Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**722**
Land:	Rusland
Kilde:	Freedom House
Titel:	Freedom on the Net 2022 – Russia
Udgivet:	18. oktober 2022
Optaget på baggrundsmaterialet:	11. januar 2023

Freedom House

FREEDOM ON THE NET 2022

Russia

NOT FREE

23 /100

A. Obstacles to Access	11 /25
B. Limits on Content	6 /35
C. Violations of User Rights	6 /40

LAST YEAR'S SCORE & STATUS

30 /100 **Not Free**

Scores are based on a scale of 0 (least free) to 100 (most free). See the research methodology and report acknowledgements.

Overview

The already restrictive online environment in Russia deteriorated dramatically during the coverage period. After Russian authorities launched a brutal military invasion of Ukraine, the government moved to block prominent social media platforms, including Facebook, Instagram, and Twitter, and issued massive fines to other platforms that refused to remove content and localize user data. Beyond social media platforms, the government restricted access to over 5,000 websites after the invasion was launched, including Ukrainian and other foreign news sites and domestic news sites that provided accurate coverage of the war. Authorities also passed legislation that expanded the powers of state bodies tasked with regulation of the internet, as well as the grounds for what content could be deemed illegal. Among other changes, the government expanded its foreign agents law and mandated that media outlets refer to the war as a "special military operation," developments that prompted many prominent independent news outlets to close rather than risk penalties for continued reporting. Authorities opened several administrative and criminal proceedings under a new law that punishes "knowingly spreading false information" with up to 15 years in prison.

Power in Russia's authoritarian political system is concentrated in the hands of President Vladimir Putin. With loyalist security forces, a subservient judiciary, a controlled media environment, and a legislature consisting of a ruling party and pliable opposition factions, the Kremlin is able to manipulate elections and suppress genuine dissent.

Key Developments, June 1, 2021 - May 31, 2022

- In February and March 2022, the Russian government blocked social media platforms including Twitter and Meta-owned Facebook and Instagram, which was ruled to be an "extremist organization" (see A3 and B1).
- In addition to social media platforms, Roskomnadzor, the media regulator, and other state bodies blocked over 5,000 websites, including Ukrainian and other foreign news sites, after the start of the invasion of Ukraine (see B1).
- Roskomnadzor launched an unprecedented campaign against Virtual Private Networks (VPNs), blocking over 20 of them during the coverage period (see B1, B7, and C4).

- Throughout the coverage period, Roskomnadzor issued escalating fines to social media platforms that refused to remove content and localize user information (see B2 and C6).
- Roskomnadzor compelled social media platforms, many of which suspended their Russian-based operations after the invasion of Ukraine, to remove content linked to opposition figure Aleksey Navalny, particularly around the elections in September 2021, and detained users who posted their support for his movement (see B2, B8, and C3).
- Restrictive measures adopted after the war, such as forcing online media outlets to remove content that used words other than "special military operation" to refer to the invasion of Ukraine, and directives dictating how the media should cover the war, forced several media outlets to stop covering the war or close, and limited accessibility to dissenting viewpoints (see B2, B4, B5, and B7).

A. Obstacles to Access

A1 0-6 pts

Do infrastructural limitations restrict access to the internet or the speed and quality of internet connections?	**5**/6

Internet access in Russia continues to expand gradually. The International Telecommunication Union (ITU) estimated the country's internet penetration rate at 88.3 percent of the population in 2021. [1]

According to Economist Impact's 2022 Inclusive Internet Index, which seeks to measure the accessibility, affordability, and relevance of the internet, 80 percent of households in Russia have internet access. [2] There are 23.2 fixed-broadband subscribers per 100 inhabitants. [3] According to 2021 data from the ITU, there were 107.6 mobile broadband subscribers per 100 inhabitants. [4]

Most of the population has access to third generation (3G) and fourth generation (4G) technology for mobile networks. The Inclusive Internet Index notes that 88.7 percent of the population has access to a 3G or 4G network. [5]

The Russian government planned to launch 5G services in Moscow in 2020 and throughout the country in 2021, [6] but the launch has repeatedly been delayed. In

January 2022, the Rostec State Corporation presented a plan to develop 5G base stations under an agreement with the government, with production scheduled to begin in 2024. [7] The authorities reduced funding for the frequency conversion of 5G networks from 43 billion rubles ($584 million) to 7.85 billion rubles ($107 million) for the period up to 2024, which could have adverse effects for the Rostec plan. [8] However, the impact of sanctions imposed by the United States and the European Union (EU) in the wake of Russia's invasion of Ukraine, as well as the withdrawal of telecom equipment manufacturers from the Russian market, could delay the launch of 5G even further. [9]

Connection speeds are stable, with median fixed-broadband download speeds at 68.8 Mbps and median mobile internet download speeds at 21.2 Mbps, according to May 2022 data from Ookla's Speedtest. [10]

A2 0-3 pts

Is access to the internet prohibitively expensive or beyond the reach of certain segments of the population for geographical, social, or other reasons?	**2**/3

During the coverage period, the cost of internet access increased. In 2022, telecom operators and internet providers in Russia increased the monthly cost of their tariffs, which led to increases between 2 and 10 percent in the cost of home internet. [11]

According to 2021 data from the ITU, a monthly fixed broadband subscription cost 0.7 percent of gross national income (GNI) per capita, while a mobile plan offering 2 GB of data cost 0.9 percent of GNI per capita. [12]

The growing cost of the internet in Russia, which began to climb notably in 2020, is due in part to the growth of operators' costs resulting from the implementation of new laws: the Yarovaya law, and the law on sovereign Runet. [13] The Yarovaya law, which was enacted in 2018, requires operators to install expensive equipment to record and store user traffic data on their networks. In addition, it led to an annual increase in traffic storage volumes, which further affects the internet cost. The law on sovereign Runet also obliges operators to install additional equipment (DPI systems) on their networks to filter subscribers' internet traffic. The same equipment is used to censor and restrict access to sites, and to slow them down.

In March 2022, following the implementation of sanctions by the United States and EU, the Russian Ministry of Digital Development proposed a one-year moratorium on the 15 percent data storage requirement in the Yarovaya law in an effort to support telecom operators. [14] The ministry's plan also aims to introduce "a moratorium on the execution of additional burdens for owners of frequencies for mobile communications in the LTE (4G) standard," which effectively means the construction of communication networks in small towns and along federal highways will be suspended.

In July 2021, President Vladimir Putin signed a law on free access to socially significant websites, [15] which followed a pilot of the program from March 2020 to July 2021. The list of sites for free access included the websites of the President of the Russian Federation and the Government of the Russian Federation, sites of federal ministries and nonbudgetary funds, state media, Russian social networks (such as VKontakte and Odnoklassniki) and Russian email services (such as Mail.ru), among other sites. The law obliges providers and operators to grant access to these sites without charging a fee. Telecommunications companies advocated for the inclusion of compensation from the federal budget in the planned legislation as early as 2020 because operators suffer losses by providing free access to these websites.

In November 2021, the four largest mobile operators in Russia—Beeline, Tele2, Megafon and MTS—announced that they would no longer allow subscribers to purchase unlimited internet plans. [16] MTS and Beeline still offer unlimited mobile Internet, but there are caveats. For example, the MTS plan costs more than 2,000 rubles ($27.16).

A digital divide persists in Russia along geographic lines, with users in smaller, more remote cities, towns, and villages paying significantly more for internet access than users in major urban areas. According to one study, the cheapest fixed-internet subscriptions were available in the Central Federal District, which includes Moscow, while the most expensive fixed-internet subscriptions, which cost almost twice as much, were found in the remote Far Eastern Federal District. [17] This dynamic also held true for mobile internet subscriptions, although the price difference was less extreme.

There are no clear digital divides along religious or gender lines.

A3 0-6 pts

Does the government exercise technical or legal control over internet infrastructure for the purposes of restricting connectivity?	2 / 6

Score Change: The score declined from 3 to 2 to reflect Russian authorities' decision to block Facebook, Instagram, and Twitter following the Russian military's invasion of Ukraine.

The government continued taking steps to centralize control over the country's internet infrastructure during the coverage period, and restricted access to widely used social media platforms, including Facebook, Instagram, and Twitter following the invasion of Ukraine.

In the process of implementing of the 2019 Sovereign Internet Law, the Federal Service for Supervision of Communications, Information Technology and the Mass Media (Roskomnadzor) expanded its ability to censor the internet in Russia. The installation of the Technical Means of Countering Threats (TSPU) equipment, which is based on the use of Deep Packet Inspection technology (DPI) on telecommunications networks, allows Roskomnadzor to restrict access and block websites.

In May 2019, President Putin signed a law aimed at achieving the "sovereignization" of the Russian segment of the internet, or Runet. [18] Its basic provisions took effect in November 2019. The law defines the status of and requirements for the "critical infrastructure" of the Runet, namely international communication lines and internet exchange points (IXPs). Their owners and operators are obliged to ensure the possibility of centralized traffic management in the event of "external threats"—a vague term authorities can potentially invoke to gain control over the relevant infrastructure for almost any reason. The law also provides for the creation of a Russian domain name system (DNS) as an alternative to the global DNS maintained by the Internet Corporation for Assigned Names and Numbers (ICANN), a nongovernmental organization (NGO) based in California.

Following the invasion of Ukraine, the Russian government restricted access to social media platforms (see B1). At the end of February 2022, the Russian authorities began to partially block Facebook in the country, citing Facebook's move to block Russian state-affiliated news sites as justification; [19] the platform had done so days after the invasion, citing requests from the EU and other states. On March 4, Roskomnadzor fully blocked Facebook and Twitter, following the EU's order mandating social media

platforms to block Russian-state affiliated media outlets in member states. [20] Then, on March 14, Roskomnadzor blocked Instagram, after giving users a 48-hour warning. [21] Later in March, the Prosecutor General's Office of the Russian Federation filed a lawsuit to recognize Meta, the parent company of Facebook and Instagram, as an "extremist organization" after Reuters published an article about Facebook's decision to temporarily let posts containing death wishes or calls for violence against Putin, Belarusian president Alyaksandr Lukashenka, and the Russian military remain on its platform. [22] At the end of March, a court in Moscow granted the claim, which took effect immediately. [23]

In March 2021, Roskomnadzor used its DPI equipment to throttle the loading speeds for Twitter in order to punish the platform for what it said was systematic noncompliance with content removal requests (see B1). However, the throttling demonstrated problems with the centralized installation of DPI systems, because in its attempt to block t.co, Twitter's link shortener, Roskomnadzor inadvertently blocked any site that had "t.co" in its URL, including major sites such as Reddit and Microsoft. [24] From 2018 to 2020, the government ordered the blocking of Telegram, a popular messaging application, but it was never fully implemented.

After the Ministry of Digital Transformation cancelled a series of exercises that would test the efficacy of the sovereign internet in 2020, [25] it claimed it completed these tests during the coverage period. Throughout June and July 2021, the Russian government began to test the feasibility of cutting the RuNet off from the global internet, Russian state-affiliated media reported the tests were successful. [26] Then, in September 2021, Roskomnadzor requested that companies abandon Google and Cloudflare's DNS, and DNS over HTTPs (DoH) generally, as it considered blocking apps linked to imprisoned opposition leader Aleksey Navalny—who in the past had helped launch an app designed to coordinate protest voting in the country's choreographed elections (see B1). [27] In March 2022, the Ministry of Digital Development, Communications, and Mass Media ordered state media outlets to stop working with foreign hosting services, and adopt .ru domain names and DNS servers based in Russia. [28]

Large-scale Internet outages and intentional outages remain relatively rare in Russia. Local internet access was interrupted at times during protests in the summer of 2019 in Moscow. In July and August 2019, amid mass protests related to the September 2019 regional elections, authorities carried out targeted localised internet shutdowns

that affected fixed-line connections. [29] Separately, intentional shutdowns were actively used in the Republic of Ingushetia to stymie mass protests there in 2018–19. [30]

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**2** / 6

The ICT market in Russia, despite robust competition among ISPs, remains relatively concentrated due to regulatory and economic constraints. The displacement of local service providers by larger companies, and a number of mergers and acquisitions among these large players, particularly in the European part of Russia, have contributed to market consolidation.

