Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**609**
Land:	Rusland
Kilde:	Freedom House
Titel:	Freedom on the net 2020 – Russia
Udgivet:	maj 2020
Optaget på baggrundsmaterialet:	5. januar 2021

Freedom House

Russia

FREEDOM ON THE NET 2020

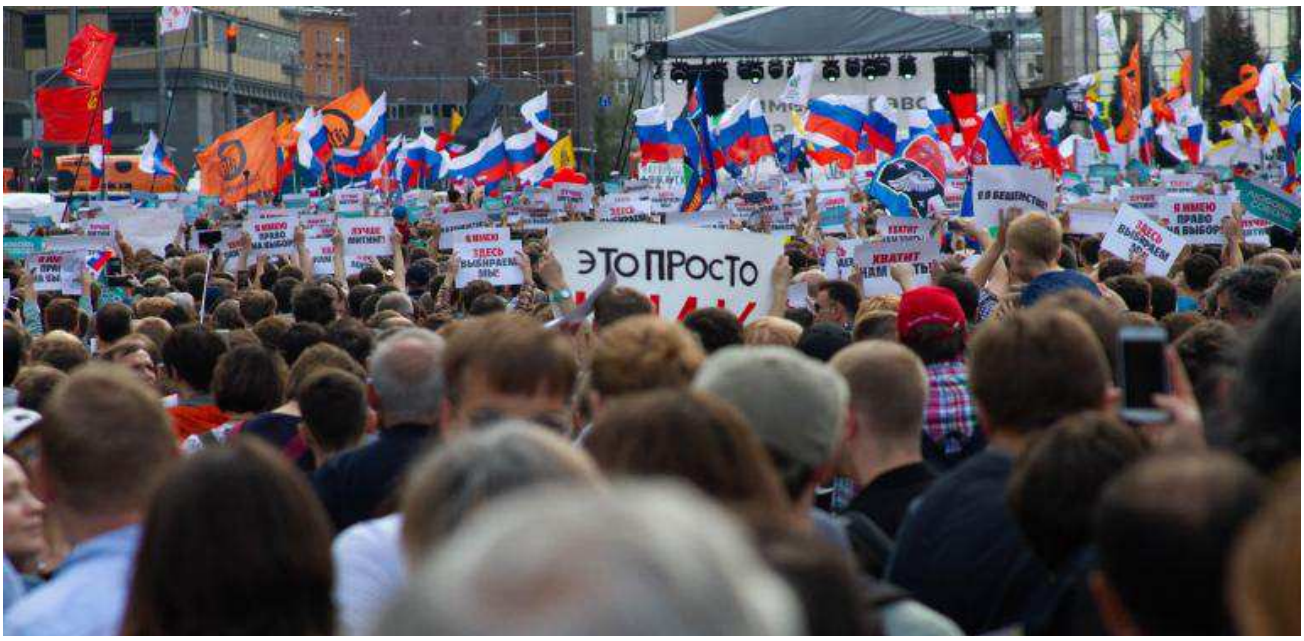
NOT FREE

30
/100

A. Obstacles to Access	11 /25
B. Limits on Content	11 /35
C. Violations of User Rights	8 /40

LAST YEAR'S SCORE & STATUS
31 /100 Not Free

Scores are based on a scale of 0 (least free) to 100 (most free)



Overview

Internet freedom in Russia contracted during the coverage period, as the government continued to fine-tune its online censorship apparatus. After the Sovereign Runet Law entered into force in November 2019, the government conducted simulations designed to ensure that the Russian portion of the internet, the so-called Runet, can function independently of the global internet in the event of unspecific threats, testing equipment that will enable authorities to more effectively restrict access to online content. A leadership shakeup at the regulatory body responsible for the Sovereign Runet agenda may accelerate the implementation of this law. The persecution of users for their online activities continued, with the state initiating new administrative and criminal proceedings against political activists and, in particular, participants in mass protests that took place before the September 2019 regional elections. The authorities also moved to restrict anonymous communications, blocking several encrypted email services. Finally, with the onset of the COVID-19 pandemic, the government began a campaign to censor information that conflicted with official statistics, accusing its distributors of publishing fake news.

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, 2019 – May 31, 2020

- The communications regulator obtained new powers to "sovereignize" the Russian segment of the internet amid a leadership reshuffle at the agency (see A5).
- In late 2019, the government began testing traffic-filtering equipment in keeping with the Sovereign Runet Law. However, the COVID-19 pandemic delayed further tests as well as the law's full implementation (see A3).

- The authorities blocked several encrypted email services in early 2020, arguing that they were facilitating calls for extremist activities (see B1, C4).
- In spring 2020, the government deployed intrusive surveillance systems, ostensibly to enforce its COVID-19 quarantine regime, and worked to censor or deter the circulation of any content that conflicted with official reports on the pandemic (see B2, B5, C5).

A. Obstacles to Access

While internet access remained relatively affordable and continued to expand during the coverage period, prices have increased as providers seek to offset the costs of compliance with new laws enabling state monitoring and content controls. The communications regulator, which is not politically independent, gained new authority over the internet infrastructure under the Sovereign Runet Law, which took effect in November 2019. Some localized service disruptions were reported in connection with politically sensitive events, including the September 2019 regional elections.

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. According to the Levada Center, a nongovernmental research organization, the overall internet penetration rate reached 76 percent by the fourth quarter of 2019, when the proportion of Russians who used the internet daily or at least several times a week was about 65 percent. [1] The Russian research company Mediascope estimated the country's internet penetration rate at 79.1 percent for the period from October 2019 to March 2020. The rate for Moscow, the capital, was 86.6 percent for the same period. [2]

In 2019, the household subscriber base for fixed broadband internet connections increased by 1 percent compared with 2018, from 33.1 million to 33.4 million subscribers, according to the Russian research

company TMT Consulting. The household fixed broadband penetration rate was about 60 percent, [3] though it exceeds 90 percent in the largest cities. [4] The government's national Digital Economy program aims to provide 97 percent of households with fixed broadband internet connections featuring speeds of 100 Mbps or more by 2024. [5]

Increasingly, users in Russia access the internet through mobile devices. The subscriber base for mobile internet connections increased to 260.6 million customers by mid-2019; this amounted to more than 175 percent of Russia's total population, meaning there were multiple subscriptions per person. [6] The number of mobile internet users in 2019 reached 85.2 million, or almost 89 percent of all internet users. [7]

According to the Economist Intelligence Unit's 2020 Inclusive Internet Index, third-generation (3G) mobile networks cover 78 percent of the population, while 4G services cover 70 percent. [8] The government planned to roll out 5G services, first in Moscow, starting in 2020. [9] However, by the end of the coverage period the Security Council still had not agreed to transfer the radio frequencies that are most suitable for 5G services to mobile operators, blocking the development of 5G networks. Currently, these frequencies are reserved for the Russian military. [10] Moreover, amid the COVID-19 pandemic and the attendant economic crisis, the Ministry of Digital Development, Communications, and Mass Media suggested redistributing funds allocated for the development of 5G networks in 2020 for other purposes, such as ensuring that small communities can access major television channels' broadcasts. A final decision on this matter had not been made by the end of the coverage period. [11]

Publicly accessible internet connections in institutions like hospitals, libraries, schools, and mass transit are fairly widespread in large cities. In rural areas, the availability of public internet connections remains limited.

Connection speeds are stable, with fixed broadband download speeds averaging 66.01 Mbps and mobile internet download speeds averaging 20.27 Mbps, according to May 2020 data from Speedtest. [12] These speeds place Russia ahead of many of its neighbors in the

Commonwealth of Independent States (CIS), but behind most European Union (EU) countries. Increased traffic associated with the COVID-19 pandemic placed some strain on networks in Russia. For example, in March 2020, the president of MTS, one of the country's largest internet service providers (ISPs), urged subscribers to "to take a responsible approach to content consumption." [13]

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

Despite economic strains and recent currency fluctuations, internet connections remain relatively affordable for most of the population. The 2020 Inclusive Internet Index ranks Russia 27 out of 100 countries in terms of the affordability of connections. [1] According to data from the International Telecommunication Union (ITU), a monthly fixed broadband subscription cost 0.7 percent of gross national income (GNI) per capita in 2019, while a mobile plan offering 10 GB of data cost 1 percent of GNI per capita. [2] In nominal terms, according to official statistics, as of January 2020 the average monthly cost of a fixed broadband subscription was 545 rubles ($8.50), while that of a mobile internet subscription was 344 rubles ($5.30). [3] In mid-2020, the average nominal monthly salary in Russia was almost 50,100 rubles ($780). [4] While people in the middle class and above can easily afford internet access, a significant portion of the population (14.3 percent as of early 2019) lives below the poverty line, and connections are prohibitively expensive for many in that group. [5]

