Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**801**
Land:	Rusland
Kilde:	Freedom House
Titel:	Russia - Freedom on the Net 2023
Udgivet:	4. oktober 2023
Optaget på baggrundsmaterialet:	12. januar 2024

Freedom House

FREEDOM ON THE NET 2023

Russia

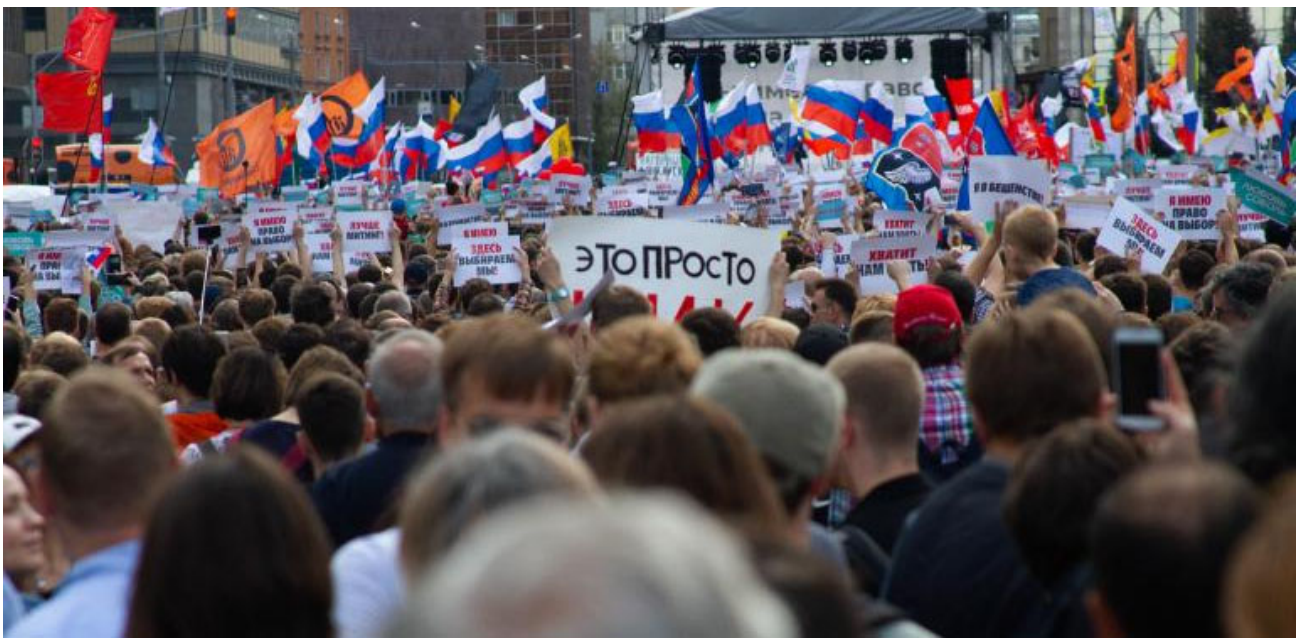
NOT FREE

21
/100

A. Obstacles to Access	10 /25
B. Limits on Content	5 /35
C. Violations of User Rights	6 /40

LAST YEAR'S SCORE & STATUS
23 /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

Internet freedom in Russia continued to plummet during the coverage period, as the government implemented even more restrictive laws to control the information space and sought to eliminate criticism of the full-scale military invasion of Ukraine. Authorities continued to block prominent social media platforms, including Facebook, Instagram, and Twitter, and issued fines to other platforms that refused to remove content and localize user data. The government further expanded the "foreign agents" law, broadening the definition to effectively include anyone and enabling the Ministry of Justice to block the websites of designated foreign agents without a court decision. The Ministry of Justice also began adding news outlets and civil society organizations to the list of "undesirable organizations," criminalizing participation in or support of them. Authorities also employed March 2022 measures that outlaw "discrediting" or "knowingly spreading false information" about the military to imprison people who criticized the Ukraine invasion on online news sites or social media.

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, 2022 - May 31, 2023

- The government introduced laws that oblige telecommunications operators to work more closely with the Federal Security Service (FSB); introduced fines for operators that refuse to install the Technical Measures to Combat Threats (TSPU) system, which facilitates website blocking and surveillance; and increased fines for those that had not yet installed surveillance tools required for a systems of operational-search activities (SORM) program (see A4 and C6).

- According to Roskomsvoboda, a digital rights organization, the government blocked over 247,000 web pages in 2022, including websites of Russian news outlets, foreign news outlets, human rights organizations, and LGBT+ sites, among others (see B1).
- Throughout the coverage period, Roskomnadzor, the media regulator, issued fines to social media platforms that refused to remove content and localize user information (see B2 and C6).
- New legislation expanded the scope of the "foreign agents" law, allowing the government to list anyone deemed to be "under foreign influence" as a foreign agent. Additionally, the Ministry of Justice began adding civil society organizations and news outlets, including the independent online news outlet Meduza, to the list of "undesirable" organizations, effectively criminalizing them (see B4 and B6).
- Individuals and journalists who criticized the Russian military were sentenced to prison and fined for violating 2022 amendments to the Criminal Code and Administrative Code, which prohibit "discrediting" or "knowingly spreading false information about" the military. For instance, Ilya Yashin, a politician, was sentenced to eight and a half years in prison in December 2022 for sharing a YouTube video about atrocities committed by the Russian military in Bucha, a city in Ukraine's Kyiv Oblast (see C3).
- Investigations based on leaked data from Roskomnadzor revealed the extent to which government agencies monitor individuals' social media activity for the purpose of cracking down on opposition, and the automated systems they deploy to detect critical content (see C5).

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 90.2 percent of the population in 2021. [1] According to 2021 data from the ITU,

there were 23.7 fixed-broadband subscribers per 100 inhabitants, [2] and 107.6 mobile broadband subscribers per 100 inhabitants. [3]

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. [4]

Most of the population has access to third generation (3G) and fourth generation (4G) technology for mobile networks. The Inclusive Internet Index noted 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] However, the authorities reduced funding for the frequency conversion of 5G networks from 43 billion rubles ($704 million) to 7.85 billion rubles ($130 million) for the period up to 2024, which could have adverse effects for the Rostec plan. [8] 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, have also impacted the launch of 5G. [9] In December 2022, the government announced that it would develop future 4G and 5G networks exclusively on Russian equipment; it set a goal of 6 million people having access to domestically produced 4G networks by 2025, and 300,000 having access to domestically produced 5G networks in 2024. [10]

Connection speeds are stable, with median fixed-broadband download speeds at 79.93 Mbps and median mobile internet download speeds at 25.36 Mbps, according to May 2023 data from Ookla's Speedtest. [11]

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

The impact of the Russian invasion of Ukraine and the ensuing sanctions continue to affect the cost of internet access. In 2022, telecom operators and internet providers in Russia increased the monthly cost of home internet plans by 2 to 10 percent, depending on provider. [12]

According to 2022 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 0.7 percent of GNI per capita. [13]

The growing cost of internet access 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 (the Russian segment of the internet). [14] 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. [15] 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 would be suspended. However, this moratorium ended in 2023.

In March 2023, the State Duma adopted a law that obliges owners of technological communication networks with autonomous system numbers to store user data for three years (see C6), which could further raise costs for users. [16]

At the end of 2022, analysts predicted an increase in the cost of home internet in 2023, [17] largely due to the departure of international suppliers from the Russian market and the increased cost of telecom equipment. In January 2023, Moscow-

based fixed-line broadband providers increased the cost of monthly plans by 5 to 10 percent. [18]

In July 2021, President Vladimir Putin signed a law on free access to socially significant websites, [19] 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.

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. [20] By 2023, operators no longer offered unlimited internet plans, though some offer unlimited plans exclusively for messaging.

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. [21] 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

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

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 Measures to Combat Threats (TSPU) equipment, which is based on the use of Deep Packet Inspection (DPI) technology on telecommunications networks, allows Roskomnadzor to restrict access and block websites. A November 2022 report from University of Michigan's Censored Planet project and Arizona State University [22] identified 6,000 TSPU devices, which are produced by Roskomnadzor, on Russian networks. In contrast to China's Great Firewall, the researchers have noted that the TSPU is "a model of decentralized deployment, centralized control" because Roskomnadzor is able to use these devices to block websites unilaterally across a range of networks.

