server settings into it. This way, you do not have to worry about personal data being leaked or sold, or about the RCN detecting the server.

You can also download the disappeared application from the developer's website. That said, not all developers put VPN on their sites or have a web page in the first place, if there is a high probability that Roskomnadzor has already blocked it or will do so soon.

Sometimes you can find and download a VPN from a developer on GitHub or Reddit, but that is pretty uncommon.

Related article: U.S. Urges Big Tech to Boost Anti-Censorship Tools for Russians – Reuters

The good news is that app stores usually do not totally remove VPNs at the request of the authorities. Instead, they restrict access to them for devices registered in a certain region.

iOS owners can bypass Apple's georestrictions by creating a new account and registering it as any country in the EU, United States, etc. There are quite a few sets of instructions for how to do this. The VPN verification service, VPN Love, has a step-by-step guide. Once you have done that, the VPNs you are looking for should appear.

Android owners can download VPN app program files with the .apk extension from the developer's website or from F-Droid, a directory of free apps. Once downloaded, the file can

be immediately installed and the app can be used.

There are similar catalogs for iOS, too. But to use them, you will have to work some magic.

The first is through AltStore, a store where different developers upload their products that are not available in the official App Store. AltStore is available only in the EU, as the European Commission obliged Apple to allow its users to download apps from third-party stores. After registering a foreign account, you can download an .ipa (analogous to .apk) of the desired VPN and add it to AltStore as a library. However, few developers have made their software available via this route.

The Scarlet app is similar to AltStore. It does not require a region change, but you need to change your device's settings to show that you trust it. But neither Scarlet nor AltStore are responsible for the security of the opened applications. Moreover, Apple actively fights against applications in Scarlet.

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2025/06/24/western-tech-companies-are-capitulating-to-russian-censors-heres-how-russians-can-fight-back-a89349