Telecommunications providers are licensed by Roskomnadzor. [31] The costs of complying with data-retention requirements under the 2016 Yarovaya Law (see A2 and C6) and the installation of DPI systems under the 2019 Sovereign Runet Law created a financial hardship for existing service providers and a deterrent to potential new entrants to the market (see A3 and B1). These costs are compounded by the government's import-substitution policy, which asks ICT companies to use hardware and software that is produced domestically. [32]

According to TMT Consulting, in the second quarter of 2021, the five largest internet providers accounted for more than 71 percent of the subscriber base of broadband internet access in the business to consumer segment in Russia. [33] The vast majority of the mobile market is controlled by four service providers. According to the leading provider's 2020 annual report, these companies—MTS (30 percent), MegaFon (28 percent), VEON (20 percent), and Tele2 (19 percent)—accounted for 97 percent of the market. [34] In March 2020, Rostelecom assumed a controlling stake in Tele2, [35] having previously held a 45 percent stake. [36]

In June 2022, after the coverage period, law enforcement reportedly announced they would not allow Antares, Integral, and Arctur to use the 1900-1920 MHz frequencies, which the three companies had planned to use to launch a new telecommunications operator. [37]

In the same month, the Ministry of Digital Development of Russia proposed three packages of amendments that could lead to further market concentration. The first one introduces fines for operators that do not install the systems of operational-search activities (SORM), which allows the government to conduct surveillance (see C5). [38] The proposed fines range from 0.01 to 0.05 percent of the annual revenue for communication services, but cannot exceed 0.02 percent of the annual revenue from the sale of all goods and cannot be less than one million rubles. The second set of amendments propose changes to the Tax Code, which would raise the state tax on "nine types of licenses for communication services" from 7,500 to 1 million rubles ($13,400). [39] The third initiative obliges telecom operators to obtain the FSB's approval before building a network and applying to Roskomnadzor for the appropriate license. In August 2022, after the coverage period, the Ministry of Digital Development revised the fine scheme, establishing a fixed fine for the first offense and reducing the fines for repeated offenses. [40]

A5 0-4 pts

Do national regulatory bodies that oversee service providers and digital technology fail to operate in a free, fair, and independent manner?	**0** / 4

Roskomnadzor, which regulates the ICT and media sectors, often fails to act fairly or transparently. The agency is under the control of the Ministry of Digital Development, Communications, and Mass Media, meaning it has little to no independence from the government.

Roskomnadzor is responsible for implementing the many laws regulating the internet in Russia, including those governing the blocking of online content (see B1) and the localization and retention of user data (see C6). [41] Roskomnadzor's blocking procedures are not transparent. Often, access restrictions are implemented in violation of procedural rules, including blocking the websites without informing their owners.

In March 2020, Andrey Lipov was appointed as the new head of the agency. Previously Lipov ran the Presidential Directorate for the Development of Information and Communication Technology and Communication Infrastructure, a key initiator of the Sovereign Runet Law. A number of the directorate's deputy managers also joined Roskomnadzor. [42]

Roskomnadzor's powers have gradually expanded under the Sovereign Runet Law. A body called the Center for Monitoring and Management of Public Communication Networks, which is primarily responsible for the management of data on network infrastructure, [43] was formed within the agency as part of the legislation. [44] At the same time, the Main Radio Frequency Center, a preexisting body subordinate to Roskomnadzor, has become responsible for the operation and maintenance of special equipment that ISPs must install in accordance with the law. [45]

The Sovereign Runet Law also gave Roskomnadzor a new role as the government representative at Russia's country code top-level domain (ccTLD) registrar, which administers the .ru and .РФ domains. [46]

In May 2022, President Putin appointed former president and current deputy chairman of the security council Dmitry Medvedev as the head of a newly created interdepartmental commission focused on establishing the technical sovereignty of critical information infrastructure, and ensuring that infrastructure can operate independently of the global internet. [47]

There are a number of ICT industry associations in Russia, including the Russian Association for Electronic Communications and the Association of Trading Companies and Manufacturers of Household Electrical Equipment and Computers, but they do not have a strong influence on policymaking.

B. Limits on Content

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content, particularly material that is protected by international human rights standards?	**1** / 6

During the coverage period and especially in the wake of the invasion of Ukraine, Russian authorities intensified their efforts to block access to websites and social media platforms that could host material critical of the authorities or of the invasion. According to the registry of banned sites, in 2021,162,295 IP addresses were blocked in Russia and 103,070 were unblocked. [48] According to the NGO Roskomsvoboda,

which monitors online censorship, as of September 2022 approximately 1.2 million internet resources were blocked in Russia. [49]

Following the invasion of Ukraine in February 2022, the Russian government blocked popular social media platforms, international news sites, Ukrainian news sites, and civil society websites. As of July 2022, Roskomsvobada reported that 5,300 IP addresses had been blocked in Russia as a result of their coverage of the war. [50]

Between the start of the invasion and April 2022, the Russian government blocked social media platforms including Facebook [51] and its messenger, Twitter, [52] and Instagram (see A3).

During the first wave of blocking at the end of February 2022, authorities blocked a plethora of news sites, including the Russia-based student magazine DOXA, [53] BBC, Voice of America, Deutsche Welle, Bellingcat, Paper, Meduza, Mediazona, Interlocutor, Radio Free Europe/Radio Liberty (RFE/RL), Echo of the Caucasus, Republic, Taiga.Info, 7x7 Horizontal Russia, and the Village. In addition to online media outlets, the government also blocked civil society websites, such as Amnesty International's Russian-language website, For Human Rights, the election observation organization Voice, and Human Rights Watch (HRW). [54] At the end of March, the government blocked Google News after Google announced that it would no longer permit users to monetize content that "exploits, dismisses, or condones the invasion." [55] In August 2021, the government blocked the VKontakte account of human rights group OVD-Info because of its coverage of the war. [56]

The authorities also blocked well-known Ukrainian news sites. Prior to the invasion, the Prosecutor General's Office had ordered the blocking of popular Ukrainian internet TV channel Hromadske (Public) for posting "extremist" information. [57] In March 2022, the prosecutor general's office blocked the websites of the Ministry of Health of Ukraine, Dnipro State Agrarian and Economic University, and Ukrinform, the national news agency. Authorities also blocked major Ukrainian news websites and portals, including Correspondent.Net, Ukrayinska Pravda, Left Coast, Novoye Vremya (nv.ua), Depo.ua, Gazeta.uA, Focus.uA, Zakhid.Net, and UAinfo. [58]

Though blocked websites can be accessed via a virtual private network (VPN), Roskomnadzor blocked several VPN services during the coverage period, starting in the summer of 2021 (see C4). As of March 2022, 20 popular VPN services were

blocked in Russia, including Betternet, Cloudflare WARP, ExpressVPN, Hola! VPN, IPVanish VPN, KeepSolid VPN Unlimited, Lantern, Nord VPN, Opera VPN, PrivateTunnel, Red Shield VPN, [59] Speedify, Tachyon VPN, VyprVPN and X-VPN. [60]

In December 2021, Roskomnadzor blocked the TorProject.org website, public proxy servers (nodes) of the Tor network, and some bridges (nonpublic relays to the Tor network), which allow users to access the internet anonymously. [61] Roskomnadzor ordered the blocking based on a 2017 court order. In May 2022, lawyers from Roskomsvoboda managed to successfully appeal the blocking of the Tor Project website through the appellate court, which overturned the December 2017 decision of the Saratov District Court. [62] At the next meeting on May 26, 2022, the prosecutor's office demanded that the court bring Google into the case as an interested party. [63] In addition, the prosecutor's office urged the court to consider information contained in the Tor Browser application as prohibited, recognize the Tor Browser application itself as prohibited and restrict access to it, and oblige Google to remove the Tor Browser application from Google Play. In July 2022, after the coverage period, a court banned Tor with no representatives from the Tor Project present. [64]

In March 2019, it was revealed that the two largest Russian ISPs, MTS and Rostelecom, restricted traffic to several Tor nodes, along with the simple mail transfer protocol (SMTP) servers of ProtonMail, an encrypted email service. [65] The case set a precedent for restricting access to encrypted services, as the Federal Security Service (FSB) directly requested that telecommunications providers impose the block on ProtonMail, without asking Roskomnadzor to first attempt to register the service as an "information dissemination organizer." In 2021, the secure email services anonymousemail [66] and dropmail [67] were blocked because the Prosecutor General's Office alleged the accounts associated with these services had sent emails containing fake terrorist threats.

In September 2021, ahead of elections to the State Duma, Roskomnadzor employed DPI equipment to block the Smart Voting website of Alexei Navalny. [68] In the same month, internet service providers and operators began blocking Google Docs and telegra.ph, a Telegram tool that allows users to post multimedia stories. [69] In July 2021, Roskomnadzor blocked 49 websites linked to Navalny and his Anti-Corruption Foundation (FBK), citing "extremist activity." Earlier in the month, it also blocked Pixabay, the photo-sharing website, and the website of Navalny's lawyer. [70]

In June 2021, a court ordered the blocking of activist Yulia Tsvetkova's Vkonkakte page, "Vagina Monologues," which features abstract pictures of vaginas (see C3). [71]

In March 2021, Roskomnadzor temporarily throttled Twitter after the company refused to block "banned content," which the government said included content related to drug use and suicide (see A3 and B2). [72] However, Twitter expressed concern that the content restrictions would limit free speech, and the throttling began just a day after the government sued Facebook, Google, and Twitter for refusing to delete content related to the opposition protests that began that January. [73] In May 2021, Roskomnadzor reported that the company had deleted more than 90 percent of the disputed material, and subsequently lifted restrictions on traffic for fixed broadband networks, but continued to throttle Twitter's traffic on mobile networks. [74]

Websites featuring content that touches on a host of sensitive topics are subject to blocking under the Law on Information, Information Technology, and Information Protection and associated legislation. Forbidden web content formally includes child sexual abuse images; content related to the illegal sale of alcohol; information about illegal drugs; information about illegal gambling; calls for suicide; calls for extremist activities, riots, or unsanctioned protests; violations of copyright; violations of data protection legislation; and information about skirting online censorship (see B3).

A number of different government bodies, including the Ministry of Internal Affairs, [75] the Prosecutor General's Office, [76] and Roskomnadzor are empowered to order the blocking of web content (see B3). The courts also have wide latitude to block web content.

A 2015 law allows the government to designate foreign organizations as "undesirable," which bars them from disseminating information (see B3). In some cases, these organizations' websites are blocked. [77]

Rules requiring companies to store Russian users' personal data on Russian territory (see C6) are invoked by the government as a pretext for restricting access to certain websites. In 2016, LinkedIn became the first major international platform to be blocked in Russia for failing to comply with data-localization requirements. [78]

B2 0-4 pts

Do state or nonstate actors employ legal, administrative, or other means to force publishers, content hosts, or digital platforms to delete content, particularly material that is protected by international human rights standards?	**0** / 4

Score Change: The score declined from 1 to 0 due to the Russian government's efforts to compel major social media platforms to remove content, and content removal orders issued to news outlets concerning the invasion of Ukraine.

During the coverage period, Roskomnadzor continued to mandate the removal of online content, including content related to the invasion of Ukraine, LGBT+ rights, and the political opposition. When companies have refused to comply, the courts have issued escalating fines. Prior to the war the Russian government had already attempted to compel social media platforms to remove content, but these companies' decision to restrict access to Russian state media outlets in the European Union and elsewhere, led to their blocking (see B1) in some cases, and heftier fines in others.

The Russian government has pressured users and social media companies to delete content, including through the implementation of laws that further constrain free expression in the digital environment. The introduction of the law preventing the spread of false information about the Russian military (see C2) and the government's order to refer to the war as a "special military operation" led to further content removal. Articles punishing "fake news" and defamation of the authorities were added to Russia's code of administrative offenses in 2019 (see C2), and these have been actively employed to intimidate users and outlets into taking down content.

