Freedom House

Russia

	2014	2015
Internet Freedom Status	Partly Free	Not Free
Obstacles to Access (0-25)	10	10
Limits on Content (0-35)	22	23
Violations of User Rights (0-40)	28	29
TOTAL* (0-100)	**60**	**62**

* 0=most free, 100=least free

Population:	**143.7 million**
Internet Penetration 2014:	**71 percent**
Social Media/ICT Apps Blocked:	**No**
Political/Social Content Blocked:	**Yes**
Bloggers/ICT Users Arrested:	**Yes**
Press Freedom 2015 Status:	**Not Free**

Key Developments: June 2014 – May 2015

- In June 2014, the president signed new amendments to the criminal code that increased penalties for disseminating materials online related to "extremism" or religious hatred, and criminalized the financing of extremist activity—a vague term that has been applied to the work of nongovernmental organizations and independent media outlets (see **Legal Environment**).
- The government continued to censor content related to the conflict in Ukraine and antigovernment protests, and threatened to block entire platforms due to the increasing difficulty of blocking individual pages (see **Blocking and Filtering**).
- In July 2014, the president signed a new data localization law that required technology companies processing Russians' data to host the information on local servers. As companies decided how and whether to comply with the law ahead of the September 1, 2015, deadline, privacy advocates raised concerns that the rule could make Russians more susceptible to government surveillance (see **Media, Diversity, and Content Manipulation** and **Surveillance, Privacy, and Anonymity**).

Introduction

Internet freedom in Russia has deteriorated steadily over the past few years, with a steeper decline from 2013 to 2014 following the Euromaidan protests in neighboring Ukraine and Russia's subsequent annexation of Crimea. During this time, blocking of online content expanded significantly, and the government enacted a series of restrictive laws. Since mid-2014, the authorities have continued to constrict the environment for freedom of expression and information online by blocking or economically targeting critical media outlets, increasing criminal penalties for online activities, and prosecuting or arresting internet users for their posts.

In June 2014, the president signed new amendments to the criminal code that increased penalties for disseminating materials online related to "extremism," setting prison terms of up to five years, as well as increasing penalties for "inciting hatred" to terms of up to six years. Other amendments criminalized the financing of extremist activity—a vague phrase that has been applied to the work of nongovernmental organizations (NGOs) and independent media outlets. For example, the online news outlet Grani.ru, which had already suffered revenue losses after being blocked in March 2014 for allegedly extremist content, was unable to receive donations or funding due to these new amendments. In addition, in May 2015 a new law on "undesirable organizations" included bans on disseminating information from the blacklisted groups.

The government has continued to target social media and technology companies, though with varying success. Laws passed in May and July 2014 required the registration of bloggers and the storing of all Russians' data on servers located within Russia, but they have been difficult to enforce. Nevertheless, many are concerned that data-localization rules could make it easier for the Russian government to access internet users' information, infringing on their right to privacy. Meanwhile, the authorities continue to expand their capacity for surveillance of communications by requiring all internet and mobile service providers to upgrade to SORM-3 technology, which provides intelligence agencies with greater access to the content of communications through deep packet inspection (DPI).

Obstacles to Access

The internet penetration rate in Russia continues to grow, and the majority of would-be users can find internet access at an acceptable speed and for an affordable price. At the same time, the market for information and communication technologies (ICTs) is still heavily regulated, and most services are under direct or indirect state control.

Availability and Ease of Access

Internet access in Russia continues to expand. According to data from the Public Opinion Foundation, the internet penetration rate had reached 51 percent by the end of 2014, compared with 46 percent by the end of 2013.[1] The International Telecommunication Union (ITU) places the figure somewhat higher, reporting an internet penetration rate of 71 percent by the end of 2014, compared

1 Public Opinion Foundation, "Internet in Russia: Dynamics of Penetration. Fall 2014" [in Russian], December 29, 2014, http://bit.ly/1jR6MpM.