Robust competition in the information and communication technology (ICT) market is one of the most important factors restraining price increases. [6] However, prices have gradually risen due to compliance with the Yarovaya Law (see C6), which requires that ISPs install expensive equipment to record and store users' traffic data on their networks. ISPs have passed installation costs on to their customers. Another factor driving price increases was a hike in the value-added tax (VAT) rate, from 18 to 20 percent, in January 2019. According to a survey

of ISPs, average prices increased by 10–12 percent in 2019. [7] The Sovereign Runet Law (see A3), which obliges operators to install additional equipment on their networks (namely deep packet inspection, or DPI, systems) is similarly pushing prices higher. According to preliminary estimates, over the course of 2020, ISPs will need to increase average prices by 17–18 percent to defray the cost of installing DPI systems. [8] Some ISPs have explicitly named the Yarovaya Law and the Sovereign Runet Law as the main reasons for raising prices. [9]

A digital divide persists in Russia along regional 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, where Moscow is located, while the most expensive fixed internet subscriptions, which cost almost twice as much, were found in the remote Far Eastern Federal District. [10] This dynamic also held true for mobile internet subscriptions, although the price difference was less extreme. In February 2019, the Ministry of Digital Development, Communications, and Mass Media announced that 16,000 of the 18,000 settlements with 500 to 10,000 people had broadband access, as did 8,000 of 14,000 settlements with 250 to 500 people. [11]

There are no clear digital divides along religious or gender lines. Younger people are more likely to use the internet than their elders.

In January 2020 President Putin announced a project to ensure free access for Russian citizens to “socially important Russian internet services.” [12] The list of services was approved in March and comprised some 370 Russian websites, including those of government agencies, most Mail.ru and Yandex services, various media outlets, and e-commerce platforms. [13] The project was piloted from April to July; [14] it was then extended through the end of the year. [15] The government did not immediately explain how it would offset the cost of the project to ISPs, which initially requested state compensation based on the expectation of losing 150 billion rubles ($2.3 billion) annually. [16]

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 restricted connectivity to the internet during politically sensitive moments during the coverage period. It also took continued steps to centralize its control over the country's internet infrastructure.

In July and August 2019, authorities briefly disabled fixed and mobile internet connections in parts of Moscow, amid mass protests related to the September 2019 regional elections. [1] Public Wi-Fi hotspots were also disabled. When pressed by journalists and users, ISPs denied that their networks had been disabled, [2] claiming that overcrowding was to blame for any disruptions; independent experts determined that intentional disruptions did take place. [3] The government remained silent on the issue.

In October 2019, an intentional shutdown took place in the Arkhangelsk region, affecting a protest camp occupying the site of a planned landfill. [4]

Despite these incidents, large-scale internet disruptions remain relatively uncommon in Russia. Previously, intentional shutdowns were actively used in the Republic of Ingushetia to stymie mass protests there in 2018–19. [5]

The most prominent restriction on connectivity affecting the entire population in recent years was the blocking of Telegram, a popular messaging application, which began in April 2018 (see B1). Certain Voice over Internet Protocol (VoIP) services are also blocked. After June 2018, the government scaled back its attempts to block Telegram so as to avoid the blacklisting of millions of internet protocol (IP) addresses belonging to cloud services where Telegram is hosted, which had occurred during the first two months of the blocking campaign. In January 2019, the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor) stopped blocking most of the IP addresses of Amazon Web Services, focusing instead on blacklisting the IP

addresses of proxy services used to access Telegram. [6] In October 2019, Roskomnadzor chief Aleksandr Zharov stated that a new push to restrict access to Telegram via DPI technology should be expected within a year. [7] However, in June 2020, after the coverage period, Roskomnadzor and the Prosecutor General's Office unexpectedly announced that the government would no longer restrict access to Telegram. [8]

In May 2019, President Putin signed a law aimed at achieving the "sovereignization" of the Russian segment of the internet, or Runet. [9] Its basic provisions took effect in November 2019. Other elements of the law, including the creation of a national domain name system (DNS), will take effect in 2021. [10] The law defines the status of and requirements for the "critical infrastructure" of the Runet, namely international communication links 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. For example, the law attempts to ensure the operability of Russian internet resources in the event that Russian service providers are unable to connect to root DNS servers located abroad. The law also provides for the creation of a Russian 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. Russian national security authorities have regularly criticized ICANN for being dependent on the US government and have often suggested delegating its functions to an independent international organization. Notably, the law requires service providers to install special equipment that would enable Roskomnadzor to filter traffic. Such equipment, harnessing DPI technology, could bring about a new, more effective website-blocking regime in Russia, which currently blocks sites according to IP addresses.

Implementation of the law has been somewhat delayed. Although it came into force in November 2019, secondary regulations necessary for its implementation were developed only by the end of the coverage period; at the time of the law's effective date, only seven of 26 required bylaws had been adopted. [11] This lag can be explained by procedural problems and the difficulty of interagency coordination. Implementation was further set

back by a failure to prepare certain technical infrastructure within the original deadlines, and the onset of the COVID-19 pandemic may have contributed to additional delays.

In late 2019, equipment to be installed in accordance with the law, including DPI systems, was tested in the Ural Federal District. There were several episodes of reduced internet speeds in connection with the test. However, no significant network disruptions were reported. [12]

The Sovereign Runet Law calls for government authorities, ISPs, and other network operators to regularly simulate large-scale cyberattacks in order to be ready for the rapid restoration of the Runet's critical infrastructure and the isolation of the Runet from the global internet. The first round of simulations was conducted in late December 2019. [13] The Ministry of Digital Development, Communications, and Mass Media planned to hold four more simulations with different aims during 2020. [14] However, due to the COVID-19 crisis, these simulations were delayed indefinitely. [15]

In 2017, President Putin approved a new Information Society Development Strategy, which aims to guide ICT development until 2030. Like the Sovereign Runet Law, the strategy broadly seeks to increase the autonomy of Russia's internet, signaling the authorities' intention to wield greater control online. Among other things, the document states that imported ICT equipment should gradually be replaced with domestically made alternatives. [16] It also directs officials to ensure that Russian "spiritual and cultural values" are represented in internet governance policy (see B3).

A4 0-6 pts

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

The ICT market in Russia, despite robust competition among ISPs, remains relatively concentrated due to regulatory and economic constraints. The displacement of local service providers by larger

companies, as well as a number of mergers and acquisitions among these large players, particularly in the European part of Russia, has led to market consolidation. This enables Roskomnadzor to more easily secure the cooperation of service providers in carrying out its content-blocking procedures.

Telecommunications providers are licensed by Roskomnadzor. [1] The costs of complying with data retention requirements under the 2016 Yarovaya Law (see C6) and the installation of DPI systems under the Sovereign Runet Law created a financial hardship for existing service providers and a deterrent to potential new entrants to the market. These costs are compounded by the government's import substitution policy, which asks ICT companies to use hardware and software that is produced domestically. [2] The looming possibility of further state intervention in the ICT sector constitutes an additional risk to operators.

On the consumer side, state-owned Rostelecom commands 41 percent of the fixed broadband market by revenue. The private firms ER Telecom and MTS held 11 percent and 8 percent, respectively, as of 2019. [3] The remaining market share is split among smaller, local ISPs.

The vast majority of the mobile market is controlled by four service providers. According to the leading provider's 2019 annual report, these companies—MTS (30 percent), MegaFon (29 percent), VEON (21 percent), and Tele2 (17 percent)—account for 97 percent of the market. [4]

In March 2019, Rostelecom reported that it would soon assume a controlling stake in Tele2, having previously held a 45 percent stake. [5] Rostelecom's board of directors approved the parameters of the transaction in November 2019, and it was completed in March 2020. [6]

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

Score Change: The score declined from 1 to 0 because the internet regulator Roskomnadzor, which is not impartial or independent in practice, received enhanced powers under the new Sovereign Runet Law.

Roskomnadzor regulates the ICT and media sectors. It often fails to act fairly or transparently. Under the control of the Ministry of Digital Development, Communications, and Mass Media, 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). [1]

In March 2020, Andrey Lipov was appointed as the new head of the agency, replacing Zharov, who had held the post since 2012. 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. [2] A number of new deputy managers who previously worked at Lipov's directorate were also transferred to Roskomnadzor. These appointments underscored the agency's increasing importance and stature within the framework established by the Sovereign Runet Law.