In February 2022, days after the invasion, Russian authorities ordered a number of media outlets to delete the words "war" and "invasion" from their coverage (see B4). [79] Outlets including *Novaya Gazeta*, the Bell, Republic, and others complied.

Throughout the coverage period, the Russian government fined Alphabet, Google's parent company, increasingly large sums, most of which were linked to Google's decision not to remove "prohibited content" from the search engine and YouTube, its subsidiary. In July 2022, after the coverage period, the Moscow-based Tagansky District Court issued a fine of 21.1 billion rubles ($350 million) to Alphabet, for failing to remove content. [80] The court order specifically referenced YouTube's refusal to remove "fake" news about the war in Ukraine. [81] In May, Google's Russian subsidiary

filed an application for bankruptcy to a Moscow court, [82] prompting Russian authorities to seize the company's bank account. [83] In the same month YouTube removed over 9,000 channels and 70,000 videos about the invasion of Ukraine that violated their content policies, including their major violent events policy. [84]

The decision to file for bankruptcy stemmed from Google's failure to pay a fine of 7.2 billion rubles ($98 million), which was ordered in a December 2021 by a Moscow court and calculated based on Google's annual turnover in Russia. In this case, Roskomnadzor alleged Google had repeatedly failed remove "prohibited" information. Meta was also fined 2 billion rubles ($27.15 million) in the same month for similar reasons. [85]

The courts and Roskomnadzor also issued a series of lesser fines and took other restrictive measures against online platforms. In August 2022, after the coverage period, Roskomnadzor stated that search engines need to clearly state that TikTok, Telegram, Zoom, Discord, and Pinterest "are in violation of Russian law because they did not take down 'prohibited information.'" [86] In the same month, a Moscow court fined Telegram 4 million rubles ($64,470) because it did not remove content about the invasion. Twitch, the live-streaming service owned by Amazon, was fined 2 million rubles ($32,400) for the same reason. [87]

In April 2022, Google was fined 12 million rubles ($145,340) because it did not delete information about the war in Ukraine and calls for "extremism" against Russians. [88] In the same month, Meta was fined 4 million rubles ($52,800) because it had not removed content from Facebook and Instagram that promoted "the LGBT community" and which "insult[ed] Russia's national coat of arms." TikTok was also fined 2 million rubles ($26,400) for failing to remove content promoting "homosexual relations." [89] In March 2022, TikTok had prevented users in Russia from live streaming and uploading new videos because of the law that criminalized the spread of fake news (see C2). [90]

The Russian government also took unprecedented measures against nonprofit content hosts during the coverage period. In April 2022, a court in Moscow fined the Wikimedia Foundation, the nonprofit that oversees the Wikipedia and Wikimedia projects, 3 million rubles ($36,400) for not removing six Wikipedia articles about the actions of the Russian army during invasion of Ukraine, upon Roskomnadzor's request. [91] These materials include information about rights groups' documentation of

atrocities committed by Russian forces in Mariupol, Bucha, and Kyiv. Later in the month, the court fined the Wikimedia foundation an additional 2 million rubles ($24,260) for failing to remove other articles about the invasion. [92] In June 2022, after the coverage period, the Wikimedia Foundation filed an appeal against the judge's decision to remove information related to the Russian invasion of Ukraine, arguing that "people have a right to be aware of the facts of the war." [93]

In May 2022, Roskomnadzor also issued a 4 million rubles ($59,000) administrative fine against the Internet Archive, an American organization that preserves online content, because of its refusal to remove content prohibited in Russia. [94]

In November 2021, Google was fined 3 million rubles ($40,400) because it did not remove "banned content" from its search engine and from YouTube. At the time, Google claimed that it had already paid 32 million rubles ($439,000) in fines related to content removal. [95] In the same month, VK was fined 3 million rubles ($40,700) by a court because it did not remove "prohibited content" on the Odnoklassniki social media platform, which it owns. [96]

In September 2021, both Apple and Google removed the Smart Voting application, which was promoted by opposition candidate Aleksey Navalny ahead of the year's state duma elections, in response to a court order. Google was reportedly presented with a list of its Russia-based employees who would be prosecuted if they did not remove the application. [97] Police officers also reportedly showed up to Google's offices and pressured them to remove the application. [98] Additionally, in April 2022, YouTube had restricted access to an antiwar song at the request of Roskomnadzor. [99] In December 2021, GitHub, a hosting service for software development, was fined 1 million rubles ($13,600) by a Russian court at the behest of Roskomnadzor for refusing to delete data related to the Smart Voting application. [100]

The same month, Telegram blocked Smart Voting's bot because local law prohibits campaigning in the days immediately before the election. [101]

In July 2021, Roskomnadzor informed Google that it planned to block YouTube channels belonging to associates of Navalny, including political activist Leonid Volkov and former deputy energy minister Vladimir Milov. YouTube notified the owners of these accounts that they had to take down "prohibited content," or their accounts

would be removed. [102] In the same month, Roskomnadzor sent a letter to Twitter ordering the company to block the account of Lyubov Sobol, an ally of Navalny. [103]

In June 2021, the Tagansky District Court fined Telegram, Google, Facebook, and Twitter for refusing to delete content linked to protests in support of Navalny. Telegram received a fine of 16 million rubles ($218,000) because it refused to delete "extremist content," while Google faced a 12 million ruble fine ($163,000) and Facebook and Twitter were each fined 8 million rubles ($109,000). [104]

After the Russian government launched its invasion in Ukraine, Russia-based search engines, including Yandex, Mail.ru and Rambler, no longer provided links to blocked websites (see B1) in their search results. [105] Yandex had previously confirmed that it filters search results based on Roskomnadzor's list of blocked websites. [106] Additionally, users who search prohibited topics, including "war in Ukraine" receive a notice that "some links are missing in the search results due to the requirements of the legislation of the Russian Federation." [107]

According to Google's transparency report, Russian government agencies issued 18,710 requests for content removal in the first half of 2021 and 18,831 requests in the second half of 2021. Google complied with 67.7 percent of these requests in the first half of the year and 80.5 percent of them in the second half. The primary reason for these requests was copyright, followed by national security. [108]

According to Facebook's transparency report, the company restricted access to 3,072 items in 2021 for allegedly violating local laws related to extremism, the sale and use of regulated goods, and self-harm, among other reasons. Facebook did not report either the total number of content-removal requests it received from the Russian government or the percentage of requests it complied with. [109]

According to Twitter's transparency report, the Russian authorities submitted 10,448 content-removal requests, including court orders, in the first half of 2021, and it complied with 47 percent of them. In the second half of 2021, the company received 8,370 requests, complying with 80 percent of them. [110]

According to Reddit's transparency report for 2021, the company received 32 content-removal requests from the Russian government and complied with 72 percent of them. [111]

Russian social media platforms generally do not disclose the number of content-removal requests they receive from the government, with the exceptions of Yandex and the blogging platform Habr. In 2021, Yandex began publishing transparency reports. In the second half of 2021, Yandex delisted 149,459 search results at the request of Roskomnadzor, as well as 516 other pieces of content. [112] In 2020, social media platform VKontakte debuted an algorithm that automatically removes images included in the federal list of extremist materials from users' posts. [113]

Meduza, the independent online media outlet, also produces a rolling transparency report, detailing all the instances in which authorities requested content removal. [114] Most such requests concern the actions of the Russian military in Ukraine and investigations on government corruption.

B3 0-4 pts

Do restrictions on the internet and digital content lack transparency, proportionality to the stated aims, or an independent appeals process?	**0** / 4

The government in general and Roskomnadzor in particular justify website blocking and filtering under a range of laws and regulations. The legal framework generally does not provide clear criteria for evaluating the legality of content, and authorities do not always offer a detailed explanation for blocking decisions. Website owners have the right to appeal decisions in court, but they are often given a short time to do so. Furthermore, the judiciary's lack of independence limits the possibilities for redress through the appeals process.

The government grants the authority to block various categories of online content to several state bodies, including Roskomnadzor; the prosecutor general's office; the Federal Service for Surveillance on Consumer Rights Protection and Human Well-being (Rospotrebnadzor); the Ministry of Internal Affairs; the Ministry of Digital Development, Communications, and Mass Media; the Federal Service for Alcohol Market Regulation; the Federal Tax Service; and the Federal Agency for Youth Affairs (Rosmolodezh). [115]

In November 2019, Putin signed a law that extended the state's regulation of media outlets designated as "foreign agents" (see B6) to include individuals who "spread information to an unrestricted number of persons, namely on the internet, and receive funding from abroad." [116] The law empowers the government to block so-

called foreign agents' websites, and potentially their social media accounts. In September 2019, Roskomnadzor issued an order on behalf of several agencies that established criteria for determining whether content is subject to extrajudicial blocking. It added criteria for use by Rosmolodezh, which received the power to block internet resources in March 2019 and is responsible for initiating restrictions on content that encourages minors to commit illegal activities. [117]

These agencies can block content that touches on political and social issues enumerated in the Law on Information, Information Technology, and Information Protection, plus related legislation, including legislation prohibiting "fake news" and content that defames the authorities (see C2). Any other online content may be blocked by a court order if it is found to violate the law. Roskomnadzor typically handles blocking orders from other agencies in addition to the judiciary. For orders to block content on a website, Roskomnadzor instructs the hosting provider to issue a takedown notice to the website owner. Most website owners quickly delete the content in question rather than risk the blocking of their entire site. If the content is not removed, it is included on a list of banned material, and ISPs must block it. If an order seeks to block an entire website, Roskomnadzor simply includes that website on its list.

During the coverage period, President Putin signed amendments to the to the Law on Information, Information Technologies, and Information Protection granting the authorities extended powers to block websites without a court order. In December 2021, Putin signed a law allowing the prosecutor general's office to extrajudicially block websites that engage in "substantiation and (or) justification for the implementation of extremist activities, including terrorist activities." Extremist activities are vaguely defined under Article 20.3.1 of the code of administrative offenses. This measure comes in addition to an existing clause in the law that allows websites calling "for mass riots and extremist activity" to be blocked. [118]

In July 2021, President Putin signed additional amendments to the Law on Information, Information Technologies, and Information Protection, which allow prosecutors' offices to force websites to remove "defamatory information" and block those websites if they fail to comply. [119] When a user sends allegedly defamatory information to the prosecutor's office, they have ten days to make a decision on content removal. Once a prosecutor's office has made the decision, the Prosecutor General's Office, which refers the case to Roskomnadzor, has five days to confirm the

decision. After a website is informed they must remove defamatory content, they have 24 hours to do and face blocking in cases where they do not comply.

ISPs are obliged to regularly consult the list of banned websites, which is updated by Roskomnadzor. The means by which ISPs should restrict access to websites is not specified, so they could target IP addresses, domain names, or URLs. Often, the authorities do not clearly indicate the specific pages that they want blocked on a given website, which sometimes leads ISPs to restrict access to the broadest possible range of websites to avoid fines and threats to their operating licenses. Search engines and VPNs must also connect to Roskomnadzor's list and filter their services accordingly; however, foreign companies do not comply with this mandate.

Restrictions on online content are generally implemented opaquely, and official information does not provide a complete picture of internet censorship in Russia. Additionally, the website that lists prohibited information resources does not allow users to view the full list of websites.

Roskomnadzor has additional powers to issue warnings to organizations that are officially designated as mass media if they are deemed to abuse their position. [120] Article 4 of the Law on Mass Media indicates that such abuse can include, among other things, incitement to terrorism, extremism, propaganda of violence and cruelty, information about illegal drugs, and obscene language. If a media outlet receives two warnings within a year, Roskomnadzor has the right to apply for a court order to shut it down.