In July 2022, Putin signed a law that introduces fines for telecom operators that have not installed TSPU, [23] and in July 2023, after the coverage period, Roskomnadzor announced that it would start issuing these fines (see A4). [24] The authorities explain the need to use this equipment for censorship by the presence of "information threats to Russians." In January 2022, VPN users from several Russian regions reported problems connecting to VPN services, [25] which may indicate that protocol blocking is being tested within TSPU.

In November 2019, a law aimed at achieving the "sovereignization" of the Russian segment of the internet, or Runet, [26] took effect. 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 full-scale Russian military invasion of Ukraine in February 2022, the Russian government restricted access to some social media platforms (see B1). In March 2022, 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. [27] Later in the month, Roskomnadzor blocked Instagram, after giving users a 48-hour warning. [28] In March 2022, a court in Moscow approved a request by the Prosecutor General's Office to recognize Meta, the parent company of Facebook and Instagram, as an "extremist organization." [29] The request was filed after Reuters published an article about Facebook's decision to temporarily permit posts containing death wishes or calls for violence against Putin, Belarusian president Alyaksandr Lukashenka, and the Russian military to remain on its platform. [30]

In March 2021, Roskomnadzor used its DPI equipment to throttle the loading speeds for Twitter in order to punish the platform for what the regulator 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. [31] From 2018 to 2020, the government ordered the blocking of Telegram, a popular messaging application, but it was never fully implemented.

Throughout June and July 2021, the Russian government began to test the feasibility of cutting the RuNet off from the global internet, and Russian state-affiliated media reported the tests were successful. [32] 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). [33] 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. [34]

In June 2023, after the coverage period, the government announced plans to launch a "secure internet," which will be available only to citizens of the country who register with their passports (see C4). [35] According to Andrei Svintsov, the Deputy Chairman of the State Duma Committee on Information Policy, Information Technologies and Communications, users will only be able to access

websites and services that fully comply with existing Russian legislation, though it will not replace the existing internet. [36]

In July 2023, the government ran a test exercise to disconnect itself from the international internet. The government reported that the test was successful, though many international websites and government websites were inaccessible during the two-hour test. [37]

In April 2023, Radio Free Europe/Radio Liberty (RFE/RL) reported that Russian and Chinese officials had shared censorship strategies, with Russian officials aiming to learn how to more effectively restrict VPNs and censor messaging applications. [38]

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, [39] and intentional shutdowns were used separately in the Republic of Ingushetia to stymie mass protests there in 2018–19. [40]

A4 0-6 pts

Are there legal, regulatory, or economic obstacles that restrict the diversity of service providers?	**1** / 6

Score Change: The score declined from 2 to 1 due to the introduction of onerous obligations that threaten to limit the diversity of service providers, including measures requiring operators to obtain approval from the Federal Security Service (FSB) before launching a network.

The ICT market in Russia is relatively concentrated due to regulatory and economic constraints. The displacement of local service providers by larger companies, and several 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. [41] 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). In July 2023, Roskomnadzor

announced that it would begin fining providers who do not install the TSPU system between one and five million rubles. Additionally, directors of these companies can face up to three years in prison and their companies can be audited if they refuse to install this equipment. [42]

In the second quarter of 2022, the four largest internet service providers—Rostelecom (35 percent), MTS (12 percent), ER-Telecom (11 percent) and Vimpelcom (9 percent)—accounted for 67 percent of the subscriber base of broadband internet access in the business-to-consumer segment in Russia, according to TMT Consulting. [43]

In June 2022, law enforcement reportedly announced they would not allow the companies Antares, Integral, and Arctur to use 1900-1920 MHz frequencies. They had planned to use the frequencies to launch a new telecommunications operator. [44]

In the same month, the Ministry of Digital Development proposed three packages of amendments that could lead to further market concentration. The first one, which came into effect in May 2023, introduces fines for operators that do not install the systems of operational-search activities (SORM), which allows the government to conduct surveillance (see C5). [45] The proposed fines initially ranged from 0.01 to 0.05 percent of the annual revenue for communication services, but could not 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 ($75 to $13,400). [46] 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, the Ministry of Digital Development finalized the fine scheme, establishing a fixed fine for the first offense and reducing the fines for repeated offenses. [47]

In January 2023, the state duma passed a bill implementing the Ministry of Digital Development's guidelines I that would increase the fee for telecommunications operators to obtain a license from 7,500 rubles to 1 million rubles beginning in 2024. [48] The telecom operator must work with the FSB to build a plan for the

implementation of SORM within six months of receiving a license. Roskomnadzor is tasked with monitoring operators' compliance with the measures. [49]

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). [50] Roskomnadzor's blocking procedures are not transparent. Often, access restrictions are implemented in violation of procedural rules, including blocking of 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. [51]

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, [52] was formed within the agency as part of the legislation. [53] 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. [54]

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. [55]

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. [56]

There are several 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

Following 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, as well as international news sites, civil society websites, and Ukrainian news sites. In 2022, Roskomsvoboda reported that 247,000 webpages were blocked, including 9,000 that were blocked under military censorship since the start of the full-scale invasion. [57] A February 2023 report published by the Open Observatory of Network Interference (OONI) and Roskomsvoboda found that in 2022, Russian government agencies had blocked 494 website domains in 2022. [58]

Between the start of the invasion and April 2022, the Russian government blocked social media platforms including Facebook [59] and its messenger, Twitter, [60] and Instagram (see A3).

In a first wave of blocking at the end of February 2022, authorities blocked media sites including the Russia-based student magazine DOXA, [61] the BBC, Voice of America, Deutsche Welle, Bellingcat, Paper, Meduza, Mediazona, Interlocutor, RFE/RL, Echo of the Caucasus, Republic, Taiga.Info, 7x7 Horizontal Russia, and the

Village, among many others. Authorities 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). [62] At the end of March 2022, 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," though access was later restored. [63]

The authorities have also blocked well-known Ukrainian news sites. Prior to the invasion, the Prosecutor General's Office had ordered the blocking of popular Ukrainian internet television channel Hromadske (Public) for posting "extremist" information. [64] 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. [65]

During the coverage period, government agencies continued to issue blocking orders, often because the targets allegedly spread false news about the invasion. In 2022 Roskomnadzor blocked Nuntiare et Recreare, a website dedicated to LGBT+ members of various religious affiliations, and the site of the Museum of LGBT History in Russia. [66] In December 2022, Putin signed a law expanding the scope the ban on LGBT+ propaganda in Russia (see B3), which prevents this material from being promoted to adults in addition to children (see B3).

In August 2022, Roskomnadzor began blocking Patreon. In September 2022, Soundcloud was added to the blocklist for hosting "false information" because the website hosted Radio Svoboda, RFE/RL's Russian-language program. [67] In the same month, the Prosecutor General's Office also ordered the blocking of Grammarly, which uses artificial intelligence to edit texts users submit to the platform. Grammarly was founded in Ukraine, had donated revenue earned from business in Russia and Belarus to Ukraine, and had developed a feature urging users to support Ukraine. [68] Russian authorities claimed they blocked the website because it was spreading false news about the invasion. [69] Roskomnadzor also blocked the True Story, a prodemocracy news website created by the former head of Yandex.News, in August. [70]

In January 2023, Amnesty International's website was also blocked. [71] In the same month, Roskomnadzor blocked the websites of the United States' Central Intelligence Agency (CIA), Federal Bureau of Investigations (FBI), and "a number of resources belonging to state structures of hostile countries for disseminating material aimed at destabilizing the social and political situation in Russia." [72] Roskomnadzor alleged that the CIA and FBI had published false information about the invasion.

In February 2023, the government blocked access to the Bell, a prominent online news outlet. [73] In February and March 2023, Roskomnadzor began blocking several images from stock photograph websites Alamy and Depositphotos photo stocks because of photos suggesting acts of suicide. [74] The Shutterstock photo stock was also blocked, but access to it was later restored.