Roskomnadzor's powers have gradually expanded under this law. A body called the Center for Monitoring and Management of Public Networks was formed within the agency as part of the legislation. [3] It is primarily responsible for the implementation of certain provisions, particularly the collection, processing, and storage of information on IXPs and other network infrastructure, the control of cross-border communication links, and the maintenance of "threat countering" equipment. [4] 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. [5]

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. [6]

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

B. Limits on Content

The authorities continued to vigorously police online content, expanding the scope of technical censorship to cover encrypted email services. A law passed at the end of 2019 raised the stakes for noncompliance with a variety of regulations governing online content, for example by setting higher fines for search engines that refuse to connect to Roskomnadzor's blacklist. Amendments to the so-called foreign agents law put more pressure on media outlets and civil society groups working online. However, the coverage period also featured the development of novel digital protest tactics related to the September 2019 elections in Moscow and the COVID-19 pandemic.

B1 0-6 pts

Does the state block or filter, or compel service providers to block or filter, internet content?	**1** / 6

Russian authorities routinely restrict access to sensitive political and social content on the internet. Citing a range of justifications, they also restrict, or have attempted to restrict, many social media and communication platforms. According to unofficial data, over 4.74 million internet resources were blocked in Russia at the end of 2019. Officially, only about 315,000 internet resources were blacklisted. [1]

Telegram, the popular messaging app, remained officially blocked in Russia through the end of the coverage period. In April 2018, a district

court had ordered Telegram blocked for refusing to comply with the Yarovaya Law, which obliges the app to provide its encryption keys to the government (see C4). Officials have repeatedly asserted that Telegram is used for terrorism-related purposes. Telegram employed various methods to overcome the initial blocking, including the use of alternate cloud-hosting services. Roskomnadzor then targeted many of these services, including Alibaba Cloud, Amazon Web Services, Google Cloud, and Microsoft Azure, resulting in extensive collateral blocking. At one point, over 18 million IP addresses were blocked, affecting online stores, banks, airline ticketing systems, news sites, and other social media and communication platforms such as Viber and Odnoklassniki (OK). [2] In January 2019, Roskomnadzor signaled that it was easing its blocking regime, announcing that it had unblocked 2.7 million Amazon Web Services IP addresses. [3] However, at the end of May 2020, more than 675,000 IP addresses remained blocked in connection with the Telegram order, according to a monitoring project. [4]

After the coverage period, in June 2020, the government abruptly reversed its ban on Telegram, citing its founder's "readiness" to "counter terrorism and extremism." [5] The reasons for this reversal are opaque. Observers speculated that the government, realizing the practical impossibility of restricting access to the app, had been searching for an opportune moment to unblock it. The moment came after the leadership shakeup at Roskomnadzor—outgoing chief Aleksandr Zharov had publicly declared that Telegram would remain blocked until it complied with the Yarovaya Law, which, apparently, it still has not—and against the backdrop of the COVID-19 pandemic, during which authorities used Telegram to communicate with the public. [6]

Despite authorities' efforts to restrict access to it, Telegram remained available to Russian users. During the coverage period, most continued to reach Telegram without a virtual private network (VPN), since its developers implemented an automatic proxy feature in order to provide unfettered access. [7]

Other messaging apps remained blocked during the coverage period. Zello was blocked in 2017 by Roskomnadzor for refusing to hand over its

encryption keys under the Yarovaya Law and for failing to register as an "information dissemination organizer" under the Law on Information, Information Technology, and Information Protection, which would grant authorities access to much of the service's data (see C6). [8] BlackBerry Messenger, Imo, Line, and Vchat were blocked for similar reasons in 2017. [9]

Websites featuring content that touches on a host of sensitive topics are also 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). In October 2019, the independent news outlet Fergana News was blocked for reporting on a suicide. [10] Other categories of content are also censored on a less formal basis.

A number of different government bodies are empowered to order the blocking of web content (see B3). For example, the Ministry of Internal Affairs blocked almost 21,000 internet resources containing information about illegal drugs in 2019. [11] The Prosecutor General's Office blocked 81,000 websites that allegedly hosted extremist content that year. [12] However, the Federal Agency for Youth Affairs, which can order the blocking of content that encourages minors to break the law, has been relatively inactive in this regard, initiating only 10 blockings in total by March 2020. [13] The courts also have wide latitude to block web content.

VPNs have recently faced pressure from authorities. In a March 2019 letter, Roskomnadzor asked 10 VPN service providers to restrict users' access to websites that are blocked in Russia. [14] If they failed to comply, Roskomnadzor threatened to "limit access" to the VPN services themselves. In June 2019, Roskomnadzor announced that only one company, the Russia-based Kaspersky Secure Connection, complied with its request. [15] The agency declared that the other nine VPN services would be blocked imminently, but several days later, Zhanov stated, "We

may wait for the adoption of the new law on fines" for noncompliance with internet-related regulations. [16] However, the law in question, adopted in late 2019 (see B3), did not include any provisions concerning VPN services. By May 2020, Roskomnadzor had not made any attempt to block these services.

Other circumvention and encryption tools have come under official scrutiny. In March 2019, it was revealed that the two largest Russian ISPs, MTS and Rostelecom, restricted traffic to several nodes of the anonymous web browser Tor, along with the simple mail transfer protocol (SMTP) servers of ProtonMail, an encrypted email service. [17] 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." According to established procedure, ProtonMail's refusal to register would have allowed Roskomnadzor to initiate blocking procedures. [18] ProtonMail subsequently introduced special technical functions to prevent traffic restrictions in Russia. [19]

Russia's national security authorities initiated a new blocking campaign against encrypted email services in early 2020, ostensibly in response to a growing number of false and anonymous email messages reporting the presence of explosive devices in public spaces. Officials targeted services including Tutanota, [20] SCRYPTmail, [21] StartMail, [22] and ProtonMail, [23] arguing that they were facilitating calls for extremist activities.

In February 2020, ProtonMail agreed to comply with the Law on Information, Information Technology, and Information Protection by deleting fraudulent accounts from its service. At the same time, the company, which is headquartered in Switzerland, declared that it would only provide data on users to Russian authorities on the basis of decisions by Swiss courts. [24] As of May 2020, some Russian ISPs still restricted access to ProtonMail. Also in February 2020, Mailbox.org, another encrypted email service threatened with blocking, agreed to register as an "information dissemination organizer." [25]

The attempts to block these services are not fully supported by Russian legislation. In addition to blocking them by their IP addresses, the authorities requested that Russian mail services prevent their users from receiving messages from StartMail and ProtonMail. [26] This blocking mechanism is not reflected in current legislation, but would be provided under a bill introduced in the lower house of parliament in October 2019, which had yet to pass even its first reading (see B3). Since national security authorities considered false and anonymous messages to be a highly sensitive problem, they moved to restrict such communications before the necessary legal basis was established.

A 2015 law allows the government to designate foreign organizations as "undesirable," which bars them from disseminating information (see B3). As of May 2020, a total of 22 foreign organizations—including Open Russia, an NGO founded by Kremlin critic Mikhail Khodorkovsky, and the Open Society Foundation, created by philanthropist George Soros—were listed as undesirable; in some cases, their websites are blocked. [27] During the coverage period, the Prosecutor General's Office added seven foreign organizations to the list, including the US-based Atlantic Council, Free Russia Foundation, and Jamestown Foundation, as well as the Czech-based People in Need. The websites of the Free Russia Foundation and People in Need were blocked, while the websites of the Atlantic Council and the Jamestown Foundation remained accessible.

Rules for personal data localization (see C6) are used 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, [28] and it remains the most notable blocking of its kind. Roskomnadzor's leadership has repeatedly asserted the need to apply similar measures to Twitter and Facebook. In April 2019, however, the two companies were fined a token 3,000 rubles ($45) for their noncompliance. [29] Legislative amendments that were adopted in late November 2019 and signed by President Putin in December gradually increase such fines until they are large enough to affect companies' revenues without exposing their platforms to the threat of blocking. [30] In addition to repeated violations of data localization requirements, the stronger fines can be imposed for illegal activities of

audiovisual services, search engines' noncompliance with Russia's blacklisting system, and messaging apps' refusal to provide national security authorities with encryption keys at their request (see B3). In February 2020, a court fined Twitter and Facebook 4 million rubles ($62,000) each after they failed to meet a deadline to inform Roskomnadzor that they had complied with the data localization rules. [31] However, as of the end of the coverage period, both companies had reportedly neglected to pay the fines. [32]

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?	**1** / 4

During the coverage period, Roskomnadzor frequently mandated the removal of online content or pressured users to delete content, including through the use of new laws that further constrain free expression in the digital environment. The agency claims that, in cooperation with social media platforms and other technology companies, it removes an average of 2,500 items related to suicide, 1,300 related to extremism or terrorism, 800 related to illegal drugs, and 300 related to child sexual abuse images each week. [1]