Since December 2020, President Putin has signed a significant number of laws that pressure social media platforms and websites to remove content at the government's behest: [121]

- In March 2021, Putin signed a law aimed at counteracting electoral violations that empowers the Central Electoral Commission and the regional electoral commissions to send content removal requests to Roskomnadzor, and which increases fines for illegal electoral campaigning to as much as 500,000 rubles ($6,600). The most obvious target of these amendments was the Smart Voting website launched by Navalny's organization. [122]
- In February 2021, a law regulating the content-moderation policies of online platforms came into effect. It compels social media companies to coordinate

their content-moderation efforts with Roskomnadzor, which was tasked with establishing a special e-service for that purpose. When a user issues a complaint about "prohibited content," that may include advertisements for the remote sale of alcohol; online casinos; content that offends human dignity and public morality; and content that expresses a clear disrespect for society, the state, or official state symbols of the Russian Federation, the Constitution of the Russian Federation, or state authorities, the company must block it pending a review from Roskomnadzor. The agency will then notify the user who posted the content that it is being reviewed. [123]

- In December 2020, Putin signed a law prescribing fines for failure to remove content banned by Roskomnadzor. The fines for the first case of violation range from 800,000 to 8 million rubles ($10,000 to $100,000). Ultimately, the fines for such violations can reach a fifth of the company's income in Russia for the calendar year preceding the year in which the violation was observed. [124]
- In December 2020, Putin signed a law introducing sanctions for alleged censorship of Russian media outlets by foreign online platforms. The general sanctions for such violations are fines ranging from 600,000 to 3 million rubles ($7,900 to $39,000) for each particular content-removal action. This regulation also empowers Roskomnadzor to "restrict access to online resource fully or partially using the technical means for countering threats (i.e., DPI equipment)." [125]

Additionally, In July 2021, Putin signed a law obliging foreign tech companies with more than 500,000 Russian users to open representative offices in Russia and create special accounts in Roskomnadzor's information systems to establish direct communications with authorities. [126] The physical representation requirement came into effect in January 2022. Foreign companies face a number of penalties for noncompliance, ranging from a ban on search results and restrictions on accepting payments from Russian residents, to complete blocking. [127] In July 2022, after this report's coverage period, the State Duma passed a bill that would allow the Russian government to fine companies that fail to establish representatives up to 10 percent of their annual turnover for first offenders, and up to 20 percent if they fail to do in the following year. [128] Companies are also required to register a personal account on Roskomnadzor's website and add an electronic form on their website to facilitate feedback from Russian citizens or organizations. [129]

As of February 2022, Apple, Spotify, Viber, Tiktok, Likeme, and Twitter announced that they were taking measures to comply with the new law. [130] However, many of these companies later withdrew from the Russian market following the invasion of Ukraine.

In March 2022, against the backdrop of the invasion, Russia announced its withdrawal from the Council of Europe, which means Russians can no longer appeal the decisions of national courts to the European Court of Human Rights (ECtHR). [131] (It was expelled from the body a day later.) Previously, site owners could appeal blocking orders implemented under local laws to the ECTHR under Article 10 of the European Convention on Human Rights. However, a 2015 law had given the Russian government the right to ignore ECTHR rulings. [132]

In June 2022, the Russian State Duma adopted a package of bills on the nonenforcement of decisions of the ECtHR in Russia. [133] In particular, Russia refused to comply with decisions of the ECtHR that entered into force after March 15, 2022, the day the government filed an application to withdraw from the Council of Europe (see C1). Also, the bill stipulates that fines the government must pay under ECtHR decisions prior to March 15 will be made only in rubles and only to accounts in Russian banks. [134] In addition, the ECtHR will no longer have the authority to review the decisions of Russian courts.

In June 2022, after the coverage period, Alexander Tochenov, the executive secretary of the Human Rights Council under the President of Russia, stated that it was necessary to introduce regulation for blogging in Russia. [135] This is the second attempt by the authorities to censor the activities of bloggers. In 2014, the State Duma adopted a law, but it did not come into full force and was repealed three years later.

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**1** / 4

Score Change: The score declined from 2 to 1 to reflect increased self-censorship resulting from a government crackdown ahead of the September 2021 elections, and intensive efforts to control the online information space during and after the invasion of Ukraine.

Laws prohibiting extremist materials and other content in Russia have contributed to self-censorship online, particularly with regard to sensitive political, economic, and social topics such as the invasion of Ukraine, poor governance, corruption, human rights violations, religion, and the LGBT+ community. The vague wording of laws that touch on online expression, the arbitrary manner in which they are enforced, and the general ineffectiveness of judicial remedies make ordinary users more reticent to express themselves online. [136] The government's crackdown on online news media, as well as social media, has exacerbated self-censorship among journalists in particular.

The adoption of laws criminalizing the dissemination of "fake news" about the Russian invasion of Ukraine and preventing the dissemination of nonofficial information about the war (see C2) further contributed to an environment of self-censorship. Media outlets and individuals who use the term "war" or "invasion" to describe the Russian military's actions in Ukraine face the risk of criminal prosecution. Additionally, media outlets can have their website blocked (see B1). After the adoption of these laws, a number of media outlets were blocked and threatened with closure due to using "war" or "invasion" instead of "special military operation." Administrative and criminal cases were also opened against a number of individuals (see C3).

For example, at the beginning of March 2022, *Novaya Gazeta*, one of the largest independent media outlets in the country, announced that they were removing all coverage of the war in Ukraine and would stop covering it because they did not want their journalists to face criminal prosecution. [137] Though the media outlet planned to continue reporting on other matters, on March 28, 2022, the newspaper received a notification from Roskomnadzor and was ordered to stop publishing the newspaper until the end of the "special operation on the territory of Ukraine." [138] The outlet's media license was later revoked (see B6).

In another instance, the editors of the Bell, an online media outlet, decided to completely stop covering the war because "personal risks to journalists have significantly increased." [139] The publication said that it would focus on the economic consequences of the war. Republic, another online news sites outlet, also removed some articles about the events related to the war due to the introduction of "military censorship in Russia." [140] It's My City, another online media outlet, took similar actions. [141]

A number of Russians faced fines and other legal measures after the Russian authorities banned Navalny's Smart Voting website in September 2021. The authorities arrested people who posted the Smart Voting sticker in their Instagram stories; fined them for posting the exclamation mark—a symbol of the Smart Voting movement—on social media; and prosecuted individuals who created Telegram channels in support of the movement (see C3). [142]

The foreign agents law (see B3 and B6), which requires certain media outlets to identify themselves as "foreign agents," also contributes further to self-censorship.

The authorities have used various drug-related charges as pretexts to censor the news media, and several outlets have been forced to self-censor on this issue. [143] In December 2020, [144] the government adopted a law that imposed fines of up to 1.5 million rubles ($19,700) for promoting drugs and psychotropic substances on the internet. [145] In February 2021 the government adopted amendments to Article 230 of the criminal code ("inducement to use of narcotic drugs, psychotropic substances, or their analogues") that would punish "narcotic drug propaganda" with a minimum of 10 years in prison. [146]

B5 0-4 pts

Are online sources of information controlled or manipulated by the government or other powerful actors to advance a particular political interest?	**0** / 4

Government manipulation, which became more aggressive following the invasion of Ukraine, distorts the online information landscape. Authorities use paid commentators, regime-backed trolls, the Internet Research Agency in Saint Petersburg, and automated "bot" accounts to influence online content. Additionally, following the invasion of Ukraine, Roskomnadzor banned the use of information from unofficial sources and mandated that all media use the wording "special military operation" to refer to the war (see B4). [147] The presidential administration also encouraged state and nonstate media outlets to compare the war in Ukraine to the "the christening of Russian and the Battle of Neva," and stress that the war is a "fight against atheists." [148] The Russian government adopted the letter "Z" as a symbol of the government's war in Ukraine and promoted this symbol through social media. [149]

Domestically, Russian trolls and bots have been observed commenting on news sites and on social media, usually to defend President Putin and smear his critics, including journalists (see C7). Since the invasion of Ukraine, bots have spread false narratives about the war. Starting in the lead-up to the invasion, Russian state media promoted false information alleging that the Ukrainian government committed genocide and that North Atlantic Treaty Organization (NATO) countries would perpetrate false-flag chemical weapons attacks. [150] In March, state-linked actors and outlets intensified their promotion of the narrative that the United States was developing biological weapons in Ukraine, [151] a narrative that they had increasingly worked to push out to justify the February 2022 invasion since November 2021. [152]

New networks of bots and trolls arose in the wake of the invasion. For example, in March 2022, online media outlet Fontanka reported that the Cyber Front Z Telegram channel recruited people en masse to write comments in support of the actions of the Russian army. [153] The workers at the "troll factory" had to publish 200 comments per day on Telegram, YouTube, and other sites, from an office St. Petersburg, where around 100 people worked each shift.

The Russian government and affiliated online platforms have also co-opted the practice of fact-checking to further spread disinformation, debunking supposed "Ukrainian disinformation" and providing fake "facts" about events that purportedly occurred. [154] For example, the Telegram channel Война с фейками ("War on Fakes"), which amassed 62,500 subscribers between the start of the war and early March 2022, claims to fact check "the information war against Russia," but actually disseminates disinformation. [155]

Social media platforms based outside of Russia continue to identify and remove state-linked disinformation networks. In February 2022, Meta, the parent company of Facebook, removed a disinformation network that operated on Facebook and Instagram, as well as other platforms not owned by Meta, that aimed to promote the idea that the United States and Europe had betrayed Ukraine, and to suggest that Ukraine was a failed state. [156] In March 2022, Twitter announced that it banned 100 accounts that promoted the hashtag #IStandWithPutin under their "coordinated inauthentic behavior" policy. [157] Research from the Stanford Internet Observatory found that in December 2021 and January 2022, Twitter removed Kremlin-linked accounts that promoted the narrative that NATO had provoked the Russian invasion of Ukraine. [158]

In May 2022, YouTube announced that it had removed over 70,000 videos and 9,000 channels that violated its "major violent events" policy. A YouTube representative stated that much of the removed content was "narratives that are coming from Russian government, or Russian actors on behalf of the Russian government" (see B2). [159] In March, Twitter remove tweets from the Russian embassy in London that disseminated images claiming the Russian military's bombing of a hospital in Mariupol was fake. [160]

Facebook continued to place fact-checking labels on Russian media outlets, including Lenta.ru and Gazeta.ru, Zvezda, and RIA Novosti. The Russian government cited these labels as part of its initial justification for blocking Facebook. [161] In April 2022, Twitter also announced that it would stop recommending Russian state accounts and remove any posts that contained images of prisoners of war. [162]

During the coverage period, social media platforms also removed Russian networks conducting foreign influence operations in countries other than Ukraine and those in the European Union. For instance, in January 2022, Facebook reported that it removed a network of three Russia-based accounts that proposed to journalists in Nigeria, Cameroon, the Gambia, Zimbabwe, and the Democratic Republic of Congo that they republish articles that individuals behind the Russia-based accounts had written. [163]

The government has also sought to carefully control the domestic narrative around COVID-19. [164]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**1**/3

There are a number of economic and regulatory constraints that limit users' ability to publish content online. Onerous regulations and restrictive laws affecting online news media have pushed some outlets to downsize, change owners, or exit the market altogether. Amendments to the Law on Mass Media that came into force in 2016 prohibit foreign citizens and organizations from owning more than a 20 percent stake in a Russian media outlet. As a result, foreign media holdings have left Russia and, in some cases, transferred ownership to Russian entities. [165] According to

Roskomnadzor, 821 media outlets changed their shareholder structure shortly after the amendments entered into force. [166]

Authorities increasingly use the 2012 law, which was first employed in 2017, on "foreign agents" to limit user's ability to publish content online. The law, which was strongly opposed by Russian and international human rights organizations, [167] requires NGOs and other entities that receive some foreign funding and engage in vaguely defined "political activities" in Russia to register as "foreign agents" and label their content. If they refuse to do so, they must reveal detailed financial information or face escalating fines. [168]