with 68 percent in 2013 and just 29 percent in 2009.[2] More than half of internet users are under the age of 35. The speed of access is also increasing: According to Akamai, the average connection speed in Russia was 9 Mbps by the end of 2014, which is significantly higher than in most other post-Soviet states.[3] In addition, the mobile phone penetration rate reached 155 percent in 2014,[4] meaning there were more subscriptions than inhabitants; for mobile broadband subscriptions, the rate was 65.9 percent.[5] According to a poll by the Russia Public Opinion Research Center, 55 percent of Russian internet users access the internet through smartphones, 73 percent with desktop computers, 33 percent with mobile phones, 41 percent via tablets, and 61 percent with laptops.[6]

There is no significant gender divide when it comes to internet access in Russia.[7] Nevertheless, there is variation in access among the regions, in terms of both speed and price. For instance, in Moscow and St. Petersburg, the average download speeds range from 16 to 19 Mbps, and the price of a monthly unlimited plan starts at US$6; in the rest of the country the average download speed is not more than 4 to 6 Mbps, while the minimum price in remote areas of the Far East is US$12 per month.[8]

The median monthly income of Russian citizens in 2014, according to the Ministry of Labor and Social Protection, was US$680 (using the average annual conversion rate from the ruble).[9] Therefore, the cost of internet access is about 1.3 percent of the average income, which indicates that access is relatively affordable. Indeed, according to figures cited by the authors of the study *Economics of the Russian Internet 2013–2014*, only 4 percent of Russians stated that they would like to use the internet but cannot afford it.[10]

In May 2014, the Federal Communications Agency awarded a 10-year, US$4.7 billion contract to Russia's largest state-owned internet service provider (ISP), Rostelecom, under which the company has committed to provide all settlements with a population of 250 to 500 people with points of internet access at speeds of at least 10 Mbps, entailing the installation of 200,000 km of fiber-optic cables. Internet access points will be established in more than 13,600 towns, reaching a total of some 4 million additional people.[11]

Restrictions on Connectivity

During the coverage period, there were no government-imposed internet outages or disruptions to communication platforms. However, in two separate incidents in August 2015, the telecommunications authority banned articles on Wikipedia and Reddit (both related to recreational drug use),

2 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2000–2014, http://bit.ly/1cblxxY.

3 Akamai, *State of the Internet Q4 2014 Report*, http://bit.ly/1OPtdHC.

4 International Telecommunication Union, "Mobile-cellular subscriptions," 2014, http://bit.ly/1jR6MpM.

5 Broadband Commission for Sustainable Development, *The State of Broadband 2015*, http://bit.ly/1QTuNrB.

6 Russian Association of Internet Communication and Higher School of Economics, *Economics of Runet, 2013–2014* [in Russian], December 17, 2014, http://bit.ly/1zQ6bLz.

7 Yuri Serebrov, "RuNet is slowly growing old," [in Russian] *Telecom Daily*, March 30, 2015, http://bit.ly/1XgEOCy.

8 Yandex.ru, "Internet in Russian regions" [in Russian], http://bit.ly/1LHD7dv.

9 Ministry of Labor and Social Protection, *Annual report for 2014 and prospectives for 2015* [in Russian], March 30, 2015, http://bit.ly/1NRUHOb.

10 Russian Association of Internet Communication and Higher School of Economics, *Economics of Runet*.

11 Rostelecom, "Rossvyaz and Rostelecom signed a contract to eliminate the digital divide" [in Russian], news release, May 14, 2014, http://bit.ly/1LHDftB.

leading ISPs to temporarily block each platform in its entirety, since both employ HTTPS on their websites, which prevents ISPs from blocking individual pages.[12]

In the summer of 2014, the Ministry of Communications announced the completion of a joint exercise with the Defense Ministry, the Interior Ministry, and the Federal Security Service (FSB), in which the authorities examined ways to disconnect Russia from the global internet. They tested the scenario of switching off the servers of the domains .RU and .РФ, which are located in Moscow, Novosibirsk, New York, Amsterdam, and Hong Kong. The exercise also simulated the deployment of an alternative system of domain-name servers hosted by Rostelecom. Officials claimed that the tests were only intended to prepare for cases in which the Russian internet is disconnected from the outside, on the initiative, for example, of the United States,[13] but journalists, referring to sources in the ICT industry, said that a test for switching off the internet in Russia from the inside was also considered.[14] At the same time, President Vladimir Putin made public statements declaring that Russia had no intention of limiting access to the internet. Given that Russia has over 300 companies that have purchased connectivity with outside providers, each of which would have to be shut off in order to completely disconnect the country from the global internet, it would be much more difficult for the Russian government to implement a so-called "kill switch" than it has been for other governments whose countries only had a few connections to the international infrastructure.[15]