New articles proscribing 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 total number of cases initiated under these articles is comparable to the peak number of criminal cases for extremist activities via the internet as of mid-2018. [2] In April 2020, Roskomnadzor reported that after the introduction of the article on fake news in March 2019, the agency had removed 233 items through the end of 2019 and 172 items since the beginning of 2020. [3] The 2020 figure was expected to significantly increase, as Roskomnadzor actively began to block allegedly false news about COVID-19; in some cases the agency targeted genuine misinformation, but in others it blocked independent reporting about the epidemiological situation in the country. [4] In late March 2020,

the parliament adopted a law to increase fines for fake news about COVID-19 and other circumstances that posed a danger to the health and safety of citizens (see C2). Through June 4, 2020, the Prosecutor General's Office requested that Roskomnadzor block 120 fake news items related to COVID-19. [5]

In November 2019, acting on a request from the Prosecutor General's Office, Roskomnadzor blocked a page on the stock image service Shutterstock with a depiction of the Russian flag that allegedly defamed state power, pressuring the company to take the image down. Similar actions were taken in relation to the well-known websites 2ch, Archivist, Risovach, and LiveInternet, in addition to popular social media platforms such as Facebook, Instagram, Twitter, and YouTube (see below). [6]

The authorities have also continued to restrict online content for allegedly promoting drug use. In December 2019, the Russian outlet The Village removed an article about a convicted drug dealer. [7] In October of that year, the Russian website Baza removed an article about ketamine at Roskomnadzor's request. [8] In August 2019, the independent news outlet Meduza, which is based in neighboring Latvia to avoid censorship, restricted Russian users' access to an article about drug use after Roskomnadzor demanded its removal. [9] In 2018, the Russian website Batenka complied with Roskomnadzor's instructions to delete an article about a model struggling with addiction; in January 2020, the Supreme Court rejected an appeal against the order by the website's editors. [10]

In addition, online content about evading censorship and surveillance has been targeted for removal. In September 2019, the Russian outlet Lifehacker removed a YouTube video titled "How to Bypass Blocking of Sites and Trackers" at the request of a Russian court. That same month, the Russian human rights organization Team 29 removed an article titled "How to Bypass Site Blocking" from its website, also at the request of a Russian court. In both cases, the authorities argued that the resources could enable users to access a specific extremist Islamic text. [11]

In December 2018, Roskomnadzor fined Google 500,000 rubles ($7,800) for the company's refusal to connect to the regulator's registry of banned

websites in order to filter search results (see B3). [12] Two days after the Google fine, the Russian search engine Yandex began filtering search results in connection with Roskomnadzor's blacklist. [13] Google reportedly began to filter search results using the registry in February 2019, but in July of that year the company was again fined for failing to do so. [14]

During the reporting period, the right to be forgotten was routinely applied to require search engines to delete links to websites that contained personal information about an individual if it was no longer considered relevant. Russian law does not provide specific criteria governing the right's application. In the spring of 2019, the SOVA Center, a Moscow-based think tank, challenged the right to be forgotten in the Constitutional Court. The court rejected the center's complaint and refused to establish clear guidelines for deleting and deindexing content under the right to be forgotten. [15]

According to a transparency report from Google covering the second half of 2019, the number of content removal requests issued by Russian government agencies decreased slightly to 8,669. Google complied with about two-thirds of these requests. [16]

According to Facebook's transparency report, the company restricted access to 2,900 items for allegedly violating local laws related to extremism, disrespect for state symbols, the sale and use of regulated goods, self-harm, and suicide promotion in the second half of 2019, a record number for Russia. [17] Facebook did not report either the total number of content removal requests it received from Russian government or the percentage of requests it complied with.

According to Twitter's transparency report for the second half of 2019, Russian authorities submitted 6,107 content removal requests, including court orders. Twitter complied with 35 percent of these requests. [18]

According to Reddit's transparency report for 2019, the company received 36 requests to remove content from the Russian government. [19]

Russian social media platforms do not disclose the number of content removal requests they receive from the government, with the exception of

the blogging platform Habr. In 2019 and 2020, Habr received six requests to restrict access to content from Roskomnadzor. [20] In 2020, VKontakte (VK), the most popular Russian social media platform, debuted an algorithm that automatically removes content included in the federal list of extremist materials from users' personal correspondence. [21]

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.

Website owners can, in theory, also appeal restrictions at the European Court of Human Rights (ECtHR), since Russia is a signatory to the European Convention on Human Rights. However, a 2015 law gives the Russian government the right to ignore ECtHR rulings, [1] meaning the court offers only a limited avenue of appeal.

The following were among the relevant ECtHR cases during the coverage period:

- In June 2019, Yuriy Kartizhev, the first Russian fined under the law on defamation of the authorities adopted that March (see C2), lodged a complaint with the ECtHR. [2]
- In September 2019, Russian company Live Photography appealed to the ECtHR, accusing Roskomnadzor of illegally blocking several internet resources that were critical to the operation of the company's website as part of its attempts to block Telegram. [3] The company's

previous efforts to sue Roskomnadzor in Russian courts were unsuccessful. [4]

- In December 2019, blogger Vladislav Sinitsa, who had been sentenced to five years in prison for a social media post as part of a larger prosecution of 24 people in connection with antigovernment protests in Moscow in the summer and fall of 2019, filed a complaint with the ECtHR (see C3). [5]
- In January 2020, the ECtHR communicated a complaint from Ruslan Sokolovsky, a blogger who was convicted in 2017 under Article 148 of the criminal code—violation of the right to freedom of conscience and religion—for a YouTube video in which he played the mobile game Pokémon GO in a church. [6]
- In February 2020, the ECtHR communicated a complaint from the independent news outlet Mediazona and the opposition politician Aleksey Navalny after Roskomnadzor demanded that they remove materials about wealthy industrialist Oleg Deripaska and sex worker Nastya Rybka. [7]
- Also in February 2020, the administration of the website Gay.ru, which is blocked in Russia, appealed to the ECtHR. In 2018, a Russian court had found that Gay.ru illegally distributed “information promoting nontraditional sexual relations,” including among minors, and ordered the blocking. [8]

The government grants the authority to block various categories of online content to several state bodies, including Roskomnadzor, the Prosecutor General’s Office, the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing (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). [9] In August 2019, Roskomnadzor published a draft order on behalf of several agencies that established criteria for determining that content is subject to extrajudicial blocking, superseding a set of criteria laid out in 2017. The order took effect in September 2019. 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. [10] It and other agencies can block content that touches on political and social issues enumerated in the Law on Information, Information Technology, and Information Protection, plus related legislation, including legislation prohibiting fake news and content that defames the authorities (see C2). Any other online content may be blocked by a court order if it is found to violate the law. Roskomnadzor typically handles blocking orders from other agencies in addition to the judiciary. For orders to block content on a website, Roskomnadzor instructs the hosting provider to issue a takedown notice to the website owner. Most website owners quickly delete the content in question rather than risk the blocking of their entire site. If the content is not removed, it is included on a blacklist, and ISPs must block it. If an order seeks to block an entire website, Roskomnadzor simply includes that website on its blacklist.

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

Restrictions on online content are generally implemented opaquely, and official information does not provide a complete picture of internet censorship in Russia. According to the NGO RosKomSvoboda, which monitors online censorship, as of May 2020 approximately five million internet resources were blocked in Russia without reference to the decisions of either courts or state bodies, representing about 94 percent of the total blocks in place. The remaining 6 percent—around 316,000 internet resources—were blocked in relation to decisions by the courts or state bodies. [11] The extent to which Roskomnadzor effectively blocks websites is unclear, and some reports indicate that over half of the websites blacklisted by the regulator continue to operate. [12]

Roskomnadzor has additional powers to issue warnings to organizations that are officially designated as mass media and are deemed to abuse their position. [13] 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.

During the coverage period, the government continued to expand the legal framework that undergirds internet censorship in Russia.

In December 2019, President Putin enacted a law that set higher fines for noncompliance with a variety of regulations, including data localization requirements, requirements for messaging apps to hand over encryption keys, requirements for search engines to connect to Roskomnadzor's blacklist, and requirements for "information dissemination organizers" to retain user data and provide them to the authorities. [14] The law also raises the financial stakes for disseminating calls for extremist or terrorist activities, along with other categories of prohibited information.

Also that month, Putin signed a law that extends the state's regulation of media outlets designed as "foreign agents" (see B5) to individuals who "spread information to an unrestricted number of persons, namely on the internet, and receive funding from abroad." [15] The law empowers the government to block so-called foreign agents' websites, potentially including their social media accounts.