The government continues to expand the scope of the law. In December 2020, Putin signed a law that makes it possible to assign the status of "foreign agent" to media outlets, individuals, and organizations that are not registered as legal entities, if they are engaging in "political activities." Moreover, the law obliges media outlets to identify foreign agents as such when they are mentioned in any publication. [169] In April 2021, Putin signed a law that introduces fines for journalists and editorial offices for disseminating messages and materials from media published by "foreign agents" without specifying their status. [170] In March 2022, the State Duma approved amendments to the legislation that propose the creation of a separate register with information about individuals who are themselves considered foreign agents and people associated with them. [171] In June 2022, after the coverage period, Putin signed a law that expands the definition of foreign agents to include "anyone under foreign influence" (see B1). The law is set to come into effect in December 2022. [172]

As of March 2022, approximately 400 entities had been added to the foreign agents list. [173] In January and February 2021, RFE/RL and its Russian affiliates that were recognized as foreign agents were fined 1.1 million rubles ($14,400) and 2.2 million rubles ($28,900), respectively, because their websites did not label their content according to the law. [174] In April 2021 the government labelled Meduza, one of Russia's largest independent media outlets, as a "foreign agent," threatening its ability to maintain funding. [175] In May 2021, the Ministry of Justice also recognized the recently established media outlet VTimes as a foreign agent. [176] VTimes was created in July 2020 by journalists who had left *Vedomosti*—a leading Russian business newspaper—after its deputy chief editors resigned in mid-2020 over the paper's acquisition by new pro-Kremlin owners. In October 2021, the government labelled Bellingcat, the investigative online outlet, as a foreign agent. [177] Then, in March 2022,

the government placed Deutsche Welle, the German state-funded media outlet, on the foreign agents list. The measure followed the German government's decision to prevent Russian state-linked outlets from broadcasting and the subsequent EU-wide regulation mandating the blocking of these outlets. [178]

The government continues to add individuals to the foreign agents list as well. In December 2020, the Ministry of Justice added five people to the list of "media outlets–foreign agents," including human rights activist Lev Ponomarev and several RFE/RL journalists, marking the first time that individuals were included on the lists. Some of the affected journalists attempted to challenge the decisions. In March 2021, courts in Moscow and Pskov suspended the foreign-agent status of journalists Sergey Markelov and Lyudmila Savitskaya, who worked at 7x7, a media outlet in northwestern Russia. [179] In October 2021, the authorities designated Nobel prize winning journalist Dmitry Muratov and BBC journalist Andrei Zakharov as foreign agents. [180]

Foreign-agent status is primarily a form of economic pressure on media outlets, since it deters their private sponsors from providing financial support. The designation also entails significant reporting requirements, as well as the need to place a special disclaimer on all materials. Even ordinary users who cite these materials without using the disclaimer can be fined.

The government has also revoked media licenses for outlets that fail to mention that organizations they cover have been placed on the foreign agents' list. For example, in September 2022, after the coverage period, the Supreme Court revoked *Novoya Gazeta*'s license because it did not refer to two organizations as "foreign agents" (see B4). [181]

Users convicted of extremism or other offenses involving mass media or the internet are legally barred from serving as editors in chief at publications. [182]

The government provides state-run media with several billion rubles in subsidies each year, further distorting the digital media market and making it more difficult for independent outlets to compete. [183]

Following the Russian invasion of Ukraine, a number of social media platforms and other online platforms limited advertising services in Russia, preventing outlets and individuals from monetizing their content. For example, in March 2022, Google and its subsidiary YouTube, stopped all advertising in Russia. [184]

B7 0-4 pts

Does the online information landscape lack diversity and reliability?	**1** / 4

Score Change: The score declined from 2 to 1 to reflect the closure of a number of independent online media outlets, and the general deterioration of the diversity and reliability of the online information landscape.

The diversity and reliability of the online landscape deteriorated during the coverage period, as the range of news and opinion available to ordinary users has been severely curtailed by the government and social media platforms have been blocked. As the space for independent print, radio, and broadcast media shrinks, online publications and social media have become increasingly important platforms for critical expression and civic mobilization.

According to data from Mediascope, a market research company, 80 percent of the population over age of 12 used the internet in Russia as of April 2022. [185] The study also found that Russians began to spend less time on the internet starting in February 2022, due to the blocking of Facebook and Instagram, but internet activity picked back up to preinvasion levels by April 2022. Users of platforms that were blocked in the wake of the invasion primarily flocked to VKontakte and Telegram.

Research suggests that Russians have become less trusting of television sources and more trusting of media consumed online since the outbreak of the war. According to a study on Russian media consumption from *Accelerate Research,* 23 percent of respondents cited television as the most trusted news source in April 2022 compared to 33 percent in March. [186] Online information became slightly more trusted: 23 percent of respondents listed social networks, Telegram channels, and blogs as their most trusted information sources in April as opposed to 19 percent in March.

Russian users' ability to access critical content online was significantly limited during the coverage period due to the widespread blocking of websites and the restrictions placed on prominent independent media outlets (see B1 and B4). Following the invasion of Ukraine, social media platforms, including Facebook, Twitter, and Instagram, were blocked. The blocking of these social media platforms forced users

onto platforms with links to the Russian government, like Yandex and Vkontakte, which hid information about the war (see B2).

Although YouTube, one of the most popular online platforms, was not blocked by the government, the Kremlin continued to promote RuTube, a competitor owned by state-owned Gazprom media. Additionally, government authorities reportedly offered prominent YouTube and TikTok users $1,700 a month to use RuTube and Yappy, a Russian application that resembles TikTok, instead. [187] YouTube remains significantly more popular; however, RuTube did gain 1.1 million users in March 2022. [188]

Other blocked websites include Ukrainian news sites, international news sites, and Russian news sites that tried to accurately report on the work (see B1) After the invasion, a number of media outlets, including *Novaya Gazeta* and the Bell, shut down, reduced their coverage, or move their websites outside of the RuNet. Even before the invasion, many independent online media outlets within Russia have been forced to shut down due to government pressure (see B4, B6 and C3). [189]

Users that use a virtual private network (VPN) can still access a diverse range of media and news sources in Russia. In fact, BBC's Russian service encouraged users to use the Tor Browser (see B1 and C4) to access their site. [190] However, it has became more difficult for users to access VPNs since the Russian government intensified its efforts to block them in 2021. Approximately 20 VPN websites had been blocked as of the end of the coverage period (see B1). [191] Nonetheless, VPN usage increased significantly during the war, from 15,000 users per day prior to the war to a high of 475,000 users per day in March 2022. In May, an estimated 300,000 people were still using VPNs daily. [192]

In April 2022, government agencies, including the Federal Tax Service, stopped accepting emails from foreign domains, citing fears of cyberattacks originating from abroad. [193]

The authorities use the 2019 law on fake news to smear bloggers and other independent news sources (see B2 and C2). Roskomnadzor has piloted a public list of information resources that "repeatedly disseminate false information" on its website, ostensibly so that media outlets know not to cite them. [194] However, it compiled the list in a haphazard manner, initially including the widely respected business daily RBC. [195]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**2** / 6

Score Change: The score declined from 3 to 2 due to surveillance efforts against protesters, and punitive measures the government took against individuals who organized online.

Although the internet remains the most versatile and effective platform for activism in Russia, facilitating efforts to confront propaganda, hold officials to account, and organize protests, this function continues to come under increasing pressure from the authorities. A 2019 report from the OVD-Info human rights project highlighted how the government restricts freedom of assembly online. A 2022 investigation by the *New York Times* also shed light on Roskomnadzor's efforts to surveil users that attend or organize protests (see C5). **196**

Those calling for demonstrations on the internet may face criminal or administrative penalties. Other tactics the government employs to constrain mobilization include cyberattacks against activists, blocking social media platforms, monitoring activists' social media profiles, placing informers in public or private chat groups that are used to organize demonstrations, harassing journalists who cover protests, and otherwise preventing journalists from gathering information about protests and protesters. **197**

The authorities continue to prosecute individuals who organize and participate in protests, including those protesting the war. For example, In April 2022, a court sentenced four former journalists of the student online media outlet Doxa, Armen Aramyan, Natalya Tyshkevich, Vladimir Metelkin, and Alla Gutnikova, to two years of obligatory labor for involving minors in illegal activities in connection with a video the outlet published about students who were expelled after participating in protests (see C3). **198** Previously, in April 2021, police had raided Doxa's offices. Members of the editorial board were accused of involving minors in illegal protests and were banned from using the internet and from leaving their homes for two months. **199**

Law enforcement has also searched protesters' phones and utilized facial-recognition systems in the Moscow metro to prevent people from protesting (see C5). After protests against the Russian invasion of Ukraine erupted in early March 2022, videos

documented police in Moscow demanding access to people's mobile phones. [200] Later, on Russia Day, June 12, police detained 67 people, including journalists and activists, after the facial-recognition system in the Moscow Metro identified them to law enforcement agencies. Forty-three of the detainees were detained because the system identified them as potential protesters. [201]

Throughout the coverage period, authorities took a range of measures to stifle opposition figure Aleksey Navalny and individuals associated with his Anti-Corruption Foundation (FBK) and Smart Voting movement. In March 2022, Navalny was sentenced to nine years in a maximum-security prison on charges of fraud and contempt of court. [202] In September 2021, Roskomnadzor ordered Google and Apple to remove the Smart Voting applications from their respective app stores; [203] the companies complied (see B2). The regulator also blocked access to the Smart Voting website and 49 affiliated websites (see B1). [204] The authorities forced people who shared symbols linked to Navalny's movement on social media to remove them. and in some cases, arrested them (see B2 and C3).

Previously, in April 2021 Leonid Volkov, a close Navalny associate, was accused in absentia of involving minors in protests. [205] A law introducing stiff fines and potential jail time for individuals or organizations that encourage minors to participate in unsanctioned protests had been adopted in December 2018 (see C2). [206] Critics at the time argued that it was aimed primarily at Navalny, whose rallies are popular with young people. The first prosecution under this law targeted a Navalny supporter who had shared information about a protest on VKontakte. He was found guilty in March 2019 and fined 30,000 rubles ($390). [207] The authorities have since punished other Russians for the publication of posts urging people to participate in unauthorized rallies.

In April 2021, the Moscow prosecutor's office suspended the activities of the Navalny movement's headquarters and regional offices. Shortly afterward, Navalny's associates stated that they would curtail their organizations' activities in Russia in order to avoid criminal prosecution of employees and volunteers. [208] In late May 2021, the parliament adopted a law banning persons associated with a court-designated extremist organization from being nominated for elections at all levels. This law effectively prevented any FBK members or volunteers from participating in the 2021 parliamentary and regional elections. [209] In June 2021, the Moscow City Court ruled that the FBK and Navalny's headquarters qualified as extremist organizations.

In March 2021, data were leaked from Free.navalny.com, a site that Navalny's supporters had used to estimate the number of individuals at protests. In April 2021, unknown individuals sent intimidating emails to people who had registered on the site (see C8). Many of the individuals whose data were leaked also lost their jobs. [210]

Weeks after the rallies in support of Navalny in early 2021, several journalists were detained on charges of participating in illegal protests—including Baza editor in chief Nikita Mogutin and Dozhd television correspondent Aleksey Korostelev. [211]

C. Violations of User Rights

C1 0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	**1** / 6

Although the constitution guarantees freedom of expression, [212] this right is subject to numerous legislative restrictions and is routinely violated. Censorship is nominally prohibited by the constitution. There are no laws that specifically protect online expression. Online journalists do not have the same rights as traditional journalists, such as ability to receive accreditation at official events, unless they register their websites as mass media outlets. However, mass media outlets are subject to additional obligations, such as avoiding the use of offensive language. A number of restrictive laws, coupled with repressive law enforcement and judicial systems, have also eroded freedom of expression in practice (see C2).