In June 2023, after the coverage period, an unspecified government agency ordered the blocking of Medium, the blogging platform, and it was included in the register of prohibited information. [75] Later, Roskomnadzor explained the blocking was due to the failure to remove unreliable materials about the invasion. In the same month, several ISPs and telecommunications once again blocked Google News, as Yevgeny Prigozhin, leader of the Russian paramilitary Wagner Group, and Wagner Group fighters marched toward Moscow. [76] Later in the month, Roskomnadzor blocked online news websites linked to Prigozhin, including RIA FAN, Politics Today, Economy Today, Neva News, and People's News. [77]

In the same month, Roskomnadzor blocked the website of the environmental organization Greenpeace, which had been listed as an "undesirable organization" in May (see B6). [78]

In September 2023, Roskomnadzor blocked access to the Kyrgyzstan-based news outlet 24.kg and the Tajikistan-based outlet Payom because of their coverage of the war in Ukraine. According to digital rights organization Roskomsvoboda, Roskomnadzor initially ordered the blocking of four 24.kg articles and two Payom articles in November 2022 and May 2023, respectively. 24.kg reported that it had received takedown requests from Roskomnadzor throughout the coverage period. During the coverage period Roskomnadzor also issued takedown orders to outlets based in Kazakhstan (see B2). [79]

Though blocked websites can be accessed via a virtual private network (VPN), Roskomnadzor blocks several VPN services (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, [80] Speedify, Tachyon VPN, VyprVPN, and X-VPN. [81]

In June 2022, Proton VPN and NordVPN users reported problems accessing services. Later, Roskomnadzor confirmed that it had restricted access to Proton VPN and several other VPNs, the names of which were not announced. [82] At the end of May 2023, VPN users reported that the OpenVPN protocol, which several VPNs rely on, was blocked. The protocol is used by banks and other private companies in Russia. [83] In June, after the coverage period, the number of complaints about blocking decreased (see C4). [84] However, in August 2023, reports emerged that Open VPN and Wireguard, another VPN protocol, were blocked by major mobile operators. [85]

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. [86] 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. [87]

At the next meeting later in May, the prosecutor's office demanded that the court bring Google into the case as an interested party. [88] 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. Between July 15 and 29, 2022, the Tor project website was unblocked for a brief period before it was once again added to the list of blocked resources, [89] when a court banned Tor with no representatives from the Tor Project present. [90] In December 2022, the Court of Appeal upheld the decision of the previous court to block the Tor Project website, as well as the Tor browser on Google Play. [91]

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. [92] 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 [93] and DropmailC [94] 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. [95] 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. [96]

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, [97] the Prosecutor General's Office, [98] 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. [99]

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. [100]

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

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. However, many of the platforms that Roskomnadzor regularly issued demands to are now blocked (see B1). Historically, when companies have refused to comply, the courts have issued escalating fines. Prior to the invasion, the Russian government had already attempted to compel social media platforms to remove content. These companies' decision to restrict access to Russian state media outlets in the European Union (EU) and elsewhere, however, led to their outright 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.

The Kremlin continued to issue fines to Alphabet, Google's parent company. In May 2023, a court fined Alphabet 3 million rubles ($38,600) because YouTube had failed to remove content promoting LGBT+ information as well as news about the Russian military's invasion of Ukraine. [101] In July 2022, the Moscow-based Tagansky District Court issued a fine of 21.1 billion rubles ($350 million) to Alphabet for failing to remove content. [102] The court order specifically referenced YouTube's

refusal to remove "fake" news about the war in Ukraine. [103] In May 2022, Google's Russian subsidiary filed an application for bankruptcy to a Moscow court, [104] prompting Russian authorities to seize the company's bank account. [105] 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. [106] 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.

In 2021 [107] and 2022, [108] the Russian government fined Alphabet 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.

The courts and Roskomnadzor have also issued lesser fines and took other restrictive measures against online platforms. Amazon and its subsidiary, the live-streaming service Twitch, were fined during the coverage period for failing to remove content. In January 2023, a Moscow court fined Twitch 4 million rubles for failing to delete information about Russia's full scale invasion of Ukraine. [109] In October 2022, Amazon was fined 4 million rubles for failing to remove content about suicide and drugs. [110] In October 2022 and August 2022, Twitch was fined 4 million and 3 million rubles, respectively, because it refused to delete a video interview with Oleksiy Arestovych, who was an adviser to the president of Ukraine at the time. [111] In August, Twitch was fined 2 million rubles for failing to remove allegedly false information about the invasion. [112]

Roskomnadzor has also issued fines against the video-sharing platform TikTok. In October 2022, the platform was fined for refusing to remove "LGBT propaganda." [113] In August 2022, Roskomnadzor fined TikTok because the platform did not take down "prohibited information," though the agency did not specify the information. [114] 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). [115] TikTok also received fines earlier in 2022, during the previous coverage period. In April 2022, the company was also fined 2 million rubles for failing to remove content promoting "homosexual relations." [116]

The courts continued to fine messengers for not deleting "fake information about the special operation." In June 2023, after the coverage period, the Viber messenger was fined 1 million rubles for not removing false information about the invasion and Telegram was fined 4 million rubles for the same reason. [117] In August 2022, a Moscow court fined Telegram 11 million rubles because it did not remove content about the invasion. [118]

Smaller platforms, including Pinterest and Discord, as well as the video-conferencing platform Zoom were also fined in August 2022, for failing to remove "prohibited information." [119]

The Russian government also continued to force nonprofit content hosts to remove content during the coverage period; as of April 2023, it had issued seven fines totaling more than 8 million rubles to the Wikimedia Foundation, the nonprofit that oversees the Wikipedia and Wikimedia projects. In April 2023, a court in Moscow issued a 2 million ruble fine against the Wikimedia Foundation for failing to remove content about the 40th Engineer Regiment from Wikipedia because the page allegedly gave away compromising information about the unit. [120] Earlier in April 2023, the government fined Wikimedia 800,000 rubles for refusing to remove material about a banned song by the Psyche, a Russian alternative rock band, [121] and another 800,000 rubles for refusing to remove a video in which a person rides on the roof of a freight train car. In August 2022, Wikimedia was fined for refusing to remove "inaccurate information about the special operation in Ukraine," then in February 2023 it was fined for refusing to remove articles about military units of the Russian Federation. [122]

In April 2022, a court in Moscow fined the Wikimedia Foundation, 3 million rubles for not removing six Wikipedia articles about the actions of the Russian army during invasion of Ukraine, upon Roskomnadzor's request. [123] 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 for failing to remove other articles about the invasion. [124] In June 2022, 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." [125]

In May 2022, Roskomnadzor also issued a 4 million ruble administrative fine against the Internet Archive, an American organization that preserves online content, because of its refusal to remove content prohibited in Russia. [126]

In September 2022, Apple removed VK from its app store to comply with sanctions issued by the United Kingdom. [127]

Russian search engines and platforms also routinely remove content, including content related to the war. A July 2023 report from the University of Toronto's CitizenLab found that the takedown orders issued to VK, which is effectively owned by the state through Gazprom and Sogaz, had increased by 3,000 percent since the start of the invasion. Additionally, the report found that VK, blocked 94,942 videos, 1,569 community accounts, and 787 personal accounts in Russia, [128] including a significant amount of content related to the invasion, Belarusian issues, and LGBT+ terms. Likewise, leaked source code from Yandex revealed the search engine prevents search terms that are critical of Putin from leading users to images of him. The leaked code also showed that when users search the symbol "Z," the search engine hides terms associated with Nazism. [129]

After the Russian government launched its full-scale invasion of Ukraine, Russia-based search engines, including Yandex, Mail.ru and Rambler, no longer provided links to blocked websites (see B1) in their search results. [130] Yandex had previously confirmed that it filters search results based on Roskomnadzor's list of blocked websites. [131] 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." [132]

In December 2022, a law banning LGBT+ "propaganda" came into force (see B1), and in 2023, the authorities began issuing administrative protocols for demonstrating and promoting "nontraditional sexual relations" in films and television shows. In the second quarter of 2023, 33 protocols were issued against Russian online movie and television broadcasters, including Megafon TV, Start, More.tv, Ivi, Beeline TV, TV-3 Russia and TNT Music. [133]

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). [134] Outlets including *Novaya Gazeta*, the Bell, Republic, and others complied.

During the coverage period, Roskomnadzor ordered outlets based in Kazakhstan and Kyrgyzstan to remove content, in some cases blocking them when they did not comply (see B1).