In October 2019, a group of lawmakers introduced a bill to the lower house of parliament that would empower Roskomnadzor to order "information dissemination organizers" to restrict messages from particular email services (see B1). [16] If adopted, the bill could legitimize the restrictions already placed on messages from the ProtonMail or StartMail encrypted email services. However, despite receiving positive feedback from the government, the bill did not make significant progress during the coverage period, probably due to the slowdown in lawmaking activities

caused by a government reshuffle and the escalating COVID-19 pandemic.

In a joint report concerning pressure on internet freedom in Russia in 2019, the Agora human rights group and RosKomSvoboda noted that the scale of restrictions on access to information issued by Russian government agencies increased by 70 percent that year. Such restrictions encompass all cases of governmental interference in the freedom to receive and disseminate information on the internet. [17]

Providers of public internet connections, including libraries, cafés, and educational institutions, are responsible for ensuring that content available to their users is filtered in compliance with Article 6.17 of the code of administrative offenses, which is meant to protect children from harmful content. [18]

B4 0-4 pts

Do online journalists, commentators, and ordinary users practice self-censorship?	**2** / 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 poor governance, corruption, the conflict in Ukraine, the annexation of Crimea, 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. [1] The government's crackdown on online news media, as well as social media, has intensified self-censorship among journalists in particular. IREX's 2019 Media Sustainability Index observes, "Self-censorship has become an inextricable part of the journalism practice." [2] Electronic surveillance by the FSB, the police, and other state actors also intimidates many journalists and ordinary users into self-censorship. [3]

During the coverage period, the authorities used various drug-related charges as pretexts to censor the news media. Though the most prominent case of this kind—that of Meduza journalist Ivan Golunov—involved a fabricated offline offense, [4] various online publications were removed or blocked after being deemed to promote drug use (see B2). Several outlets were forced to self-censor on this issue. [5] In January 2020, the government submitted a bill to the lower house of parliament that would impose fines of up to 1.5 million rubles ($23,000) for promoting drugs and psychotropic substances on the internet. [6] In February, a parliamentary committee prepared 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 12 years in prison. [7] The COVID-19 pandemic prevented progress on these amendments in the spring of 2020, though they were still expected to be considered. [8]

Despite the challenging environment, many journalists and ordinary users continue to test the limits of the authorities' tolerance, particularly on Telegram channels.

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 distorts the online information landscape. Authorities use paid commentators, or trolls, and automated "bot" accounts to influence online content. This issue came to international prominence following revelations that Russian trolls and bots had attempted to influence the 2016 US presidential election by manipulating online discussions and disseminating disinformation through social media. [1] Well before that controversy, however, investigations had revealed that a "troll factory," the Internet Research Agency in Saint Petersburg, used a network of trolls to attack both domestic and international targets.

Domestically, Russian trolls and bots have been observed commenting on news sites and on social media, usually to defend President Putin while smearing his critics, including journalists (see C7). For example, ahead of the contested 2019 regional elections in Moscow, the city's government deployed troll factories to boost progovernment candidates and mock the opposition, while also paying for advertisements and sponsored posts on popular social media pages and websites. [2] Ahead of a June 2020 national referendum on constitutional amendments that reset Putin's term limits, a number of social media influencers reported that the government offered them lavish sums to surreptitiously promote the president's cause. [3]

Outside Russia, Kremlin-linked trolls and bots have been observed sowing disinformation in dozens of countries, including the United States, but mostly in post-Soviet countries. In October 2019 and February, March, and April 2020, Facebook removed networks of Russian-linked Facebook and Instagram accounts for engaging in "coordinate inauthentic behaviour," some of which the company traced back to Russian military intelligence services and the Internet Research Agency. [4] In March 2020, Twitter removed 70 inauthentic accounts that "attempted to sow discord" by engaging in conversations about social issues, like race and civil rights; the platform said it could "reliably" tie the accounts to Russia. [5]

In early 2020, thousands of Russian government-linked social media accounts launched a coordinated effort to spread disinformation about COVID-19, disrupting efforts to fight the pandemic, including by amplifying locally produced misinformation around the world. This campaign has taken aim at the governments of the United States and Ukraine. [6]

At home, the government has sought to carefully control the narrative around COVID-19 through state-run and state-aligned media. Beyond demanding the removal of information that reflects unfavorably on the government's response to the pandemic (see B2), [7] officials have reportedly barred medical workers from giving interviews to the press and ordered health care administrators to seek approval before speaking publicly. [8]

Authorities increasingly use the 2012 law on “foreign agents” to smear organizations known to be critical of the government. The law, which was strongly opposed by Russian and international human rights organizations, [9] requires NGOs that receive some foreign funding and engage in vaguely defined “political activities” in Russia to register as “foreign agents.” Under 2017 amendments to the Law on Mass Media, [10] the government can designate media outlets receiving foreign funding as “foreign agents,” requiring them to reveal detailed financial information or face fines (see B6). [11] Outlets now considered foreign agents include Voice of America, Radio Free Europe/Radio Liberty (RFE/RL), and the local services of RFE/RL. [12] These amendments were adopted in response to the United States compelling the Russian state-run television network RT to register there as a foreign agent. The Russian law was expanded at the end of 2019 to apply to individuals who disseminate information online and receive foreign funding (see B3).

On the Russian internet, foreign and independent news outlets must contend with a powerful array of state-run and -aligned media outlets that set the domestic agenda. According to 2019 survey data from the Levada Center, just 35 percent of Russians consume news from independent outlets. [13] Television, rather than the internet, remains the primary source of information, [14] though trust in the media in general is low. [15]

The authorities use the 2019 law against fake news to smear bloggers and other independent news sources. Roskomnadzor has piloted a public list of information resources that “repeatedly disseminate false information” on its website, ostensibly so that media outlets know not to cite them. [16] However, it compiled the list in a haphazard manner, initially including the widely respected business daily *RBC*. [17]

B6 0-3 pts

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

There are a number of economic and regulatory constraints that limit users’ ability to publish content online. Onerous regulations and restrictive

laws affecting online news media have pushed some outlets to downsize, change owners, or exit the market altogether. Amendments to the Law on Mass Media that came into force in 2016 prohibit foreign citizens and organizations from owning more than a 20 percent stake in a Russian media outlet. As a result, foreign media holdings have left Russia and, in some cases, transferred ownership to Russian entities. [1] According to Roskomnadzor, 821 media outlets changed their shareholder structure shortly after the amendments entered into force. [2]

The foreign agents law is also employed to limit users' ability to publish content online. For example, by January 2020, a court in Moscow had fined the human rights NGO International Memorial 22 times for allegedly failing to label itself as a foreign agent on its websites and social media accounts. The fines totaled 4.5 million rubles ($70,000). [3] That month, Roskomnadzor drew up four administrative protocols against the Samara-based online outlet Gagarin Park for not labelling itself as a foreign agent on its social media accounts. [4] National Public Organization for Human Rights chairman Lev Ponomarev was also repeatedly fined in 2019–20 for failing to label his group's website. [5] A third human rights group, the Public Verdict Foundation, was fined 400,000 rubles ($6,200) under the foreign agents law in March 2020 for not labelling its YouTube channel. [6]

These fines limit the viability of independent publishing in Russia. In December 2019, they were increased to a maximum of 5 million rubles ($78,000) (see B3). [7] Fines against individuals for posting social media content that violates the law (see C3) also restrict independent publishing. Users convicted of extremism or other offenses involving mass media or the internet are legally barred from serving as editors in chief at publications. [8]

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. [9]

B7 0-4 pts

Does the online information landscape lack diversity?	

2 / 4

Russia's online information landscape is relatively diverse, although the range of news and opinion available to ordinary users has been curtailed by the government. As the space for independent print, radio, and broadcast media shrinks, online publications and social media have become increasingly important platforms for critical expression and civic mobilization. Several online resources, including Google, Yandex, VK, YouTube, and Mail.ru, are more popular than the largest television channels among younger urban audiences. [1]

According to a survey published by the Public Opinion Foundation in September 2019, although television remains the main source of information for Russians, a growing share (44 percent) get their news from online sources. Confidence in information from the internet is increasing, even as confidence in information from television is decreasing. [2] Similar results were reported in 2020 by the Levada Center, although its research found that trust in television has stabilized. [3]

Russian users can still access critical content online, but independent outlets increasingly publish from abroad due to the repressive environment at home. For example, during the coverage period, several veteran journalists set up an investigative portal titled Vazhnie Istorii (Important Stories) that is based in neighboring Latvia. [4] Many independent online media outlets within Russia have been forced to shut down in recent years due to government pressure. Human rights organizations have noted the intensification of government pressure, with Roskomnadzor and other state agencies penalizing outlets that take an independent editorial line (see C3). [5] In March 2020, a progovernment editor-in-chief was installed at the renowned business daily *Vedomosti*, allegedly at the behest of the Kremlin. [6] The new editor promptly barred the outlet's reports from referencing sources deemed unfriendly to the government, [7] and deleted an op-ed criticizing a state-backed oil and gas company. [8]