ICT Market

The communications market in Russia is still relatively concentrated among a few companies. The five largest operators control 67 percent of the market for broadband internet access. The state-owned Rostelecom controls 36 percent of the market, followed by TransTelecom, ER-Telecom, MTS, and Vimpel Communications (Beeline).[16] The market for mobile phone access has become more concentrated over the past year: As of the fourth quarter of 2014, four major companies—Mobile TeleSystems, Megafon, Vimpel Communications, and Tele2—controlled 99 percent of the market, compared with 92 percent in 2013.[17]

Regulatory Bodies

The ICT and media sector is regulated by the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), under the control of the Ministry of Communications and Mass Media. The head of Roskomnadzor, Aleksandr Zharov, was appointed by executive decree on May 3, 2012. Roskomnadzor is responsible for carrying out orders issued by the Prosecutor General's Office to block content that is extremist or contains calls for participation in unsanctioned public actions, according to a new law that went into effect on February 1, 2014. As a result, Roskomnadzor has become a primary player in the field of controlling and filtering information on the internet.

12 Shaun Walker, "Russia briefly bans Wikipedia over page relating to drug use," *Guardian*, August 25, 2015, http://bit.ly/1hbj-dvn; Andrew Griffin, "Reddit banned in Russia because of one thread," *Independent*, August 13, 2015, http://ind.pn/1PvYKzY.

13 Nataliya Raibman, "Peskov: 'Mad voices' can demand to switch Russia off the internet" [in Russian], *Vedomosti*, October 1, 2014, http://bit.ly/1KltRXa.

14 "Putin and Security Council will discuss Russia's shutdown of the internet from outside" [in Russian], *Forbes Russia,* October 1, 2014, http://bit.ly/1LAqnSr.

15 Luke Johnson, "Explainer: Can Russia Disconnect From the Internet?" RFE/RL, October 2, 2014, http://bit.ly/1jy7mcC.

16 Anastasiya Gavrilyuk, "Broadband is at the limit" [in Russian], *Telecom Daily*, January 21, 2015, http://bit.ly/1W1YWG6.

17 Advanced Communication & Media, "Cellular Data, 4Q2014," accessed May 19, 2015, http://bit.ly/1MQTvt6.

Limits on Content

The benefits of increases in access and the expansion of internet infrastructure have been offset by increasing censorship. The government continues to block websites based on an expanding list of restricted content. The leading independent online news outlets that were originally blocked in the spring of 2014 for their critical coverage of the Kremlin are still restricted, while others, facing economic pressure, have changed their editorial positions to become less critical of the government. In addition, the authorities are increasingly pressing large foreign companies like Google, Twitter, and Facebook to comply with content-removal demands. Meanwhile, the government actively manipulates public opinion through state-controlled media and paid commentators.

Blocking and Filtering

Since June 2014, the government has continued to block content related to antigovernment protests, the conflict in Ukraine, or support of opposition figures. This campaign of censorship began in earnest in March 2014, when, in the run-up to the Crimean secession referendum, the prosecutor general issued an order to block access to three major opposition websites—Grani.ru, a news site known for its criticism of the Kremlin, particularly the crackdown on and subsequent prosecution of participants in the 2012 Bolotnaya Square protests; *Ezhednevny Zhurnal* (Ej.ru), a news and opinion site; and Kasparov.ru, the website of former chess champion and current opposition figure Gary Kasparov.[18] The owners of the websites were not provided with an explanation as to what content had violated the law and prompted the blocking order. At the same time, the authorities blocked access to the personal blog of opposition leader Aleksey Navalny and the website of the radio station Ekho Moskvy (Echo of Moscow), though these two were unblocked within a few days.[19]