As of the end of the coverage period, the Russian government had not declared martial law in response to the invasion of Ukraine, but in June 2022, Putin did sign a decree creating a Main Directorate of Rapid Response within the Interior Ministry, which would implement martial law in the case it was enacted in June 2022. [213]

Russia's judiciary is not independent. The courts tend to side with the government, refusing to apply provisions of the constitution and international treaties that protect the rights of citizens. In 2019, the courts acquitted defendants in fewer than 1 percent of criminal cases. [214]

In March 2022, Russia was expelled from the Council of Europe. [215] The Committee of Ministers of the Council of Europe pointed out that the country's actions in Ukraine represented a serious violation of Article 3 of the charter on the principle of the rule of law. The expulsion also means Russia is no longer party to Convention for the Protection of Rights and Fundamental Freedoms. In June 2022, after the coverage period, the State Duma passed a law invalidating the European Court of Human Rights (ECtHR) decisions made after March 15 and stipulating that Russians will no longer be able to appeal to the court. [216]

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities, particularly those that are protected under international human rights standards?	**0** / 4

Score Change: The score declined from 1 to 0 because of a new law stipulating that those deemed to have spread false information about the Russian armed forces can face up to 15 years in prison.

Users in Russia can face civil and criminal penalties under a range of laws, the majority of which are contained in the criminal code and the code of administrative offenses. New laws and amendments that can be invoked in order to criminalize legitimate, nonviolent expression online are introduced regularly.

The criminal code imposes penalties, usually in the form of fines, for defamation (Article 128.1); slandering judges, public prosecutors, or other members of the justice system (Article 298.1); and insulting representatives of the authorities (Article 319). [217] Article 6.21 of the administrative code prescribes fines for "advocacy of nontraditional sexual relations among minors," [218] while Article 148 of the criminal code bans insulting religious feelings, which is punishable by fine or imprisonment. [219] Articles 20.3 and 20.29 of the administrative code prescribe fines for displaying extremist symbols (such as Nazi symbols) and distributing extremist materials, [220] and Article 354.1 of the criminal code bans spreading false information about the Soviet Union's actions in World War II. [221] In March 2020, Article 20.3 of the administrative code was amended to allow extremist symbols to be displayed without penalty for nonpropagandistic purposes. [222]

In addition, more severe criminal penalties are also provided for public calls to commit suicide (Article 110.2 of the criminal code) and incitement to mass riots (Part 3 of Article 212 of the criminal code).

In March 2022, Putin signed a law that amended the criminal code to outlaw the dissemination of "knowingly false information about the activities of the armed forces of the Russian Federation" and discrediting the actions of the Russian military. Spreading "knowingly false information" results in up to 15 years in a penal colony in cases where it causes "serious consequences." In other cases, the offense results in a fine ranging from 700,000 to 1.5 million rubles ($9,300 to $20,100), to up to three years in prison. Statements that "obstruct the use of Russian troops to protect Russian interests" or "maintain peace and security" result in a fine ranging from 100,000 to 300,000 rubles ($1,300 to $4,000) or up to three years in prison. In cases where these calls entail "serious consequences," users face a fine from 300,000 to 1 million rubles ($4,000 to $13,000) or up to five years in prison; calls for sanctions against Russia lead to a fine of up to 500,000 rubles ($6,700) or up to three years in prison. [223] The amendments regarding knowingly "spreading false information" were codified under Article 207.3 of the criminal code, and the crime of "public actions aimed at discrediting" the military were introduced under article 280.3 in the criminal code and article 20.3.3 of the code of administrative offenses. [224]

Articles 280 and 280.1 of the criminal code punish online calls for extremism and separatism with up to five years in prison. [225] Article 20.3.1 of the administrative code assigns fines or up to 15 days in jail for those found guilty inciting hatred online, [226] and repeat offenders can face longer prison terms under Article 282 of the criminal code. [227] If a criminal case is opened against an individual for "extremist" activities, that person could be included on a list maintained by the Federal Financial Monitoring Service (RosFinMonitoring). [228] Those on the list are banned from certain professions, and their bank accounts can be frozen, even if they are not convicted of a crime.

In April 2022, Putin signed a law that criminalized equating the role of the USSR and Nazi Germany in World War II, likening the actions of the USSR's military personnel to Nazi Germany, and denying the role the USSR played in defeating Nazi Germany. [229] The measures, which were included in the code of administrative offenses, stipulates that citizens can a fine of up to 2,000 rubles ($27), or administrative arrest of up to 15 days for a first offense.

In March 2021, the parliament adopted amendments to the administrative and criminal codes that introduced penalties for the rehabilitation of Nazi ideology and defamation of World War II veterans via the internet. The maximum punishments for Russian users are a fine of 5 million rubles ($66,000) or five years in prison. The provisions related to the defamation of war veterans were added just ahead of the second reading of the bill, and shortly after Navalny was fined for allegedly defaming a World War II veteran under the previous version of the law, which prohibited online speech denigrating the honor and dignity of a person. [230]

In August 2020, the Supreme Court recognized the Russian criminal subculture known as AUE ("Prisoner's Codex Is Unified") as an extremist organization, approving a request from the prosecutor general's office. Since then, the activities of creators and administrators of AUE-related online communities have fallen under Article 282.1 of the criminal code ("organization of an extremist community"), with a maximum penalty of 12 years in prison. The AUE online communities have millions of followers.

A pair of laws signed in March 2019 introduced new penalties for online speech. One penalizes the dissemination of fake news online under Article 13.15 of the administrative code (see B2). [231] Individuals or organizations found to have shared fake news face fines of up to 1.5 million rubles ($19,700), and if they do not remove the offending content, their websites can be blocked. The second law penalizes the spread of information that "exhibits blatant disrespect for the society, government, official government symbols, constitution or governmental bodies of Russia"—commonly referred to as "defamation of power"—under Article 20.1 of the administrative code with fines or, for repeat offenders, 15 days of jail time. [232]

In April 2020, Putin signed a law that set increased penalties for spreading fake news related to the coronavirus. [233] Following this legislative change, individuals can be fined up to 700,000 rubles ($9,200), or up to 2 million rubles ($26,000) if the false information led to anyone's death, under Articles 207.1–2 of the criminal code, while media outlets and other legal entities can be fined up to 5 million rubles ($66,000) under Article 13.15 of the code of administrative offenses. [234] Individuals who share coronavirus-related fake news can also be imprisoned for up to three years, or five years if the false information led to anyone's death. [235] Later that month, the Supreme Court published clarifications on this law, stating that it could be applied only if two conditions are met: first, the perpetrators knew about the false nature of

the information, and second, they knowingly presented it as if it were reliable information. [236]

The 2016 Yarovaya Law altered nearly a dozen existing laws, with significant ramifications for internet freedom. [237] Among these changes were amendments to Article 205.2 of the criminal code, which imposed prison terms of up to seven years for calling for or justifying terrorism online. [238]

In July 2022, after the coverage period, the State Duma adopted amendments to the criminal code that introduce criminal penalties for "public calls to carry out activities directed against the security of the state" and for "confidential cooperation of Russians with foreign intelligence services" and "international or foreign organizations." [239] For those who make public calls against the security of the state, fines range from 200,000 to 1 million rubles ($2,700 to $13,400). Criminal liability for cooperation with foreign intelligence services, international, or foreign organizations results in three to eight years imprisonment and a fine of up to 1 million rubles.

C3 0-6 pts

Are individuals penalized for online activities, particularly those that are protected under international human rights standards?	**1** / 6

Criminal and administrative charges are widely used to stifle critical discussion online. Numerous individuals have been charged for their posts or reposts on social media, including a number of users charged under new legislation passed during the coverage period.

In July 2022, after the coverage period, Andrei Pivovarov, the former director of opposition group Open Russia, was sentenced to four years in a penal colony for "running an outlawed prodemocracy movement." [240] He has been held in prison since he was arrested at the end of May 2021 as his flight to Warsaw was about to take off from St. Petersburg (see C7). The initial arrest concerned a Facebook post he shared in August 2020, in which he voiced his support for a candidate in Krasnodar. [241]

Following the invasion of Ukraine in February 2022, a number of people were charged under a March 2022 law that criminalizes "knowingly spreading false information" about the war (see C2). According to OVD-Info LIVE news, as of the end of March

2022 the police had issued more than 400 administrative charges under the new measure. [242] According to an August 2022 report from OVD Info, there have been 75 criminal cases opened under Article 207.3, which concerns the dissemination of false information. [243] In July 2022, Aleksei Gorinov, a municipal councilperson in Moscow, was the first person to be sentenced to prison time under the new law, receiving seven years in prison for offline comments he made at a council meeting about the deaths of Ukrainian children. [244] In other cases:

- In July 2022, after the coverage period, opposition politician Ilya Yashin, who was already detained after being arrested on separate charges the previous month, was charged under the law over a YouTube video he posted about the Russian military's actions in Bucha, where rights groups have documented evidence of a massacre. He faces up to 15 years in prison. [245]
- In March 2022, a man in the Kemerovo region was fined 60,000 rubles ($530) after he posted a video urging people to join antiwar protests. [246]
- In the same month, Ioann Burdin, a priest, was fined for a speech he gave to his parishioners condemning the "fratricide" in Ukraine as well as a statement he posted on the parish website advocating for the end of the armed conflict. [247]
- On March 13, Channel One journalist Marina Ovsyannikova, who had been depicted in a viral video after the start of the war in which she displayed an antiwar poster while on the air, was fined 30,000 rubles ($270). [248] Later in the month, Nikolay Kuzmin, a municipal deputy from the Yabloko party, was fined 30,000 rubles for reposting the video. [249]
- On March 24, the chief director of the Kudymkar Drama Theater, Yulia Belyaeva, was charged with discrediting the actions of the Russian armed forces because of a statement she had posted on VKontakte the day the Russian government launched the invasion. [250]
- A resident of Novokuznetsk was fined 50,000 rubles ($450) for publishing a video on her personal social media page calling on people to condemn the invasion. [251]
- In March, a Yekaterinburg court fined Yevgeny Roizman, the former mayor of the city, 100,000 rubles ($830) for antiwar statements he made on YouTube and Twitter. [252]

Throughout the coverage period, users were also prosecuted and detained for sharing links to the Smart Voting app and symbols linked to the Smart Voting movement,

including the red exclamation mark:

- In July 2022, after the coverage period, at least three individuals who participated or planned to participate in municipal elections in Moscow were charged under the article on displaying the symbols of an extremist organization (part 1 of article 20.3 of the code of administrative offenses) for posting about Smart Voting in September 2021 and 2019. [253]
- In December 2021, Rostislav Pavlishchev, a student from Rostov-on-Don, was detained for ten days because he posted about Navalny, Smart Voting, and the Anti-Corruption Foundation on Instagram. [254]
- In September 2021, Bella Nasibyan, who worked for parliamentary candidate Alexander Ryabchuk and hosted the RusNews YouTube channel, was placed in administrative detention in Rostov-on-Don for five days because she posted a Smart Voting sticker in an Instagram story. [255]
- In September 2021, The Krasnoyarsk prosecutor's office filed an administrative protocol against Natalya Peterimova, the former head of Navalny's local headquarters, because of Instagram posts from 2018 and 2020, which featured Alexei Navalny's logo: a white letter "H" with a red exclamation mark inside. [256]

Users continued to face charges for posts allegedly calling for violence and rallies. Examples include:

- In April 2022, a court sentenced four journalists who used to work for DOXA, a student-run online media outlet, to two years of obligatory labor for allegedly involving minors in illegal activities. The charge stemmed from a video about students who faced expulsion from their universities after participating in protests (see B8). [257] In April 2021, authorities searched the office of DOXA and charged four editors, who also had their apartments searched, with "inciting minors to protest in illegal protest rallies." [258]
- In April 2022, Laysan Sultangareyeva, who was previously arrested at a protest, was arrested again because of her social media posts and photos she posted in an antiwar Telegram group. [259]
- In February 2022, a Chita court sentenced blogger Aleksey Zakruzhny (Lyokha Kochegar) to two years and two months of suspended imprisonment for a 2021 YouTube livestream in which he chastised the local authorities for blocking access to cemeteries on Parent's Day because of the COVID-19 pandemic. He was charged with inciting mass riots under Article 212 of the criminal code and

public calls for extremist activities under Article 280 of the criminal code. [260] The court also banned him from operating his YouTube channel for three years and confiscated his equipment. In February 2021, he had been sentenced to two years and three months of probation for allegedly inciting extremist activity on YouTube. He had previously been fined several times for criticizing President Putin. [261]