Although VPN usage remains low overall, some people use the services to circumvent censorship. More than 20 percent of Russians between 18 and 24 used VPNs in 2018. [9] During the coverage period, Russians represented the second-largest share of Tor relay and bridge users. [10] Due to Roskomnadzor's threats against VPNs (see B1), at least one provider, Avast, discontinued its VPN service for Russian users. [11]

B8 0-6 pts

Do conditions impede users' ability to mobilize, form communities, and campaign, particularly on political and social issues?	**4** / 6

Despite sustained pressure from authorities, the internet remains the most versatile and effective platform for activism in Russia, facilitating efforts to confront propaganda, hold officials to account, and organize protests. However, the government has sought to block mobilization tools, including Telegram (see B1). A 2019 report from the OVD-Info human rights project highlighted how the government restricts freedom of assembly online. Those calling for demonstrations on the internet may face criminal or administrative penalties, and the government sometimes restricts connectivity before and during demonstrations, as in Ingushetia in 2018 and 2019. Other tactics the government employs to constrain mobilization include hacking activists, monitoring activists' social media profiles, placing informers in public or private chat groups used to organize demonstrations, targeting journalists who cover protests, and otherwise preventing journalists from gathering information about protests and protesters. [1]

Restrictions on assembly put in place during the COVID-19 pandemic forced many Russians to turn exclusively to the internet to protest. [2] In April 2020, residents of Rostov-on-Don protested the government's response to COVID-19 by leaving comments en masse in the representation of the city's main square within the Yandex.Navigator navigation application. [3] The protests soon spread virtually to other cities, although Yandex began to remove users' comments. [4]

In addition, the pandemic has led Russian users to organize communal self-help over the internet. For instance, the independent Doctors' Alliance, a trade union, crowdsourced information from its members about shortages of personal protective equipment (PPE) and other problems in the health care sector, displaying it on an interactive map. [5] However, the government has taken aim at these initiatives, smearing one as an "opposition project" and claiming another was fomenting "clashes with the police." [6] The authorities has also moved to co-opt civic activism around COVID-19, backing the creation of several volunteering portals, including #WeAreTogether and We Will Continue to Act. [7]

In the lead-up to a referendum on constitutional changes that would reset President Putin's term limits, originally scheduled for April 2020 but postponed until a week-long period in June and July, Roskomnadzor blocked a website, Net2020.ru, that was set up by opposition politician Aleksey Navalny to coordinate his campaign against the amendments. [8] After the coverage period, in June and July 2020, the Safe Internet League, [9] a government-organized nongovernmental organization (GONGO), reportedly identified nearly 8,500 items of fake news related to the conduct of the referendum, such as a report from Navalny's campaign that election observers were being intimidated. [10] (The referendum was deeply flawed, according to observers, although some of the reports of fraud were indeed false. [11]) The Safe Internet League flagged these items for deletion orders by the Prosecutor General's Office and Roskomnadzor. [12]

In July and August 2019, a series of mass protests erupted in Moscow after independent candidates were disqualified from running in municipal elections scheduled for September. [13] Protests were organized online, and demonstrators used social media to amplify their message. Telegram in particular was used to track police movements and coordinate support for detained demonstrators. [14] Authorities attempted to clamp down on digital mobilization surrounding the protests by arresting online activists and journalists (see C3), disrupting internet service in some sections of Moscow (see A3), and instructing Google not to run ads promoting the protests. [15]

In September 2019, members of parliament who were investigating "foreign interference in the internal affairs of Russia" stated that Google, along with Facebook, had allegedly violated Russian law during the election period by providing a platform for political materials and electioneering. The lawmakers proposed tightening control over their activities in Russia, including through a special restrictive bill, though this was not introduced during the coverage period.

In December 2018, President Putin had approved a law introducing stiff fines and potential jail time for individuals or organizations that encourage minors to participate in unsanctioned protests (see C2). [16] Critics argued that the law was aimed primarily at Navalny, whose rallies are popular with young people. Navalny is a prominent social media user and often organizes his events online. The first prosecution under this law targeted a Navalny supporter who shared information about a protest on VK. He was found guilty in March 2019 and fined 30,000 rubles ($470). [17]

The authorities have since punished other Russians for the publication of posts urging people to participate in unauthorized rallies. Such prosecutions were observed in August 2019 in Moscow ahead of the contested elections. [18] In December 2019, one of the defendants, blogger Yegor Zhukov, was sentenced to three years' probation. The court found him guilty under Article 280 of the criminal code for publishing videos calling for antigovernment protests which could involve "an unlimited circle of individuals in extremist activities." [19]

During the COVID-19 pandemic, would-be protesters could be fined, and possibly even imprisoned, for violating quarantine protocols. [20]

C. Violations of User Rights

During the coverage period, "fake news" replaced "extremism" as the authorities' preferred pretext for prosecuting online expression. This trend accelerated amid the COVID-19 pandemic, which also prompted officials to pioneer new surveillance modalities, including location-tracking apps. At the same time, the pandemic's economic toll led the government to suspend certain data-retention rules and delay the implementation of a

law requiring Russian-made apps to be preinstalled on all new mobile devices.

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, [1] 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 possess the same rights as traditional journalists, such as receiving 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. Both outlets and individual journalists can be designated as foreign agents if they directly or indirectly receive funding from abroad (see B5). [2]

Russia's judiciary is not independent. The courts tend to side with the government, refusing to apply provisions of the constitution and international treaties that protect the rights of citizens. In 2019, the courts acquitted defendants in fewer than 1 percent of criminal cases. [3]

Russia remains a member of the Council of Europe and a party to the European Convention on Human Rights, which enshrines the right to free expression. However, a number of restrictive laws, coupled with repressive law enforcement and judicial systems, have eroded freedom of expression in practice (see C2).

C2 0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	**1** / 4

Users in Russia can face civil and criminal penalties under a range of laws, the majority of which are contained in the administrative and criminal codes. 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). [1] Article 6.21 of the administrative code prescribes fines for "advocacy of nontraditional sexual relations among minors," [2] while Article 148 of the criminal code bans insulting religious feelings, which is punishable by fine or imprisonment. [3] Articles 20.3 and 20.29 of the administrative code prescribe fines for displaying extremist symbols (such as Nazi symbols) and distributing extremist materials, [4] while Article 354.1 of the criminal code bans spreading false information about the Soviet Union's actions in World War II. [5] In March 2020, Article 20.3 of the administrative code was amended such that extremist symbols may be displayed without penalty for nonpropagandistic purposes. [6]

Articles 280 and 280.1 of the criminal code punish online calls for extremism and separatism with up to five years in prison, [7] while Article 282—prior to being revised at the end of 2018 (see below)—punished inciting hatred with up to six years in prison. [8] 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). [9] Those on the list are banned from certain professions, and their bank accounts can be frozen, even if they are not convicted.

Prosecutions of users for "extremist" activity on social media—mostly under Article 282, which prohibits incitement to hatred—peaked in 2017 at 1,521 cases, [10] before declining slightly in 2018 to 1,265 cases. [11] The vigorous enforcement of the law provoked a significant public backlash. In response, the parliament passed legislation easing penalties for inciting hatred, which was signed by the president in December 2018. [12] Those found guilty of making extremist statements online now face fines or up to 15 days in jail under a new provision in the administrative code, Article 20.3.1, although criminal prosecution under Article 282 is possible for repeated violations within one year. The new legislation also had

retroactive effect, giving authorities discretion to close Article 282 criminal cases and review all relevant convictions. According to official statistics, the number of prosecutions under Article 282 dropped to 585 in 2019. [13] The SOVA Center concluded in a 2019 report that, despite the partial decriminalization, antiextremist enforcement trends under other articles of the criminal code were growing worse, and the transparency of the relevant legislation was decreasing. The number of people convicted for "extremist" public statements remains high, and punishments are often not proportional to the social danger of the supposed crime. [14]

A pair of new laws signed in March 2019 introduced harsh penalties for online speech. One penalizes spreading fake news online under Article 13.15 of the administrative code. [15] Individuals or organizations found to have shared fake news face fines of up to 1.5 million rubles ($23,000), and if they do not remove the offending content, their websites can be blocked. The second law penalizes spreading 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. [16] Defamatory content on the internet must be removed within 24 hours of receiving a notice from Roskomnadzor. Since their enactment, these laws have been actively enforced by the authorities.

In early December 2019, the code of administrative offenses was significantly updated in terms of increasing fines for violation of various content distribution rules (see B3).