In December 2014, ahead of the sentencing of Navalny and his brother Oleg in what was widely seen as a trumped-up fraud case, Roskomnadzor issued a request to Facebook to block an event page for a planned protest on Moscow's Manezh Square on January 15, which thousands of users had already indicated they would attend. Facebook initially complied with the request, though it refrained from blocking subsequent event pages.[20] On December 30, when the sentencing was moved up in a bid to preempt the protests, Roskomnadzor issued warnings to four media outlets that reported on the sentencing and carried links to a video of Navalny calling for demonstrations. The agency claimed the sites had posted content that was inciting extremism.[21] Similarly, the former technical director of the social-networking site VKontakte, Nikolay Durov, reported that on December 21 the company had received 53 requests from Roskomnadzor to "block all pages, groups, and events that mention the name 'Navalny.'"[22]

From 2012 to 2013 the Russian government enacted legal amendments that gave several agen-

18 Access to a number of online resources calling for unauthorized mass events was blocked. Roskomnadzor, "Ограничен доступ к ряду интернет-ресурсов, распространявших призывы к несанкционированным массовым мероприятиям," news release, March 13, 2014, http://bit.ly/1hfY7Gh.

19 Steven Wilson, "The logic of Russian internet censorship," *Washington Post*, March 16, 2014, http://wapo.st/1W30wwI.

20 Michael Birnbaum, "Facebook blocks Russian page supporting Navalny, Putin's biggest critic," *Washington Post*, December 20, 2014, http://wapo.st/1hP9nPL.

21 Roskomnadzor, "Вынесены предупреждения ряду средств массовой информации" [Roskomnadzor issued warnings to a number of media outlets], news release, December 30, 2014, http://bit.ly/1ZSHkkw.

22 Zhanna Ulyanova, Vitaly Akimov, Darya Luganskaya, Svetlana Reiter, "Block unavailable: How they try to cut 'people's assembly' for Navalny off the social networks" [in Russian], *RBC*, December 22, 2014, http://bit.ly/1EDyn0k.

cies—including Roskomnadzor, the Prosecutor General's Office, the Federal Service for Surveillance on Consumer Rights and Human Wellbeing (Rospotrebnadzor), and the Federal Drug Control Service—the authority to make decisions about blocking various categories of information. Currently, these agencies have the authority to block, without a court order, the following types of content: information about suicide, drug propaganda, child pornography, information about juvenile victims of crimes, materials that violate copyright, content related to extremism, and calls for unsanctioned public actions or rallies. Any other information may be blocked by a court decision, provided that the court finds the content illegal.

According to the nonprofit project RosComSvoboda, which conducts ongoing monitoring of blocked content, the following were blocked by the end of May 2015:

- 773 sites for extremism and calls for protests (by orders from the Prosecutor General's Office)
- 3,981 sites containing drug-related content (by orders from the Federal Drug Control Service)
- 82 sites containing suicide propaganda (by the decision of Rospotrebnadzor)
- 2,613 sites for the distribution of child pornography (by the decision of Roskomnadzor)
- 2,701 sites, based on other court decisions, for the publication of various banned information

In most cases the legal framework offers no clear criteria for evaluating the legality of content, and public authorities do not always offer a detailed explanation for blocking decisions. The lack of precise guidelines sometimes leads telecom operators, which are responsible for complying with blocking orders, to carry out the widest blocking possible so as to avoid fines and threats to their licenses. Telecom operators are obliged to regularly consult the "blacklist" of banned websites, updated by Roskomnadzor. Moreover, the law does not specify how ISPs should restrict access; for example, based on the internet protocol (IP) address, the domain name, or the URL of the targeted page. Often the authorities do not consider it necessary to clearly indicate the specific pages that are meant to be blocked on a given site. As a result, entire sites, against which the authorities do not have any formal complaints, are often blocked. According to RosComSvoboda statistics, there are currently 262,991 websites that have been accidentally blocked due to blocking orders carried out on the basis of IP addresses.

Content Removal

The existing process for blocking online content, which only gives website owners a few hours or a few days to comply with the request, often leads them to delete the banned information rather than risk having the entire site blocked.