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. [135] Police officers also reportedly showed up to Google's offices and pressured them to remove the application. [136] Throughout 2021, Roskomnadzor issued fines to several platforms for refusing to remove smart voting content [137] and demanded that platforms block accounts of people associated with Navalny. [138] Additionally, in April 2022, YouTube restricted access to an antiwar song at the request of Roskomnadzor. [139]

According to Google's transparency report, Russian government agencies issued a record 36,117 requests to remove 214,717 pieces of content in the second half of 2022, primarily because the content threatened "national security." Google complied with 33 percent of these requests. In the first half of the year, Russian government agencies issued 21,841 requests concerning 244,282 pieces of content and Google removed 27.3 percent of them. Russian law also mandates that search engines, including Google, delete material that is illegal in Russia. In the second half of 2022, government agencies made 130 requests to deindex 717,893 URLs, and Google removed 53.3 percent of them. In the first half of the year, government agencies issued 225 requests for deindexing concerning 682,612 URLs, and Google removed 61.3 percent of them. [140]

According to Facebook's transparency report, between January and June 2022, the company restricted access to 1,723 items at the request of Roskomnadzor for allegedly violating local laws related to dangerous content for minors, 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. [141]

X, formerly known as Twitter, did not produce a transparency report covering the reporting period. [142]

According to Reddit's transparency report, in the second half of 2022, the company received 37 content-removal requests from the Russian government concerning 42 pieces of content and complied with 72 percent of them. [143]

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. Between January and June 2022, Yandex removed 149,364 links based on requests from Roskomnadzor. Meduza, the independent online media outlet, also produces a rolling transparency report, detailing all the instances in which authorities requested content removal. [144] Most such requests concern the actions of the Russian military in Ukraine and investigations on government corruption.

In 2020, VK debuted an algorithm that automatically removes images included in the federal list of extremist materials from users' posts. [145]

The Kremlin has announced plans to further automate content removal. In February 2023, the General Radio Frequency Center (GFRC), a subsidiary of Roskomnadzor, began internal testing of the Vepr system, which is designed to "search for and neutralize information bombs." [146] The system aims to resist information "which creates a threat of harm to the life and/or health of citizens and property or the threat of a mass violation of public order and/or public safety." Testing of the new system is scheduled for the end of 2023. [147]

In February 2023, the GFRC announced that the Oculus system (see C5), a surveillance tool, can allegedly identify information in images or videos that violates Russian law, which could lead to further content removal. [148]

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, which along with the judiciary typically handles blocking orders from other agencies; as well as 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). [149] December 2022 amendments to the foreign agents law (see B6) empowered the Ministry of Justice to order Roskomnadzor to block websites without obtaining a court order. [150] In June 2023, after the coverage period, the Ministry of Justice itself began blocking websites, even though no law supports the practice. [151]

Empowered state 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. In November 2022, entries began to appear in the blocking registry without indicating the authority that demanded a site to be blocked, which had previously been standard practice. [152]

In November 2019, Putin signed a law that extended the state's regulation of media outlets designated as "foreign agents" to include individuals who "spread information to an unrestricted number of persons, namely on the internet, and receive funding from abroad." [153] 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. [154]

In December 2022, Putin signed a law banning "LGBT propaganda," adding the term to the list of information that is illegal to distribute online (see B1 and B2). [155] This includes information promoting "nontraditional sexual relations," and transgender identity alongside acts like pedophilia. The law, which expands on a 2013 law "propaganda of nontraditional sexual relations" among minors, gives Roskomnadzor the authority to order the blocking of the websites or the removal of content.

In August 2022, the Ministry of Digital Transformation released a proposal empowering Roskomnadzor to block mirrors of previously blocked sites. [156] The decree came into effect in March 2023 and will be valid for 6 years.

In 2021, 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. Amendments signed the same year allow prosecutors' offices to force websites to remove "defamatory information" within a certain time period and to block those websites if they fail to comply. [157] Also in 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. [158]

Search engines and VPNs must connect to Roskomnadzor's list and filter their services accordingly, under Law 276-FZ, which was enacted in 2017. [159]

In February 2022, the Ministry of Internal Affairs determined a mechanism for blocking websites containing personal data of persons under state protection. [160] Roskomnadzor was recognized as responsible for entering such sites into the register of prohibited sites, which will be obliged to make an appropriate entry in the register within 24 hours from the date of receipt of the decision to recognize the information as prohibited and the decision to restrict access to it.

Restrictions on online content are generally implemented opaquely. The official website listing prohibited information resources does not list all sites that are

prohibited in practice.

Roskomnadzor can issue warnings to organizations officially designated as mass media if they are deemed to abuse their position. [161] 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.

In 2020 and 2021, President Putin signed laws that placed pressure on social media platforms and websites (see B2). [162] In July 2021, Putin signed a law obliging foreign tech companies with more than 500,000 Russian users to open representative offices in Russia. [163] Foreign companies face a variety of penalties for noncompliance with the physical-representation requirement, which took effect in 2022, including a ban on search results, restrictions on accepting payments from Russian residents, complete blocking, [164] and fines of up to 20 percent of their annual Russian income. [165] Under another measure, companies also must register with Roskomnadzor and add an electronic form on their website to facilitate feedback from Russian citizens or organizations. [166] By February 2022, Apple, Spotify, Viber, Tiktok, Likeme, and Twitter had announced that they were taking measures to comply with the measures. [167] However, many of these companies later withdrew from the Russian market following the invasion of Ukraine.

In March 2021, Putin signed a law empowering the Central Electoral Commission and regional electoral commissions to send content removal requests to Roskomnadzor. The law increased fines for illegal electoral campaigning to as much as 500,000 rubles. The most obvious target of these amendments was the Smart Voting website launched by Navalny's organization. [168]

In February 2021, a law took effect compelling 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" (for example, online gambling, illicit sales, material that disrespects society or the state, among others) 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. [169]

In December 2020, Putin signed a law prescribing fines for failure to remove content banned by Roskomnadzor. 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. [170]

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 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)." [171]

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 (ECHR), [172] and it was expelled from the body a day later. Previously, site owners could appeal blocking orders implemented under local laws to the ECHR under Article 10 of the European Convention on Human Rights. However, a 2015 law had given the Russian government the right to ignore ECHR rulings. [173]

In June 2022, the Russian State Duma adopted a package of bills on the nonenforcement of decisions of the ECHR in Russia. [174] In particular, Russia refused to comply with decisions of the ECHR that entered into force after March 15, 2022, the day the government filed its application to withdraw from the Council of Europe (see C1). Also, the bill stipulates that fines the government must pay under ECHR decisions prior to March 15 will be made only in rubles and only to accounts in Russian banks. [175] In addition, the ECHR will no longer have the authority to review the decisions of Russian courts.

Russians can still apply to the ECHR if it concerns violations that occurred before this date. In the case of the slowdown of Twitter traffic in 2021, a class action complaint was previously filed in Russian courts. Now, after the refusal in all Russian courts, lawyers, together with the applicants, are preparing a complaint to the ECHR. [176]

B4 0-4 pts

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

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. [177] 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, several 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. [178] Though the media outlet planned to continue reporting on other matters, on March 28, 2022, the newspaper received an order from Roskomnadzor to stop publishing until the end of the "special operation on the territory of Ukraine." [179] The outlet's media license was later revoked (see B6).

In another instance, the editors of the Bell, an online media outlet that was later blocked (see B1), decided to completely stop covering the war because "personal risks to journalists have significantly increased." [180] 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." [181] It's My City, another online media outlet, took similar actions. [182]

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). [183]

The foreign agents law (see B3 and B6), which requires certain media outlets and individuals to identify themselves as "foreign agents," also contributes further to self-censorship. Additionally, in 2022 and 2023, the government added news organizations, including Meduza and Bellingcat, to the list of "undesirable organizations," which means anyone who collaborates with these organizations can be fined 300,000 rubles or sentenced to prison for up to 6 years (see B6). [184]

The authorities have used various drug-related charges as pretexts to censor the news media. [185] In December 2020, [186] 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. [187] 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. [188]

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 continued to 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). [189] The Russian government adopted the letter "Z" as a symbol of its war in Ukraine and promoted it through social media. [190]

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. [191] In March 2022, state-linked actors and outlets intensified their promotion of an existing narrative that the United States was developing biological weapons in Ukraine. [192]

The messaging application Telegram has become increasingly popular since the invasion (see B7) and according to an October 2022 study from the Atlantic Council's Digital Forensic Research Lab, 9 of the 10 most popular "political" Telegram channels in Russia spread Kremlin propaganda (see B5). [193]