In April 2020, Putin signed a law that set increased penalties for spreading fake news related to the coronavirus. [17] Under this law, individuals can be fined up to 700,000 rubles ($11,000), or up 2 million rubles ($31,000) if the false information led to anyone's death, under Articles 207.1–2 of the criminal code, while media outlets and other legal entities can be fined up to 5 million rubles ($78,000) under Article 13.15 of the code of administrative offenses. [18] Individuals who share coronavirus-related fake news can be imprisoned for up to three years, or five years if the false information led to anyone's death. [19] On April 30, the Supreme

Court published clarifications on this law, stating that it could be applied only if two conditions are met: first, the perpetrators knew about the false nature of the information, and second, they knowingly presented it as if it were reliable information. [20] But even with these clarifications, the criteria for defining fake news remained vague, leaving the law open to abuse by law enforcement authorities. There were no reported cases of penal custody under this law during the coverage period.

In 2016, the government introduced the Yarovaya Law, which altered nearly a dozen extant laws with significant ramifications for internet freedom. [21] 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. [22] These harsh penalties, along with broad wording in the amendments, are vulnerable to abuse aimed at criminalizing legitimate, nonviolent expression online.

C3 0-6 pts

Are individuals penalized for online activities?	**1** / 6

Criminal and administrative charges are widely used to stifle critical discussion online. Individuals have been charged for their posts or reposts on social media. Many arrests for online activities within the coverage period fell under Articles 205.2, 280, 280.1, and 282 of the criminal code (see C2). However, in absolute figures, the number of criminal prosecutions fell sharply in 2019. [1]

A joint report by Agora and RosKomSvoboda identified 200 criminal prosecutions of users for their online activities in 2019, versus 384 in 2018. The number of prison sentences decreased slightly, from 45 to 38. The key factor behind these decreases was the partial decriminalization of offenses under Article 282 of the criminal code, which was applied far less frequently as a result. In 2018, according to Supreme Court data, there were 518 sentences under Article 282, while in 2019 there were only 36 (see C2). [2]

However, the outbreak of COVID-19 ushered in a new wave of repression. By early June 2020, according to Agora, the authorities launched 42 criminal prosecutions for the dissemination of “knowingly false information about circumstances that pose a threat to the life and safety of citizens” under the amended Article 270 of the criminal code. In addition, Agora recorded 157 cases under Article 13.15 of the administrative code during the first three months of the pandemic in Russia. [3]

The following were among the many prosecutions for online activities during the coverage period:

In July 2019, a military court in Samara sentenced Togliatti resident Aleksandr Dovydenkov to a year in prison, accusing him of publicly calling for terrorism, under part 2 of Article 205.2 of the criminal code, in a social media post about the 2018 bombing of an FSB facility in Arkhangelsk. [4]

In August 2019, a criminal case was initiated against the director of Aleksey Navalny’s Anticorruption Foundation, Ivan Zhdanov, for refusal to delete an online investigative video about then prime minister Dmitriy Medvedev. Zhdanov faced up to two years in prison. The video was watched by more than 33 million people on YouTube and prompted a wave of mass protests against corruption. [5] The case was ongoing at the end of the coverage period.

One of the comparatively few cases filed under Article 282 of the criminal code in 2019 involved blogger Vladislav Sinitsa. In late July 2019, amid a violent state response to protests in Moscow (see B8), he made a sharp comment on Twitter in which he threatened the families of police. Four days later, he was detained on charges of inciting hostility toward law enforcement officers combined with the threat of violence. In September 2019, he was sentenced to five years’ imprisonment. [6]

In December 2019, a Belgorod court ordered five days of detention for local resident Maksim Osetrov under Article 20.29 of the administrative code, over an eight-year-old social media post in which he shared a Navalny video about the ruling United Russia party’s 2002 electoral promises. [7] The same video resulted in fines for a number of other users

during the coverage period, even though they had shared it in 2011, two years before it was deemed “extremist.” [8]

In January 2020, the authorities initiated a criminal case against blogger Nikolay Gorelov under Article 354.1 of the criminal code. He was accused of rehabilitating Nazism after posting several fictitious monologues on VK, with characters including a milkmaid from North Korea, a pensioner from Smolensk, a plumber from China, Soviet leader Joseph Stalin, and Nazi leader Adolf Hitler. [9] The case was dropped in June 2020, just after the coverage period. [10]

In January 2020, the police opened a new administrative case, for the alleged promotion of “nontraditional sexual relations” among minors, against LGBT+ activist Yuliya Tsvetkova of Komsomolsk-on-Amur. The case was filed over a picture posted by Tsvetkova on VK with the words "Family is where the Love is. Support LGBT+ families.” [11] In July 2020, after the coverage period, she was fined 75,000 rubles ($1,200) for this offense. [12] She had previously been fined in a similar case in December 2019. Earlier in 2019, Tsvetkova was accused of violating Article 242 of the criminal code, which prohibits the distribution of pornography, for running a VK page called “Vagina Monologues”; this case was pending at the end of the coverage period. [13] The charge carries a maximum sentence of six years in prison. [14]

In March 2020, a resident of Kaluga, Ivan Lyubshin, was sentenced to five years and two months in a penal colony for a comment on VK about the bombing of the FSB building in Arkhangelsk; the alleged offense, under part 2 of Article 205.2 of the criminal code, was public justification of terrorism on the internet. This was the most severe punishment for online speech during the coverage period. In 2017, three criminal cases had been initiated against Lyubshin for other comments on VK. He was found guilty of extremism, but in 2019 that case was closed after the reform to Article 282 of the criminal code. He was also fined 200,000 rubles ($31,000) for allegedly rehabilitating Nazism, while charges of pornography distribution were dropped. [15]

In May 2020, police arrested Vladimir Vorontsov, a former police officer and the administrator of the VK group and Telegram channel “Police Ombudsman,” which is known for calling out abuses within Russia’s law enforcement agencies. [16] He was accused of extorting 300,000 rubles ($4,700) from a police officer, but many observers speculated that he was being punished for his exposés.

In 2019, 1 million rubles ($15,500) in fines were collected from citizens for online expressions of disrespect for President Putin, judges, or national security officials. Such penalties are most often imposed on Putin’s critics—44 out of 78 known cases by the beginning of 2020. [17] In a typical example, a 30,000 ruble ($470) fine was imposed on Sverdlovsk resident Aleksandr Skutin for “defamation of power” over a comment about Putin diving in the Gulf of Finland. [18]

Nevertheless, insulting the president was not the only reason for “defamation of power” convictions. In October 2019, a Nizhny Novgorod court fined KozaPress journalist Irina Slavina 70,000 rubles ($1,100) for commenting on the installation of a memorial plaque devoted to Stalin. In November, a Yekaterinburg court fined political analyst Fedor Krasheninnikov 30,000 rubles ($470) for “defamation of power” after he commented on his Telegram channel about the arrest of politician Leonid Volkov. [19]

C4 0-4 pts

Does the government place restrictions on anonymous communication or encryption?	**2** / 4

Anonymous communication is restricted in Russia, as are encryption tools.

A 2017 law mandates the blocking of VPN services that allow their clients to access banned content. [1] 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 blacklist (see B1). [2] Most of the VPNs immediately refused, and others

that had not received such a request preemptively refused. [3] By the end of May 2020, Roskomnadzor had not yet blocked any of the VPN services for refusing to cooperate.

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

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. [4]

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. [5] In November 2018, the government approved new rules requiring such platforms to verify users' phone numbers with the help of mobile service providers. [6] 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. [7] The rules came into force in May 2019. [8] Roskomnadzor interprets the rules to apply to both foreign and domestic platforms. [9] 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 ($80,000). Fines for failure to hand over encryption keys were increased in December 2019 (see B3). The Electronic Frontier Foundation has suggested that the impossibility of full compliance is a deliberate

feature of the law, giving authorities leverage over the affected companies. [10]

C5 0-6 pts

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

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

The government utilizes the System for Operational Investigative Measures (SORM) for its online surveillance activities. Under current legislation, in order to receive an operating license, ISPs are required to install equipment that allows security services to monitor internet traffic. Providers that do not comply with SORM requirements are promptly fined and may lose their licenses if problems persist. The latest version of the system, SORM-3, uses DPI technology, enhancing the ability of security services to monitor content on all telecommunications networks in Russia. The Sovereign Runet Law provided authorities with additional DPI capabilities, which were tested in late 2019. [1]

In December 2019, threat simulations were conducted pursuant to the Sovereign Runet Law. The Ministry of Digital Development, Communications, and Mass Media, Roskomnadzor, the Ministry of Emergency Situations, and various law enforcement agencies took part in these simulations. [2] Four more were planned for 2020 but put on hold due to the COVID-19 pandemic.