- In October 2021, the Kolomna City Court issue a year-and-three-month sentence against environmental rights activist Vyacheslav Yegorov, who had written articles about issues with waste disposal. He was convicted under Art. 212.1 of the criminal code, which criminalizes "repeated violation of the established procedure for organizing or holding a meeting, rally, demonstration, march, or picket." [262]
- A resident of St. Petersburg, Vadim Tsvetkov, was sentenced to three years of probation for reporting on police activity on Telegram; authorities said his reporting contained calls for violence. Tsvetkov was found guilty of incitement to extremism under Article 280 of the criminal code). [263]
- In April 2021, a Moscow court convicted Pavel Zelensky, a cameraman who worked for the FBK, of inciting extremism, sentencing him to two years in a penal colony for social media posts that criticized the Russian government. He posted the comments after journalist Irina Slavina self-immolated in October 2020 (see C7). [264] The authorities also opened a criminal case on the involvement of minors in protests actions, targeting Leonid Volkov, an ally of Navalny and the founder of the Society for the Protection of the Internet. Soon after the case was opened, Volkov was put on a wanted list and charged in absentia. [265]
- In March 2021, a district court in Krasnodar sentenced Marina Melikhova, leader of the local branch of the Citizens of the Soviet Union movement, to three years and six months in prison for inciting extremist activities; she had posted a video in a VKontakte group calling for the dissolution of the Putin regime and the legal restoration of the Soviet Union. The case was the latest in a series of prosecutions targeting members of the movement, which emerged in the late 2010s. [266]
- In late January and February 2021, mass demonstrations were held in various Russian cities to protest the arrest of Aleksey Navalny. The authorities detained thousands of participants for alleged offenses that included their online activities (see B8 and C5). [267]

- In the same month, top officials in Navalny's FBK, including lawyer Lyubov Sobol and press secretary Kira Yarmysh, were detained or fined for posting calls to participate in mass protests. [268]

In March 2022, a court in Rostov-on-Don sentenced journalist Remzi Bekirov, who is a Crimean Tartar, to 19 years in prison for allegedly "organizing the activities of a terrorist organization" and "preparing to a violent seizure of power." [269] Bekirov works for Crimean Solidarity, a human rights group, and Grani.ru, an opposition site. He covered the Russian authorities' raids and arrests of Crimean Tartars and pro-Ukrainian activists in occupied Crimea, and uploaded interviews with activists of Crimean Solidarity to their YouTube channel. [270] Apart from Bekirov, the court also sentenced lawyer and human rights activist Riza Izetov and activists Shaban Umerov, Rayim Aivaziv, and Farkhod Bazarov. [271] All of them were sentenced from 15 to 19 years of imprisonment in the same case of participating in the activities of a terrorist organization.

In June 2020 and later in January 2021, the Investigative Committee charged Yuliya Tsvetkova with distribution of pornography because she posted abstract pictures of vaginas on a public VKontakte page titled "Vagina Monologues," which authorities said promoted "nontraditional sexual relations among minors" (article 6.21 of the code of administrative offenses). [272] In July 2022, after three years of litigation, Tsvetkova was acquitted of distributing and "illegally producing pornography." [273]

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**1** / 4

Score Change: The score declined from 2 to 1 to reflect the widespread blocking of VPNs during the coverage period.

Anonymous communication is restricted in Russia, as are encryption tools. During the coverage period, the Russian government went to unprecedented lengths to block VPNs. The authorities used the Technical Means of Countering Threats (TSPU) equipment (see B1), which relies on DPI technology, to restrict access to VPN services. [274] As of March 2022, approximately 20 popular VPN services had been blocked in Russia. [275]

A 2017 law mandates the blocking of VPN services that allow their clients to access banned content. [276] In March 2019, Roskomnadzor began to enforce this law for the first time, sending 10 VPN services a request to connect to the Federal State Information System—Roskomnadzor's list of banned content (see B1). [277] Most of the VPNs immediately refused, but they were not blocked. [278]

In June 2021, Russia banned the use of certain VPN services for the first time, restricting access to VyprVPN and the browser extension OperaVPN, which refused to provide its services to users located in Russia. [279] In July 2021, at the request of the Russian authorities, Google agreed to remove hundreds of thousands of links to VPN services from search results [280] over a two-year period. [281]

In September 2021, Roskomnadzor announced the blocking of six additional VPN services, including ExpressVPN and NordVPN (see B1). [282] The blocking affected sites unrelated to VPNs, including Twitch, other live-streaming platforms, and online gaming sites, due to the use of DPI technology to block certain protocols. [283] In January 2022, the authorities blocked the Tunnelbear VPN, [284] which was included in the register of prohibited sites in 2018. [285]

In May 2022, Roskomnadzor's Public council met and listed VPN services as tools in the information warfare campaign against Russia. By the end of the coverage period, the blocking of VPNs had become more effective. [286] In December 2021, Roskmonadzor ordered the blocking of Tor and blocked the service using DPI technology, but after lawyers from the digital rights organization Roskomsvoboda appealed the ruling, it was overturned in May 2022 (see B1). In July, after the coverage period, Roskomnadzor unblocked the Tor browser, [287] though a court banned Tor again in the same month.

Previously, the national security authorities initiated a campaign against encrypted email services in early 2020. Such services as SCRYPTmail.com, Mailbox.org, ProtonMail, Tutanota, and StartMail were blocked (see B1).

In February 2020, it was reported that in the summer of 2019, the FSB had sent letters to a dozen Russian online services—including Avito, Habr, and RuTube—demanding that they provide the agency with encryption keys allowing it to decrypt users' correspondence, and that they organize "around-the-clock access to their information systems." [288] Exactly how these services responded is not publicly known.

Since 2014, mobile phone subscribers in Russia have been required to register with their official state identification in order to purchase a SIM card, limiting anonymity for mobile users. [289]

A 2017 amendment to the Law on Information, Information Technology, and Information Protection requires users of social media platforms and communication apps to register with their mobile phone numbers, further restricting online anonymity. [290] In May 2019, [291] new rules requiring such platforms to verify users' phone numbers with the help of mobile service providers entered into force. [292] If a user's phone number cannot be verified, they will no longer be able to send messages. Furthermore, mobile service providers are now obliged to inform communication apps and social media platforms when users cancel their contracts. In those cases, users will no longer be able to send messages unless they reregister with a new phone number. [293] Roskomnadzor interprets the rules to apply to both foreign and domestic platforms. [294] However, as of May 2020, none of the platforms had reported compliance with the procedures for user identification.

The authorities have also sought to limit the privacy safeguards of encryption tools. The Yarovaya Law requires online services that offer encryption to assist the FSB in decoding encrypted data, including by providing encryption keys. Though this is an impossible task for many service providers, such as those that use end-to-end encryption, companies that fail to cooperate can currently face fines of up to 6 million rubles ($79,000). Fines for failure to hand over encryption keys were increased in December 2019 (see B3). The Electronic Frontier Foundation (EFF) has suggested that the impossibility of full compliance is a deliberate feature of the law, giving authorities leverage over the affected companies. [295]

In December 2021, President Putin signed a law authorizing the development of a unified biometric database. [296] Then, in July 2022, after the coverage period, the State Duma approved amendments that would allow banks to transfer clients' personal data to the system without their consent. [297] In June 2022, after the coverage, the Ministry of Digital Development announced plans to establish a single database for International Mobile Equipment Identity (IMEI) numbers for mobile phones, which could facilitate surveillance. [298]

C5 0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	1 / 6

State surveillance of internet activities greatly affects users' privacy rights, and a number of laws have increased authorities' power to conduct intrusive surveillance.

The government utilizes the System for Operational Investigative Measures (SORM) for its online surveillance activities. Under current legislation, in order to receive an operating license, ISPs are required to install equipment that allows security services to monitor internet traffic. Providers that do not comply with SORM requirements are promptly fined and may lose their licenses if problems persist. The latest version of the system, SORM-3, uses DPI technology, enhancing the ability of security services to monitor content on all telecommunications networks in Russia. The Sovereign Runet Law provided authorities with additional DPI capabilities, which were tested in late 2019 and later in the summer of 2021 (see A3). [299]

A September 2022 *New York Times* investigation of leaked data from Roskomnadzor's Bashkortostan office revealed the scope of the agency's social media monitoring activities. According to the investigation, Roskmonadzor regularly monitored Telegram chats and Instagram pages, with a particular focus on individuals who were supportive of Navalny. The agency also targeted those who played roles in organizing protests, identified individuals who ran critical accounts, and produced reports on the general reaction to political situations, including the invasion of Ukraine. [300]

Throughout the coverage period, the Russian authorities used cameras with facial-recognition software to detain people (see B8). In July 2021, the Ministry of Internal Affairs reported that more than 5,000 cameras with facial recognition capabilities were installed across the country, excluding Moscow. [301] In Moscow, as of 2020, there were 178,000 such cameras, and the government announced plans to add another 9,000 cameras in 2021. [302]

Law enforcement has used facial-recognition cameras in the Moscow metro, as well as other cameras installed across the city, to detain people, including municipal deputies. For example, in July 2021, police detained municipal deputy Yulia Shcherbakova in front of her building and falsely accused her of participating in a pro-Navalny rally based on information obtained from facial-recognition cameras. [303] In the same month, municipal deputy Volodymyr Zalishchak, who was present at the protest to

provide support to demonstrators, was detained as a result of facial-recognition technology. [304] Law enforcement officers found him based on the results of the facial recognition system, and he was arrested and detained for 15 days. In June 2022, on Russia Day, police detained 67 people who were identified by the facial-recognition system on the Moscow metro. Forty-three of the detainees were identified as protesters (see B8). [305]

In December 2019, President Putin signed a law requiring that mobile devices in Russia come preloaded with Russian software, raising privacy concerns among advocates who suspect that such software could be compromised. [306] As of April 2021, Russian smartphones have come with the predetermined Russian software after the Ministry of Digital Development, Communications, and Mass Media expanded the scope of the law. [307]

Russian authorities are nominally required to obtain a court order before accessing electronic communications. According to Supreme Court data, in 2019 security services requested 514,974 court orders to tap telephones, open letters, and intercept electronic communications; the data were not disaggregated. Of these requests, 514,115—over 99 percent—were granted. [308]

The authorities are not required to show interception warrants to service providers, and FSB officers have direct access to providers' servers through local control centers. [309] Experts note that there is no publicly available information about accountability for FSB officers who may abuse this power. [310]

In May 2019, Roskomsvoboda reported that the government was soliciting bids for a social media and news media monitoring service that would perform "sentiment analysis" of posts on platforms including Facebook, Telegram, Twitter, and VKontakte to determine whether they supported or opposed the government's positions. [311] In 2018, the government awarded a larger contract for monitoring work of a similar nature. [312]

Law enforcement agencies often conduct their own human monitoring of social media, mainly on VKontakte, the most popular social media platform in Russia, and the most cooperative with authorities. For example, in the words of one former employee at an antiextremism center, officers work proactively to "sort through shared posts on

VKontakte" and field complaints about "extremist" posts on social media from third parties. [313]

Early in the COVID-19 pandemic, the government stepped up mass surveillance of users through internet-enabled tools, but it eased these efforts starting in June 2020. [314] In addition, COVID-19 patients in Moscow who were required to remain at home were instructed to install the Social Monitoring mobile app. [315]

C6 0-6 pts

Does monitoring and collection of user data by service providers and other technology companies infringe on users' right to privacy?	**1** / 6

The legal system requires service providers and technology companies to cooperate with the government in its surveillance operations. According to the Law on Communications, service providers must grant network access to law enforcement agencies conducting search operations and turn over other information requested by the prosecutor general's office, the Ministry of Internal Affairs, the FSB, or the Investigative Committee. [316] The Law on Investigative Activities states that court orders are needed to intercept communications, although exceptions can be granted if there is an "immediate risk" that a serious crime, defined as a crime that can draw 10 or more years of prison time, will be committed or if an "immediate threat" to national security is ascertained. [317]

Under provisions of the Yarovaya Law that came into force in July and October 2018, [318] service providers and "information dissemination organizers," which includes people or entities that own a site that facilitates communications between users, are required to store the content of users' online communications—including video, text, and audio communications—for six months, while metadata must be stored for three years by service providers and one year by other entities. [319] Service providers must store users' browsing history for 30 days. [320] Companies are required to arrange a storage plan with the authorities and increase their storage capacity by 15 percent annually, beginning five years after implementation. [321] Under the law, the authorities are nominally obliged to obtain a court order to access the data.