Social media platforms based outside of Russia continue to identify and remove state-linked disinformation networks. Meta's adversarial threat report for the second quarter of 2023 shed more light on a disinformation campaign dubbed "Doppelganger." The Doppelganger campaign, a term coined by the EU Disinfolab, [194] initially targeted the United Kingdom and countries in the European Union, mimicking popular news outlets in those countries. The campaign, which later expanded to target entities in the United States and Israel, shares original articles, videos, and memes, that spew disinformation about the Kremlin's invasion of Ukraine on a host of social media platforms and messengers. Recently, the campaign has engaged in less sophisticated operations with higher volume, though Meta noted that the spoofed websites themselves are fairly sophisticated. In September 2022, Meta announced it had removed 1,633 accounts, 703 Pages, one Group and 29 accounts on Instagram that were part of the Doppelganger campaign, and later linked the project to two Russian companies, Structura National Technologies and Social Design Agency. [195] Meta's adversarial threat report for the second quarter of 2022 also noted that the two largest operations concerning the war in Ukraine were linked to two private actors, including Yevgeny Prigozhin. [196]

in March 2022, online media outlet Fontanka reported that the Cyber Front Z Telegram channel had recruited people en masse to write comments in support of the actions of the Russian army. [197] 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. Following this report, Meta removed 45 Facebook accounts and 1,037 Instagram accounts associated with Cyber Front Z. Meta noted that these trolls were active on Facebook, TikTok, Twitter, YouTube, LinkedIn, VKontakte, and Odnoklassnki. [198]

In February 2022, Meta 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. [199]

In February 2023, YouTube revealed that it had removed over 4 million videos and 800 channels as a result of the platform's ban on Russian state-funded media outlets. [200] In May 2022, YouTube announced that it had removed over 70,000 videos and 9,000 channels that violated its "major violent events" policy (see B2). [201]

In March 2022, Twitter announced that it banned 100 accounts that promoted the hashtag #IStandWithPutin under their "coordinated inauthentic behavior" policy. [202] In March, Twitter removed tweets from the Russian embassy in London that disseminated images claiming the Russian military's bombing of a hospital in Mariupol was fake. [203]

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. [204] 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. [205]

A May 2023 joint investigation conducted by a consortium of French, German, Swiss, Danish, Norwegian, and Swedish news outlets obtained leaked documents indicating agents of the Russian government had infiltrated protests that were

unrelated to the Kremlin's full-scale invasion of Ukraine, held signs in support of the invasion, and shared pictures of the protests on social media. [206]

After the coverage period, Prigozhin's June 2023 march towards Moscow, his subsequent expulsion from Russia, and his death in an August 2023 plane crash have left the fate of the Internet Research Agency uncertain. At the end of June, Russian media began to report that Prigozhin had closed all of his companies based in Russia, including the Internet Research Agency, and fired all of its employees. [207] However, following Prigozhin's death in an August 2023 plane crash, *Wired* reported that trolls that operated similarly to those linked to the Internet Research Agency promoted narratives in favor of Prigozhin on X, formerly known as Twitter. [208]

Platforms based in Russia, including VKontakte, routinely remove content critical of the government (see B2). Officials have also propped up newer platforms that are rife with disinformation. For example, in August 2022, Duma State Deputy Anton Gorelkin promoted the launch of "Runiversalis," a website that mirrors Wikipedia's architecture, but largely promotes Kremlin propaganda, including about the full-scale invasion of Ukraine. When the site was launched, Gorelkin stated it will follow "the requirements of the legislation of the Russian Federation and our traditional values. This means that any attempts to give the articles a left-liberal and Western-centric bias will be thwarted." Unlike Wikipedia, which the Russian government has repeatedly tried to pressure to remove or alter content (see B2), only Runiversalis members may contribute to articles. [209]

B6 0-3 pts

Are there economic or regulatory constraints that negatively affect users' ability to publish content online?	**0**/3

Score Change: The score declined from 1 to 0 because of the expansion of the foreign agents law and the practice of adding media outlets and civil society organizations to the list of "undesirable organizations."

Several economic and regulatory constraints limit users' ability to publish content online, and the government introduced new measures during the coverage period. Onerous regulations and restrictive laws affecting online news media have pushed some outlets to downsize, change owners, or exit the market altogether. Many

foreign media holdings left Russia following measures in 2016 that prohibited greater than 20 percent foreign ownership of Russian media outlets. [210]

Since 2017, authorities have increasingly used the 2012 "foreign agents" law to limit user's ability to publish content online, and have repeatedly expanded its scope. The law initially required NGOs and other entities that received foreign funding in Russia to register as "foreign agents" and label their content, or face escalating fines. [211] By June 2022, the law defined foreign agents as any individual or entity "under foreign influence," [212] and contained rules obliging media to identify foreign agents as such when they are mentioned in any publication. [213] In March 2022, the State Duma approved amendments that propose the creation of a register with information about individuals considered foreign agents and people associated with them. [214] In the same month, approximately 400 entities had been added to the foreign agents list. [215] As of December 2022, [216] the Ministry of Justice gained the right to publish personal data of designated foreign agents and maintain a list of people affiliated with them. In August 2023, after the coverage a law came into effect that outlines penalties for ″persons under foreign influence″ and prohibits individuals and state agencies from supporting entities recognized as "foreign agents" violators will first receive a warning, and then fines ranging from 30,000 to 300,000 rubles. [217] In June, the State Duma's Committee on Foreign Interference revealed that 861 people are listed as affiliates of foreign agents, under the December 2022 law. [218]

In January and February 2021, RFE/RL and its Russian affiliates that were recognized as foreign agents were fined 1.1 million rubles and 2.2 million rubles, respectively, because their websites did not label their content according to the law. [219] In April 2021 the government labelled Meduza—one of Russia's largest independent media outlets, which operates from Latvia—as a "foreign agent," threatening its ability to maintain funding. [220] (Meduza was labeled an "undesirable organization" in January 2023, effectively criminalizing it in Russia.) [221] In May 2021, the Ministry of Justice also recognized the recently established media outlet VTimes as a foreign agent. [222] 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. [223] 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. [224]

More organizations were added to the list during the coverage period, including Roskomsvoboda, an organization that advocates for digital rights, which was added to the list in December 2022. [225] The Ministry of Justice added environmental groups Sakhalin Environmental Watch and Movement 42 to the foreign agents list in December 2022 and January 2023, respectively. Both outlets closed after being designated as foreign agents. [226]

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. [227] In October 2021, the authorities designated BBC journalist Andrei Zakharov as foreign agent. [228] During the coverage period, the register of foreign agents was further expanded to include Russian artists, musicians, politicians, and public figures. For example, former State Duma deputy Yevgeny Roizman [229] and editor of the Dozhd TV channel Tikhon Dzyadko, [230] among others, were added to the list in November and October 2022, respectively. In March 2023, blogger Ilya Varlamov and Pavel Chikov, the head of the Agora human rights and legal advocacy group, were added to the list. After the coverage period, in September 2023, the Ministry of Justice added Dmitry Muratov, the editor in chief of *Novaya Gazeta*, to the list of foreign agents. [231]

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, the Supreme Court revoked *Novaya Gazeta*'s license for violating that provision (see B4). [232]

During the coverage period, the Ministry of Justice named media outlets and organizations, including Bellingcat, Insider, [233] Meduza, [234] the Andrei Sakharov

Foundation, [235] Transparency International, [236] Greenpeace, and the Anti-Corruption Foundation International [237] as undesirable organizations, which makes it more difficult for these outlets and organizations to publish online, and criminalizes the sharing of their content (see B4). The designation includes administrative and criminal liability for those who participate in these organizations, provide financial assistance, distribute their materials, organize their activities. After the coverage period, the Ministry of Justice added the World Wildlife Fund (WWF) [238] Agora, [239] and Novaya Gazeta Europe [240] to the list of "undesirable organizations." Administrative fines range from 5 to 15 thousand rubles for citizens, from 20 to 50 thousand rubles for officials, from 50 to 100 thousand rubles for legal entities, [241] though repeated offenses can result in fines up to 500,000 rubles or four years of correctional labor. Participation in undesirable organizations' activities is also punishable under criminal law. In this case, the punishments are stricter: fines start at 300 thousand rubles and violators can be imprisoned for up to 6 years. [242]

The Anti-Corruption Foundation (FBK), the Foundation for the Protection of Citizens' Rights (FZPG) and the headquarters of Alexei Navalny remain on the list of extremist organizations.