In cases where websites are registered as mass media, Roskomnadzor has additional powers to issue warnings to the editorial board about "abuse of freedom of mass media." Article 4 of the law "On Mass Media" implies that such abuse can include, for example, 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 down the media outlet. Usually, the warnings from Roskomnadzor contain instructions to remove or edit the offending material. For example, in August 2014, at least 14 media outlets received warnings for publishing reports on a protest movement calling for greater regional autonomy, or "federalization," particularly in Siberia. For instance, the magazine *New Times* was forced to remove from its website a large overview of the federalization phenomenon by journalist Aleksandr Litoy.

On December 30, 2014, Roskomnadzor issued warnings against four media outlets—Polit.ru, *Business Online,* BFM.ru, and *Mediazona*—for publishing materials containing "calls to change the constitutional order." The content was actually a video of Aleksey Navalny's speech after the verdict in the fraud case.[23] In January 2015, at least six media outlets received warnings for publishing materials on that month's terrorist attack against the French satirical magazine *Charlie Hebdo*, with Roskomnadzor issuing a formal statement that any cartoons on religious themes would be treated as extremism.[24] Most of the media outlets that received these warnings chose to remove the materials.

According to Twitter's Transparency Report covering July to December 2014, the company received 91 requests to remove information from Russian authorities, of which 13 percent were satisfied—two accounts and nine tweets were withheld.[25] After the publication of the report, the head of Roskomnadzor publicly expressed dissatisfaction with the fact that Twitter was not fully cooperating and had refused to disclose user data or delete information at the request of Russian authorities.[26] In the second half of 2014, Facebook limited access to 55 pieces of content "under local laws prohibiting content that promotes drug use and self-harm, extremist activities, unsanctioned mass riots/marches, and for violating the integrity of the Russian Federation."[27]

Media, Diversity, and Content Manipulation

The online media environment is becoming more restricted as the government attempts to counteract information that might undermine its authority. While Russians are still able to access a wide variety of outside sources, many independent online media outlets within Russia have been forced to shut down over the past two years due to increasing pressure from the government, and progovernment trolling continues to be a problem. Self-censorship is encouraged by the vague wording of restrictive legislation, the seemingly arbitrary manner in which these laws are enforced, and the near-total ineffectiveness of judicial remedies. Laws prohibiting "extremist content" and the government's crackdown on several media outlets have resulted in a chilling effect on free speech, particularly with regard to such sensitive topics as governance failures by the authorities, corruption, war with Ukraine, the annexation of Crimea, violation of civil rights, religion, and the LGBTI (lesbian, gay, bisexual, transgender, and intersex) community.

Several online media outlets that were originally blocked in March 2014 remain restricted. A number of other media outlets have received warnings from Roskomnadzor for their coverage of protests, the attack on *Charlie Hebdo,* or the criminal cases of Aleksey Navalny, meaning they run the risk of receiving a second warning and losing their licenses. While individuals are still able to use circum-

23 Roskomnadzor, "Roskomnadzor issued warnings to a number of media outlets" [in Russian].

24 Roscomnadzor, "Explanation about the cartoons on religious issues" [in Russian], news release, January 16, 2015, http://bit.ly/1ZSIJaO.

25 Twitter, "Removal requests: Worldwide," *Transparency Report,* July–December 2014, http://bit.ly/1wZlsZK.

26 "Roscomnadzor unsatisfied with the way Twitter withheld negative comments: only 55 tweets" [in Russian], *Newsru,* March 25, 2015, http://bit.ly/1M3Thjt.

27 Facebook, "Russia," *Transparency Report*, July–December 2014, http://bit.ly/1klKnkS.

vention tools to access blocked content, officials at various levels have repeatedly spoken about the need to block access to such tools, though legislation to that effect has not yet been adopted. Despite the continued availability of circumvention tools, all blocked resources have reported a significant reduction in traffic.