In December 2019, it was disclosed that ISPs had purchased 10 billion rubles ($130 million) in special equipment from the state corporation Rostech in order to comply with the Yarovaya Law. [322] Previously, service providers had warned that the

legislation would impose excessive costs on them, estimating the cost could reach as high as 60 billion rubles ($790 million).

In June 2022, after the coverage period, the FSB sent letters to telecom operators demanding they provide signed SORM plans under the Yarovaya Law by the end of the second quarter of 2022. [323] In this letter, the FSB indicated that operators are required by law to organize and store text messages, voice information, video, and other data of their users. Some large operators did not initially implement the required technical measures, which prevented the FSB and other security service from collecting user data.

Due to the COVID-19 pandemic, the government in 2020 temporarily eased traffic storage requirements for service providers under the Yarovaya Law. In particular, it approved a one-year suspension of increases in traffic storage requirements and a one-year moratorium on the storage of heavy video traffic until September 1, 2021. [324] The government introduced a similar measure in March 2022, after the invasion of Ukraine.

Service providers operating in Russia typically do not disclose the scale and scope of government requests for user data. It is not clear whether they may do so under Russian law. [325]

As of January 2022, more than 300 organizations and companies were in the register of "information dissemination organizers," including social networks, communication apps, online dating services, file-sharing services, and email platforms. [326]

The data-localization law enacted in 2015 requires foreign companies that possess Russian citizens' personal data to store their servers on Russian territory (see B1), potentially enabling easier access for security services. [327] Some foreign companies, such as Uber and Viber, [328] have moved to comply with the law.

Roskomnadzor's leadership has repeatedly asserted the need to apply data-localization measures to online platforms, and it ramped up fines during the coverage period. Fines were first issued April 2019, when Twitter and Facebook were fined a token 3,000 rubles ($40) for their noncompliance. [329] Legislative amendments that were adopted in late November 2019 and signed by President Putin that December gradually increase such fines until they are large enough to affect companies' revenues without exposing their platforms to the threat of blocking. [330]

In July 2021, a court in Moscow fined Google 3 million rubles ($40,400) for refusing to localize users' data in Russia. [331] Then, in June 2022, after the coverage period, Google was fined 15 million rubles ($259,302) for repeatedly refusing to localize users' personal data in Russia. [332] In the same month, a Russian court fined Twitch, Pinterest, Airbnb, and UPS for refusing to localize Russian data. [333] The latter three companies received a fine of 2 million rubles ($34,600), while UPS was fined 1 million rubles ($17,200).

In August 2021, Meta-owned WhatsApp was fined 4 million rubles ($54,534), marking the first fine for the messaging service, while Facebook and Twitter were fined a further 15 and 17 million rubles ($204,500 and $231,800), respectively. [334] Facebook previously paid a 4 million ruble ($51,700) fine in November 2020. [335]

In 2021, Facebook received 57 requests for user information from the Russian government, but it complied with none of them. [336] Likewise, Twitter received one request for user information, but it did not comply. [337] In the first half of 2021, Google received 602 requests for user information. In the majority of cases it did not comply, but it did acquiesce 77 percent of the 65 data requests from its local subsidiary. [338] In a transparency report that covers the first nine months of 2021, Coinbase, the major cryptocurrency exchange, revealed that it received five requests from the Russian authorities to disclose information about users, marking the first time it had received such a request from the Russian government. [339]

In May 2022, the Cabinet of Ministers submitted a draft law to the State Duma that would oblige taxi-ordering services to provide the FSB with access to their databases as well as remote access to their systems. [340]

C7 0-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in relation to their online activities?	**1** / 5

Physical attacks on online activists and journalists by state and nonstate actors are relatively common in Russia, and authorities rarely conduct meaningful investigations of such incidents. Law enforcement agents also apply other forms of extralegal pressure against journalists and break into their devices. [341]

At the end of May 2021, Andrey Pivovarov, the former executive director of opposition group Open Russia, was arrested shortly after boarding a flight to Poland, over his Facebook posts. [342] He was later sentenced to four years in a penal colony (see C3).

In April 2021, the FSB conducted a night search at the house of Roman Anin, the editor in chief of independent online media outlet Vazhnie Istorii (Important Stories), in relation to a criminal case initiated in 2016. The journalist was considered a witness in the case. [343]

in October 2020, Irina Slavina, editor in chief of the Nizhny Novgorod media outlet KozaPress, publicly self-immolated in front of the regional Ministry of Internal Affairs office. She had previously been fined several times both for civic activism and for publications in her outlet. The day before the suicide, her apartment was ransacked. [344]

The authorities of the Chechen Republic routinely kidnap and torture activists. In September 2020, individuals linked to the Chechen government kidnapped Salman Tepsurkayev, a teenage activist who frequently moderated the critical 1ADAT Telegram channel. A video that appeared on the internet after he was kidnapped showed Tepsurkayev, who was clearly under duress, torturing himself. [345] Elena Milashina, a Russian journalist working for *Novaya Gazeta*, has also regularly faced death threats for her coverage of human rights issues in Chechnya. Most recently, in April 2022, Ramzan Kadyrov, the head of the Chechen Republic, issued a death threat to Milashina after she wrote about the Chechen government's efforts to prevent people with COVID-19 from receiving medical care. [346] In February 2022, Milashina fled the country following an investigation she conducted on Chechen government officials who threatened a judge, which led Kadyrmov to label her a "terrorist." [347]

In the fall of 2019, investigators who initiated a criminal case against Pskov journalist Svetlana Prokopyeva for alleged justification of terrorism hacked her iPhone, which they had previously seized during a house check. According to Prokopyeva, investigators looked at her correspondence in messaging apps, trying to interpret her messages as attempts to bribe criminal experts. [348] In July 2020, a court found Prokopyeva guilty and fined her 500,000 rubles ($6,600). [349]

Online intimidation and physical violence against LGBT+ people has escalated since the adoption of the 2013 law banning so-called propaganda of nontraditional sexual

relations to minors. [350] In July 2019, LGBT+ activist Yelena Grigoryeva was stabbed to death in Saint Petersburg after her name was included on a "death list" circulated on the internet by an anti-LGBT+ group called Saw. [351]

In the summer of 2021, Russian businesses faced persecution for supporting the LGBT+ community and promoting diversity in their marketing materials. [352] Tanuki and Yobidoyobi, two Japanese restaurant chains, as well as VkusVill, a chain, received threats from "Male State," a movement promotes the ideas of patriarchy, racism, and nationalism in Russia, after the companies posted in support of diversity on social media. Male State demanded an apology and the removal of the social media posts promoting diversity. Vladislav Pozdnyakov, the head of the organization, urged his supporters to leave negative reviews, create fake orders, and write threats to the authors of these publications. The websites of the victims were subjected to Distributed Denial of Serbice (DDoS) attacks. An LGBT+ family that was featured in an advertisement for VkusVill was forced to leave the country due to threats. [353] The police did not take any action, despite appeals from businesspeople. [354]

C8 0-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	**0** /3

Cyberattacks against independent media and civil society organizations continue to inhibit users' ability to access these resources. Following the Kremlin's invasion of Ukraine, state websites faced several significant cyberattacks.

After Russia invaded Ukraine in February 2022, cyberattacks against state and state-affiliated websites increased dramatically. At the end of February 2022 hacking group Anonymous claimed responsibility for cyberattacks that displayed antiwar messages on the websites of the Russian government, Roskomadzor, and other state entities, as well as state-affiliated media outlets including RT, TASS, and *Kommersant*. [355] Following the first week of Anonymous' campaign, more than 2,500 Russian- and Belarusian-linked websites faced cyberattacks. [356]

By February 26, 2022, Gosulugi, a website Russians use to access public services, experienced more than 50 debilitating cyberattacks. In March 2022, the website of the Emergency Situations Ministry faced a cyberattack that replaced the websites home

page with a number Russian soldiers who wish to defect could call. At the same time, a number of judicial websites were hacked to display insults towards President Putin. [357] In May 2022, RuTube, Russia's alternative to YouTube, suffered a hacking attack and was offline for three days. In June 2022, after the coverage period, the Russian Ministry of Construction, Housing, and Utilities' website was hacked to display a message in support of Ukraine. [358]

Following the Russian invasion of Ukraine, Ukrainian hackers formed an "IT Army" and launched DDoS attacks on Russian websites. The group of hackers targeted a range of companies and government agencies and issued instructions and updates via Telegram. [359]

Private companies also faced significant cyberattacks. In March 2022, personally identifiable information about 58,000 customers of Yandex.Eda, Yandex's food delivery application, and customers of Delivery Club, a rival, were leaked. In May, users' personal data from a number of private companies, which the government refused to name, also leaked online. [360]

In April 2022, in response to the barrage of attacks on government websites and private companies, Roskomnadzor announced plans to create a national system for protecting online resources from DDoS attacks originating from abroad. [361] To do this, Roskomnadzor intends to upgrade its Deep Packet Inspection (DPI) equipment, which is also used to block websites and enforce the law on the sovereign Internet. [362]

Government-backed organizations allegedly engaged in coordinated attacks on digital media. For example, in late January 2021, the social media accounts of many opposition-oriented outlets faced massive bot attacks, which temporarily prevented them from functioning. [363]

In April 2021, registered users on Freenavalny.com, a website launched in March 2021 to help coordinate protests, started receiving emails containing their personal information from unknown accounts. The perpetrators may have correlated the email addresses from the hacked database with other personal details available on Russia's extralegal information market. [364] Subsequently, some of the users were fired by their employers (see B8). [365]

Journalists and civil society activists have been notified of attempts in recent years to compromise their online accounts, including on Telegram and Gmail, suggesting a coordinated campaign to access their data.

Footnotes

1 International Telecommunication Union (ITU), "Statistics, Percent of Individuals Using the Internet," accessed September 2022, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

2 Economist Impact, "The Inclusive Internet, Russia 2022," accessed September 2022, https://impact.economist.com/projects/inclusive-internet-index/2022/cou....

3 Economist Impact, "The Inclusive Internet, Russia 2022," accessed September 2022, https://impact.economist.com/projects/inclusive-internet-index/2022/cou....

4 International Telecommunications Union, "Statistics," "Mobile Broadband Subscriptions, accessed August 2022," https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

5 Economist Impact, "The Inclusive Internet, Russia 2022," accessed August 2022, https://impact.economist.com/projects/inclusive-internet-index/2022/cou....

More footnotes

On Russia

See all data, scores & information on this country or territory.

See More ›

Country Facts

Global Freedom Score

19 /100 **Not Free**

Internet Freedom Score

23 /100 **Not Free**

Freedom in the World Status
Not Free

Networks Restricted
No

Social Media Blocked
Yes

Websites Blocked
Yes

Pro-government Commentators
Yes

Users Arrested
Yes

In Other Reports

Freedom in the World 2022

Other Years

2021

Be the first to know what's happening.

Join the Freedom House weekly newsletter

Subscribe

ADDRESS

1850 M St. NW Floor 11
Washington, DC 20036
(202) 296-5101

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org