Users convicted of extremism or other offenses involving mass media or the internet are legally barred from serving as editors in chief at publications. [243]

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. [244]

Following the invasion of Ukraine, several 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. [245]

B7 0-4 pts

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

The diversity and reliability of the online landscape deteriorated further since the start of the Kremlin's full-scale invasion of Ukraine, 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 (see B1 and B4). During the coverage period, the government intensified its efforts to block and force the removal of LGBT+ content (see B1 and B2).

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. [246] Research conducted in May 2022 suggests that Russians have become less trusting of television sources and more trusting of media consumed online since the invasion. 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. [247] 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.

Following the full-scale invasion, social media platforms, including Facebook, Twitter, and Instagram, were blocked. In October 2022, Roskomnadzor added Meta, which was labelled an extremist organization in March 2022, to the list of "terrorist and extremist organizations," which means anyone who buys advertisements on the platforms could face up to 10 years in prison. [248]

Users of platforms that were blocked in the wake of the invasion primarily flocked to VKontakte, which has hidden information about the war and criticism of the Russian government (see B2), and Telegram. In September 2022, VKontakte, which is effectively owned by state companies, purchased Zen and News from Yandex, two of the company's most popular services, further restricting diversity in the online space. [249] Research from Mediascope found that Telegram's daily audience in the country increased by 66 percent between January 2022 and July 2022. [250]

Although YouTube, one of the most popular online platforms, was not blocked by the government, the Kremlin has promoted 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. [251]

Other blocked websites include Ukrainian news sites, international news sites, and Russian news sites that tried to accurately report on the invasion (see B1). After the invasion, a number of media outlets, including *Novaya Gazeta* and the Bell, shut down, reduced their coverage, or moved their websites outside of the RuNet. Even beforehand, many independent online media outlets within Russia were forced to shut down due to government pressure (see B4, B6 and C3). [252]

Virtual private network (VPN) users can still access a diverse range of media and news sources in Russia. However, it has become more difficult for users to access internationally available 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). [253] Nonetheless, VPN usage increased significantly since the start of the full-scale invasion; the Russia-based media group RBC reported that as of July 2022, VPN downloads had increased sixfold from January 2022. [254] Additionally, in May 2022, Top10VPN reported that Russian companies and government agencies have invested significant close to $10 million in VPN technology as of May 2022, with legislative entities spending the most money. [255]

In April 2022, government agencies, including the Federal Tax Service, stopped accepting emails from foreign domains, citing fears of cyberattacks originating from abroad. [256] In February 2023, reports surfaced that major Russian companies and Russian state agencies were abandoning Google products and limiting employees' use of them, in favor of domestically produced alternatives. [257]

B8 0-6 pts

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

Although the internet remains a platform for activism in Russia, this function has come under significant pressure, particularly since the full-scale invasion of Ukraine. Those calling for demonstrations on the internet can 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. [258]

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). [259]

Law enforcement officials have 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. [260] 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. [261] A September 2022 investigation by the *New York Times* also shed light on Roskomnadzor's efforts to surveil users that attend or organize protests (see C5). [262]

Authorities have taken a range of measures to stifle opposition figure Aleksey Navalny and individuals associated with his Anti-Corruption Foundation (FBK) and Smart Voting movement. In September 2021, Roskomnadzor ordered Google and Apple to remove the Smart Voting applications from their respective app stores, and they complied (see B2). [263] The regulator also blocked access to the Smart Voting website and 49 affiliated websites (see B1), [264] and forced people who shared symbols linked to Navalny's movement on social media to remove them, arresting them in some cases (see B2 and C3). In June 2021, the Moscow City Court ruled that the FBK and Navalny's headquarters qualified as extremist organizations. In March 2022, Navalny was sentenced to nine years in a maximum-security prison on charges of fraud and contempt of court. [265]

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, [266] 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. Several restrictive laws, coupled with repressive law enforcement and judicial systems, have also eroded freedom of expression in practice (see C2).

Russia's judiciary is not independent. The courts tend to side with the government, including in cases where constitutional protections or provisions of international treaties apply. In 2019, the courts acquitted defendants in fewer than 1 percent of criminal cases. [267]

In March 2022, Russia was expelled from the Council of Europe, [268] with the Committee of Ministers of the Council of Europe noting that Russian military 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, the State Duma passed a law invalidating the European Court of Human Rights (ECHR) decisions made after March 15 and stipulating that Russians will no longer be able to appeal to the court. [269]

C2 0-4 pts

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

human rights standards?

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). [270] Article 6.21 of the administrative code prescribes fines for "advocacy of nontraditional sexual relations among minors," [271] while Article 148 of the criminal code bans insulting religious feelings, which is punishable by fines or imprisonment. [272]

Articles 20.3 and 20.29 of the administrative code prescribe fines for displaying extremist symbols (such as Nazi symbols) and distributing extremist materials, [273] and Article 354.1 of the criminal code bans spreading false information about the Soviet Union's actions in World War II. [274] In March 2020, Article 20.3 of the administrative code was amended to allow extremist symbols to be displayed without penalty for nonpropagandistic purposes. [275] 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. [276] The measures, which were included in the code of administrative offenses, stipulates that citizens can a fine of up to 2,000 rubles, 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 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. [277]

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 and criminal procedure 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, 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 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 or up to five years in prison; calls for sanctions against Russia lead to a fine of up to 500,000 rubles or up to three years in prison. [278] 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. [279]

In March 2023, the State Duma passed amendments that broaden the definition of discrediting the military. [280] The amendments criminalize "discrediting" any participants in the "special operation," with violators facing a punishment of up to 15 years in prison. These measures would now apply to volunteer formations, organizations and individuals who assist in the fulfillment of the tasks assigned to the Russian army, including the activities of private military companies, as well as information on the collection of equipment, food, and other materials. The amendments provide for fines of up to five million rubles or in the amount of wages or other income of the convicted person for a period of up to five years, correctional or forced labor for up to five years, or imprisonment for up to fifteen years. [281]

In July 2022, the State Duma adopted amendments to the criminal code that introduce 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." [282] For those who make public calls against the security of the state, fines range from 200,000

to 1 million rubles. 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.

Articles 280 and 280.1 of the criminal code punish online calls for extremism and separatism with up to five years in prison. [283] Article 20.3.1 of the administrative code assigns fines or up to 15 days in jail for those found guilty inciting hatred online, [284] and repeat offenders can face longer prison terms under Article 282 of the criminal code. [285] 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). [286] 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 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). [287] Individuals or organizations found to have shared fake news face fines of up to 1.5 million rubles, 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. [288]

In April 2020, Putin signed a law that stipulated fines for spreading fake news related to the coronavirus of up to 2 million rubles for individuals [289] and 5 million for media outlets and other legal entities. [290] 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. [291] The Supreme Court later 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. [292]

The 2016 Yarovaya Law altered nearly a dozen existing laws, with significant ramifications for internet freedom. [293] 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. [294]

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 legislation that criminalizes discrediting the Russian military and participants in the special military operation (see C2). The Online Freedoms Project recorded a record 779 cases of criminal prosecution for online expression in 2022. [295]

In July 2022, 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." [296] 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 local election candidate in Krasnodar. [297]

Following the invasion of Ukraine in February 2022, several people were charged under March 2022 amendments to the criminal code that prohibits "knowingly spreading false information" about the war or discrediting the military (see C2). In March 2023, the Ministry of Internal Affairs reported that there had been 5,000 "offenses" related to the spread of false information about the war. [298] The Online Freedoms project reported that 187 criminal cases were opened under the amendments in 2022. In July 2022, Aleksei Gorinov, a municipal councilperson in Moscow, was the first person to receive prison time under the new law: seven

years for offline comments he made at a council meeting about the deaths of Ukrainian children. [299] In other cases:

- In August 2023, after the coverage period, Yelena Dovrovskikh, a progovernment editor in chief of the Rostov-on-Don-based 1RND news sites, was charged with "discrediting the army" over an article the site had published about bulletins posted in the city that instructed people on how to surrender to the Ukrainian army. [300]
- In July 2023, after the coverage period, law enforcement officials arrested Igor Kilbin, a former KGB officer who supported the invasion, because he had criticized Putin's handling of the war—especially in the wake of Prigozhin's march to Moscow the previous month. [301]
- In June 2023, after the coverage period, blogger Roman Ushakov was sentenced to eight years in prison by a military court in Moscow, and he was prohibited from running websites for an additional three years. The conviction stemmed from comments Ushakov made about the invasion of Ukraine on Telegram. He was arrested in December 2022 and claimed law enforcement had used "electric shocks" to torture him while he was detained. [302]
- In March 2023, Andrei Novashov, a a freelance journalist who had previously worked with the RFE/RL-affiliated Siberia.Relatiies outlet, was sentenced to eight months of corrective labor over social media posts covering the Russian military's attacks on civilian targets in Mariupol. [303]
- In the same month, a court sentenced a man in Yefremov to two years in prison for criticizing Putin's handling of the war on social media. He was charged after his daughter drew a picture at school that indicated his opposition to the war. He fled before he was sentenced. [304]
- In February 2023, journalist Alexander Nevzorov was sentenced to eight years in a penal colony in absentia for publishing material about the shelling of Mariupol by the Russian army. [305]
- In the same month, the Leninsky District Court in Barnaul sentenced Maria Ponomarenko, a journalist who worked for the online website RusNews, to six years in a penal colony for social media posts about the Russian military's attack on a theatre in Mariupol. She was initially arrested in April 2022. [306]
- Also in February, a court sentenced Veronika Belotserkovskaya, blogger and founder of Sobaka.ru, in absentia to nine years in prison for social media

posts criticizing the Russian military's attacks on civilians in Ukraine. [307] The case against her was initially opened in 2022. In May 2022, she was put on the wanted list, and in June the court seized her property.

- In the city of Cheboksary, the former coordinator of Navalny's headquarters was fined three times, most recently in February 2023, for posts in Telegram and videos "discrediting" the Russian army. [308]
- In February 2023, Ruslan Agbalov, a former policeman from Kursk, received an administrative charge for "discrediting" the army on his YouTube channel. [309] The man later left the country due to persecution by the authorities (see C7).
- In December 2022, politician Ilya Yashin was sentenced to eight and a half years in prison. According to a court decision, after his release, he will also be prohibited from administering websites for four years. [310] Yashin, who was already detained after being arrested on separate charges the previous month, was charged under the law in July 2022 over a YouTube video he posted about the Russian military's actions in Bucha, where rights groups have documented evidence of a massacre. [311]
- In September 2022, a Yekaterinburg court fined Stanislav Shminke, the founder of the Uralnash website, 400,000 rubles for an article that "discredited" the army. [312] A deputy of the United Russia party filed the initial report to the prosecutor's office. [313]
- In March 2022, a man in the Kemerovo region was fined 60,000 rubles after he posted a video urging people to join antiwar protests. [314]
- 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. [315]
- Also in March, 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. [316] Later in the month, Nikolay Kuzmin, a municipal deputy from the Yabloko party, was fined 30,000 rubles for reposting the video. [317]
- In the same month, 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. [318]

- A resident of Novokuznetsk was fined 50,000 rubles for publishing a video on her personal social media page calling on people to condemn the invasion. [319]
- In March, a Yekaterinburg court fined Yevgeny Roizman, the former mayor of the city, 100,000 rubles for antiwar statements he made on YouTube and Twitter. [320]

During 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. For example, In July 2022, 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. [321] In the previous coverage period, several individuals also faced similar charges. [322]

Users have also faced charges for posts allegedly calling for violence or rallies. [323]

In September 2022, journalist Ivan Safronov, who worked for Vedomosti and Kommersant, was sentenced to 22 years in prison in a treason case for allegedly sharing information about Russia's military in the Middle East with the Czech government. [324] Reporters Without Borders (RSF) named this sentence the most severe in the 2022 edition of its annual report on global press freedom. [325] In August 2023, after the coverage period, the Supreme Court upheld the sentence. [326] In March 2023, *Wall Street Journal* reporter Evan Gershkovich was arrested on charges of espionage in Yekaterinburg, and his detention was most recently extended through November 2023. [327]

In March 2022, a court in Rostov-on-Don sentenced journalist Remzi Bekirov, a Crimean Tatar, to 19 years in prison for allegedly "organizing the activities of a terrorist organization" and "preparing to a violent seizure of power." [328] 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 Tatars and pro-Ukrainian activists in occupied Crimea, and uploaded interviews with activists of Crimean Solidarity to their YouTube channel. [329] Apart from Bekirov, the court also sentenced lawyer and human rights activist Riza Izetov and activists Shaban Umerov, Rayim Aivaziv, and Farkhod Bazarov. [330] 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). [331] In July 2022, after three years of litigation, Tsvetkova was acquitted of distributing and "illegally producing pornography." [332]

C4 0-4 pts

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

Anonymous communication is restricted in Russia, as are encryption tools. The Russian government continues to block internationally available VPNs. The authorities used the Technical Measures of Combating Threats (TSPU) equipment (see A3 and B1), which relies on DPI technology, to restrict access to VPN services. [333] As of March 2022, approximately 20 popular VPN services had been blocked in Russia. [334]

A 2017 law mandates the blocking of VPN services that allow their clients to access banned content. [335] 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). [336] Most of the VPNs immediately refused, but they were not blocked. [337]

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. [338] 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 [339] over a two-year period. [340]

In September 2021, Roskomnadzor announced the blocking of six additional VPN services, including ExpressVPN and NordVPN (see B1). [341] 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. [342] In January 2022, the authorities blocked the Tunnelbear VPN, [343] which was included in the register of prohibited sites in 2018. [344] In June 2022, Roskomnadzor began blocking ProtonVPN.

In May 2022, Roskomnadzor's Public council met and listed VPN services as tools in the information warfare campaign against Russia, which made the blocking of VPNs more effective. [345] In December 2021, Roskomnadzor 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, Roskomnadzor briefly unblocked the Tor browser, [346] though a court banned Tor again in the same month.

In May 2023, VPN users reported that the OpenVPN protocol, which is used by many private institutions in Russia, was blocked (see B1). [347] In June, after the coverage period, the number of complaints about blocking decreased. [348] In August 2023, reports emerged that Wireguard, another open VPN protocol, as well as OpenVPN were blocked across several mobile operators. [349]

Previously, the national security authorities initiated a campaign against encrypted email services in early 2020. And services, including SCRYPTmail.com, Mailbox.org, ProtonMail, Tutanota, and StartMail were blocked. [350]

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." [351] 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. [352] 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. [353] In May 2019, [354] new rules

requiring such platforms to verify users' phone numbers with the help of mobile service providers entered into force. [355] 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. [356] Roskomnadzor interprets the rules to apply to both foreign and domestic platforms. [357] 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. 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. [358]

In December 2021, President Putin signed a law authorizing the development of a unified biometric database. [359] In July 2022, the State Duma approved amendments that would allow banks to transfer clients' personal data to the system without their consent. [360]

In June 2022, 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, [361] though the plan had not come into fruition by the end of the coverage period.

At the end of June, Russian banks began to notify customers who had previously submitted biometrics that their data would be transferred to the state Unified Biometric System. [362] Banks must complete the data transfer process by September 30, 2023.

In November 2022, Putin ordered the creation of a state information resource with citizens' data "necessary for updating military records." [363] This resource will

generate data on citizens who are registered with the military. In February 2023, the authorities began testing the database, with plans to launch it in the spring of 2023. [364] The database, according to Putin's decree, should contain information about phone numbers and email addresses, places of registration and driver's licenses, real estate and cars of military-aged men, their work, family, health status, judicial history, and deferrals from mobilization, among other things. In September 2023, the Ministry of Digital Development, Communications and Mass Communications announced that a full register of those liable for military service will begin work no earlier than 2025. [365]

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 several 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 they do not comply. 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 (see A3). [366]

Some researchers have argued the sanctions imposed on Russia by the United States and EU in response to the full-scale invasion of Ukraine have made it more difficult for the Kremlin to acquire the necessary technology to maintain and upgrade SORM. Nokia, which pulled out of the country in March 2022, had previously supplied telecommunications operators and the government with much of the technology necessary to operate these systems. [367] However, a July 2023 *New York Times* investigation revealed that in spite of sanctions Russian firms had produced tools that can "track certain kinds of activity on encrypted

apps like WhatsApp and Signal, monitor the locations of phones, identify anonymous social media users and break into people's account." [368]

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, Roskomnadzor regularly monitored social media platforms, including 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. [369]