Also in December, 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. [3] However, implementation of the law was delayed until 2021 due to COVID-19, and the necessary subordinate regulations had not been prepared by the end of the coverage period.

Russian authorities are nominally required to obtain a court order before accessing electronic communications. According to Supreme Court data, in 2019 security services requested 514,974 court orders to tap telephones, open letters, and intercept electronic communications; the data were not disaggregated. Of these requests, 514,115—over 99 percent—were granted. [4]

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. [5] Experts note that there is no publicly available information about accountability for FSB officers who may abuse this power. [6]

In May 2019, RosKomSvoboda reported that the government was soliciting bids for a social media and news media monitoring service that would perform "sentiment analysis" of posts on platforms including Facebook, Telegram, Twitter, and VK, to determine whether they supported or opposed the government's positions. [7] In 2018, during the previous coverage period, the government awarded a larger contract for monitoring work of a similar nature. [8]

However, law enforcement agencies often conduct human monitoring of social media, mainly on VK, the most popular and most cooperative social media platform in Russia. For example, in the words of one former officer, personnel at the Anti-Extremism Center, known as Center E, both proactively "sort through shared posts on VK" and field complaints about "extremist" posts on social media from third parties. [9]

In February 2020, it became known 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." [10] Exactly how these services responded is not publicly known.

During the COVID-19 pandemic, the government stepped up mass surveillance of users through three internet-enabled tools. First, the government repurposed its growing network of security cameras equipped

with facial-recognition software to track the movements of COVID-19 patients in Moscow and elsewhere. [11] In some cases, individuals were targeted in error. For example, in Yuzhno-Sakhalinsk, a fine was issued for a violation of the self-isolation regime based on flawed data from a facial-recognition system. [12] Second, COVID-19 patients in Moscow who were required to remain at home were instructed to install the Social Monitoring mobile app, which tracks geolocation and also has access to a large amount of information on the host device. Users of this app regularly received notifications on the need to take a selfie to confirm compliance, also using a facial-recognition mechanism. If such a notification is ignored for an hour, users are almost guaranteed to receive a fine of 4,000 rubles ($60), which is very difficult for patients under the self-isolation regime to challenge. [13] By mid-May 2020, Muscovites using the app had reportedly racked up over 200 million rubles ($3.1 million) in fines. Third, in regions throughout the country, authorities mandated the use of electronic passes that accumulate data in the form of QR code information from the citizen's identification card and information on how he or she moves around the city. [14]

C6 0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	**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. [1] 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. [2]

Under provisions of the Yarovaya Law that came into force in July and October 2018, [3] service providers and "information dissemination organizers" 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. [4] Service providers must store users' browsing history for 30 days. [5] 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. [6] 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 ($160 million) in special equipment from the state corporation Rostech in order to comply with the Yarovaya Law. [7] Previously, service providers had warned that the legislation would impose excessive costs on them. MegaFon estimated the cost of enforcing the law at 40 billion rubles ($620 million) over five years; VimpelCom (VEON) estimated 45 billion rubles ($700 million), and MTS 60 billion rubles ($930 million).

Due to the COVID-19 pandemic, in May 2020 the government approved a temporary easing of 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. [8]

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. [9]

As of March 2020, 204 companies were in the register of "information dissemination organizers," including social networks, communication apps, online dating services, file-sharing services, and email platforms. [10]

The data localization law enacted in 2015 requires foreign companies that possess Russian citizens' personal data to store their servers on Russian territory, potentially enabling easier access for security services. [11] Some

foreign companies, such as Uber and Viber, [12] have moved to comply with the law.

C7 0-5 pts

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

Attacks on online activists and journalists are relatively common in Russia, and authorities rarely conduct meaningful investigations of such incidents.

In 2019, cases of violence or threats of violence in response to online expression were noted in 20 regions. In total, 57 cases were detected in 2019, compared with 59 in the previous year. [1]

In June 2019, blogger Vadim Kharchenko was beaten and stabbed by unknown assailants while meeting with a whistle-blower from the regional police in the city of Krasnodar. [2] Kharchenko, who posts political commentary and reports on his popular YouTube channel, said he was attacked in retribution for his videos.

Also that month, the editor in chief of *Snob*, Kseniya Chudinova, reported that an unknown person had entered the outlet's headquarters and "hammered the editorial office." [3]

In July 2019, in the Republic of Ingushetia, a former journalist for the opposition newspaper *Fortang*, Rashid Maysigov, was reportedly tortured in police detention. [4]

In October 2019, the blogger Ivan Lyubshin was abducted and beaten—allegedly by FSB officers, one of whom the blogger said he recognized—after which he was taken to the Investigative Committee. Lyubshin was convicted of publicly justifying terrorism, under part 2 of Article 205.2 of the criminal code, because of his comments on VK (see C3). [5]

In February 2020, *Novaya Gazeta* journalist Yelena Milashina and a collaborator, human rights lawyer Marina Dubrovina, were beaten by a group of unidentified assailants at a hotel in the Chechen capital of Grozny. Milashina was apparently attacked in retaliation for her published work, in which she reported on the Chechen government's vicious crackdown on the local LGBT+ community, along with other sensitive issues. She said she was likely tracked down after she posted a photo on Facebook of a grocery store on the ground floor of the hotel. [6]

In May 2020, paramedic Aleksandr Shulepov fell from a window in the hospital where he worked, sustaining critical injuries. Days earlier, Shulepov had posted a video to VK in which he claimed that he was forced to work with insufficient PPE, despite contracting COVID-19. [7] Shortly afterward, he recanted his complaints. Foul play was suspected but unconfirmed, as Shulepov's apparent accident was preceded by the deaths of two other medical workers, both of whom fell from windows. In addition, a number of government critics and investigative reporters have died in this manner in recent years, including *Novy Den* journalist Maksim Borodin in 2018. [8]

In addition to the use of violence, law enforcement agents apply other forms of pressure against journalists and hack their devices. [9]

In the fall of 2019, investigators who initiated a criminal case against Pskov journalist Svetlana Prokopyeva for alleged justification of terrorism hacked her iPhone, which they had previously seized during a house check. According to Prokopyeva, investigators looked at her correspondence in messaging apps, trying to interpret her messages as attempts to bribe criminal experts. [10]

The editor-in-chief of media outlet The Project, Roman Badanin, reported in October 2019 on threats to the outlet's journalists, cases of surveillance, and an attempt to hack their accounts (see C8). [11]

Online intimidation and physical violence against LGBT+ people has escalated since the adoption of the 2013 law banning so-called gay propaganda. [12] 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. [13]

C8 0-3 pts

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

Cyberattacks against independent media and civil society organizations continue to inhibit users' ability to access these resources. According to the joint report of RosKomSvoboda and Agora, 32 cyberattacks were identified in 2019, compared with 20 in the previous year. [1] The NGO Justice for Journalists documented three distributed denial of service (DDoS) attacks against media outlets in 2019. [2]

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.

In May 2019, for example, suspected progovernment hackers attempted to break into the Telegram accounts of Meduza's correspondent in Yekaterinburg, the editor in chief of the news website Znak, and several local reporters in the Ural Federal District. [3] These attempts coincided with popular protests in Yekaterinburg, which had attracted media attention.

In June 2019, local journalists in Yekaterinburg identified a new attempt to hack their Telegram accounts. In particular, unknown persons tried to access the accounts of the director of the Hearst Shkulev Digital network, Rinat Nizamova, and the founder of Znak, Aksana Panova. In addition, the political scientist Fedor Krashennikov reported an attempt to hack his Telegram account; he said the unknown attacker tried to delete his account without the possibility for restoration. [4]

In July 2019, Andrey Buzin, cochair of the Golos voter rights movement, announced that his Facebook and Telegram accounts were hacked. [5]

In October 2019, staff at the media outlet The Project reported attempts to hack into their Facebook, Gmail, and Telegram accounts after they started investigating the activities of Russian private military companies in Africa and the Middle East.

In November 2019, one of the leaders of the Russian Libertarian Party, Mikhail Svetov, said that someone tried to hack his accounts on social networks and other internet services, causing him to simultaneously receive password recovery notices from Amazon, Facebook, Twitter, and Sberbank. [6]

On Russia

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

See More ›

Country Facts

Global Freedom Score

20 /100 **Not Free**

Internet Freedom Score

30 /100 **Not Free**

Freedom in the World Status

Not Free

Networks Restricted

Yes

Social Media Blocked

Yes

Websites Blocked

Yes

Pro-government Commentators
Yes

Users Arrested
Yes

In Other Reports

Freedom in the World 2020

Other Years

2019

ADDRESS

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

GENERAL INQUIRIES
info@freedomhouse.org

PRESS & MEDIA
press@freedomhouse.org