A separate investigation published by RFE/RL in February 2023, which relied on a second set of leaked Roskomnadzor data published in November 2022, found that Roskomnadzor's Main Radio Frequency Center (GFRC) engaged in similar social media monitoring. The investigation revealed that the GFRC had a "Protest Moods" chatroom, which included employees from other government agencies, and monitored the likelihood of protests based on what people shared on social media platforms and messengers. The GFRC also used bot farms in attempts to infiltrate closed groups and messenger channels. [370]

Additionally, in August 2022, the GFRC spent 57 million rubles on an artificial intelligence monitoring system, known as Oculus (see B2), which allows employees to identify "prohibited information" in social media posts, including multimedia posts. [371]

The Kremlin has also used 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. [372] In Moscow, as of 2020, there were 178,000 such cameras, and the government announced plans to add another 9,000 cameras in 2021. [373]

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. 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). [374] Since September

2022, authorities in Moscow have used facial-recognition cameras to track down and detain conscripts trying to avoid mobilization, and at least seven arrests have been made using this system. [375]

In September 2022, after the coverage period, Galina Timchenko, who runs the Latvia-based online news outlet Meduza, reported that her iPhone had been infected with NSO Group's Pegasus spyware, which allows the attacker to gain access to the infected device, a couple of weeks after the Ministry of Justice listed Meduza an "undesirable organization" (see B6). [376] The case marked the first time a Russian journalist's device had a confirmed Pegasus infection. Researchers were not able to definitively identify the culprit behind the attack.

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. [377] 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. [378]

Russian authorities are nominally required to obtain a court order before accessing electronic communications. [379]

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. [380] Experts note that there is no publicly available information about accountability for FSB officers who may abuse this power. [381]

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. [382] 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. [383]

Under provisions of the Yarovaya Law that came into force in July and October 2018, [384] 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. [385] Service providers must store users' browsing history for 30 days. [386] 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. [387] 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 in special equipment from the state corporation Rostech in order to comply with the Yarovaya Law. [388] 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.

In March 2023, the State Duma passed a law that obliging owners of communication networks with autonomous system numbers to store user data for three years. [389] The law also obliges them to provide information upon request to law enforcement agencies. Network owners must store voice information, text messages, images, sounds, video or other messages for three years. Previously, according to the Yarovaya Law, such data was stored and transferred to the security forces by telecom operators only in relation to end users, but now the data includes that of company employees and internal networks. [390]

Beginning in March 2023, telecom operators in Russia must notify Roskomnadzor of the implementation of cross-border data transfer. [391] At the same time, the supervisory authority may decide to ban or restrict it "in order to protect the morality, health, rights and legitimate interests of citizens."

In June 2022, 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. [392] 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. In August 2022, the Ministry of Digital Development issued a fine scheme for operators who refuse to install SORM, [393] which will come into effect in May 2023 (see A4).

In July 2023, after the coverage period, Roskomnadzor announced It would begin issues fines ranging from one to five million rubles to ISPs and mobile operators that fail to install the TSPU system (see A3, A4, and B1), the DPI system it uses to block website that also collects data on user traffic. [394]

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. [395] 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. [396]

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. [397] Some foreign companies, such as Uber and Viber, [398] 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 continued to issue fines during the coverage period. Fines were first issued April 2019, when Twitter and Facebook were fined a token 3,000 rubles for their noncompliance. [399] 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. [400]

In July 2022, WhatsApp and Snapchat were fined 18 million rubles and 1 million rubles, respectively, for failing to store user data locally. [401] WhatsApp was previously fined 4 million rubles in August 2021, marking the first fine for the messaging service. Facebook and Twitter were fined in 2021 before they were blocked. [402]

In July 2022, a Moscow court fined Apple 2 million rubles for because the company did not store user data locally. [403]

In June 2022, Google was fined 15 million rubles for repeatedly refusing to localize users' personal data in Russia. [404] The company was fined 3 million rubles for the same reason in July 2021. [405] In June 2022, a Russian court fined Twitch, Pinterest, Airbnb, and UPS for refusing to localize Russian data. [406] The latter three companies received a fine of 2 million rubles, while UPS was fined 1 million rubles.

The government has also fined companies based in the country for refusing to share data with the security services. In June 2023, after the coverage period, Yandex was fined 2 million rubles because it reportedly refused to share data, including encryption keys, with the FSB, as is required under the Yarovaya law (see C6). [407] The company was previously fined 400,000 rubles for the same reason in 2022. [408]

In 2021, Facebook received 11 requests for user information from the Russian government, but it complied with none of them. [409] Twitter did not produce a report during the coverage period. [410] In the first half of 2022, Google received 43 requests for user information, and it produced some data in 62 percent of those cases. In the second half of the year, it received 43 requests from the Russian government and produced some data in 47 percent of the cases. [411]

In December 2022, Putin signed a law obliging taxi-ordering services to provide the FSB with access to their databases, including geolocation and payment information, [412] as well as remote access to their systems. [413]

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. [414]

During the coverage period, some users who were arrested for spreading false information about or discrediting the Russian military (see C2 and C3) reported that they were tortured or attacked. For example, Roman Ushakov, a blogger who was sentenced to eight years in prison for spreading false information about the military (see C3), alleged that law enforcement agents tortured him with "electric shocks" during his initial detention in December 2022. [415] In February 2023, Ruslan Agbalov, who served as a police officer in Kursk, posted a video In which he had a black eye and implied he had been beaten, after he was charged with "discrediting" the army (see C3). [416] He later fled the country.

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. [417] Elena Milashina, a Russian journalist working for *Novaya Gazeta*, has regularly faced death threats for her coverage of human rights issues in Chechnya. 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. [418] In February 2022, Milashina fled the country following an investigation she conducted on Chechen government officials who threatened a judge, which led Kadyrov to label her a "terrorist." [419] In July 2023, after the coverage period, she was beaten as she was on her way to the Chechen regional capital of Grozny to cover the trial of a human rights activist. [420]

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. [421] 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. [422]

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

Since the Kremlin's full-scale invasion of Ukraine, state websites have continued to face significant cyberattacks.

Researchers at the Network Freedoms project documented at least 60 major hacks in 2022, [423] which included data from state systems, including Gosuslugi and the Moscow Electronic School; operators, including Rostelecom and Beeline; and medical centers. Between January and April 2023 Roskomnadzor reported more than 40 major data breaches, though it did not disclose further information about the breaches. [424]

In November 2022, the Cyber Partisans announced that they had hacked Roskomnadzor's General Radio Frequency Center (see B2 and C5). This followed a 2022 hack of Roskomnadzor's office in the Republic of Bashkortostan. [425]

In July 2022, it was reported that Turla, a hacker group aligned with the Russian government, had launched a spoof application that claimed to launch DDoS attacks on Russian websites, but in reality it enabled the hackers to siphon user data. [426]

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. [427] In May 2022, RuTube, Russia's alternative to YouTube, suffered a hacking attack and was offline for three days. In June 2022, the Russian Ministry of Construction, Housing, and Utilities' website was hacked to display a message in support of Ukraine. [428]

Following the Russian invasion of Ukraine, Ukrainian hackers formed an "IT Army" and launched distributed denial-of-service (DDoS) attacks on Russian websites. The hackers targeted a range of companies and government agencies, issuing instructions and updates via Telegram. [429]

In February 2022, the hacking group Anonymous claimed responsibility for cyberattacks that displayed antiwar messages on the websites of the Russian government, Roskomnadzor, and other state entities, as well as state-affiliated media outlets including RT, TASS, and *Kommersant*. [430] Following the first week of Anonymous' campaign, more than 2,500 Russian- and Belarusian-linked websites faced cyberattacks. [431]

Private companies also faced significant cyberattacks. In January 2023, Yandex confirmed that the source codes of its services were leaked (see B2). [432] Code related to Yandex's Maps, Search, Mail, voice assistant, marketplace, taxi, food-ordering service, and payment service were exposed to the public. 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. [433]

In January 2023, the 1C company, which develops computer programs and tools for business automation, had personal data, including passwords, of people enrolled in one of their courses leaked. [434]

In February 2022, the data of more than 100,000 customers and employees of the logistics and tracking company SberLogistics service turned out to be openly available. [435]

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. [436] To do this, Roskomnadzor intends to upgrade its DPI equipment, which is also used to block websites and enforce the law on the sovereign internet. [437]

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 2023, 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 International Telecommunications Union, "Statistics," "Mobile Broadband Subscriptions," accessed September 2023, https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

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

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

16 /100 **Not Free**

Internet Freedom Score

21 /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 2023

Other Years

2022

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