In the spring of 2015, hackers published leaks of correspondence from the deputy head of the Office of Internal Policy of the Presidential Administration, which indicated that the administration is actively involved in a number of media outlets' editorial policies and uses Roskomnadzor and the Prosecutor General's Office to exert pressure on those who resist such directives.[28]

Russian authorities continue to use the assistance of paid commentators to influence online content. A 2013 investigation conducted by journalists at *Novaya Gazeta* showed that some members from the pro-Kremlin youth movements Nashi and Molodaya Gvardiya organized paid campaigns on social-networking sites.[29] In January 2014, the editors of the German newspaper *Die Zeit* reported a wavelike increase in the number of anti-Western user comments, believed to be propaganda, on the paper's website at the time of the Euromaidan protests in Ukraine.[30] Other media outlets, including *Forbes* and the *Guardian*, reported a similar flood of "insulting, combative" comments on any articles related to Russia or Ukraine. In March 2015, journalists at *Novaya Gazeta* and the St. Petersburg outlet *Moy Rayon* published an investigation into the activity of pro-Kremlin paid commentators, revealing more than 500 accounts on the LiveJournal blogging platform that specialized in the publication of progovernment views and harassment of opposition activists.

Several new laws enacted during the coverage period also had the potential to restrict the information available online. In October 2014 Putin signed amendments to the law "On Mass Media" that prohibit foreign citizens and organizations from owning more than 20 percent stakes in Russian media; the changes are scheduled to take effect in January 2016, though outlets have until 2017 to reduce their existing foreign ownership. In May 2015, a new law on "undesirable organizations" included bans on disseminating information from the blacklisted organizations.

Data-localization laws can also have an impact on companies' ability to operate within a given jurisdiction, and in July 2014 the Russian government enacted a law requiring technology companies processing Russians' data to host the information on local servers. As international companies decided how and whether to comply with the law ahead of the September 1, 2015, deadline, some chose to reduce their presence in the country. In September 2014 the Russian branch of Adobe applied for liquidation.[31] In November, Microsoft announced that it was closing its engineering office in Zelenograd and moving part of its staff to Prague.[32] One month later, Google announced that it would also be closing its engineering offices in Russia.[33]

Digital Activism

Despite the continued government pressure, the internet in Russia remains the most versatile and

28 "The modern history of the Russian policy told in SMS" [in Russian], *Insider*, April 1, 2015, http://bit.ly/1IRolhh.

29 Aleksandra Garmazhapova, "Where the trolls live. How internet-provocateurs work in Saint Petersburg and who rules them" [in Russian], *Novaya Gazeta*, September 9, 2013, http://bit.ly/1RTq1dZ.

30 Annika von Taube, "Russische Botschaft" [in German], *Zeit Online*, January 27, 2014, http://bit.ly/1GQlUJ7.

31 Darya Trosnikova, "Adobe liquidates its office in Russia" [in Russian], *Vedomosti*, September 26, 2014, http://bit.ly/1jy8pJk.

32 Pavel Kantyshev, "Zelenograd without Skype" [in Russian], *Vedomosti*, November 10, 2014, http://bit.ly/1XgGps9.

33 Andrew Griffin, "Google engineers to leave Russia," *Independent*, December 12, 2014, http://ind.pn/1XgGtbh.

effective tool for activism. In 2014, social-networking sites were used successfully to organize public events. Some experts believe that the large groups that mobilized to demonstrate support for the Navalny brothers drove the courts to move up their sentencing date from January 15 to December 30—to preempt planned protests—and influenced the eventual outcome, in which Aleksey Navalny was sentenced to probation instead of imprisonment. Information about the protests spread on Facebook, Twitter, Vkontakte, Odnoklassniki, Google+, and other platforms, and demonstrations were organized in Moscow, Yekaterinburg, Perm, Novosibirsk, Berlin, New York, and London.

In addition to organizing protests via social media, Russians have continued to use crowdfunding as a tool for activism and mobilization. The crowdfunding platforms Planeta.ru and Boomstarter.ru have collected approximately US$7 million over two years to fund various community projects.

Violations of User Rights

The Russian government continues to enact laws that restrict online activity and increase the penalties for violations. In June 2014, the government passed amendments to the criminal code that set penalties of up to five years in prison for posting extremist content online. The amendments also made it illegal to finance an organization deemed extremist, with punishments including fines and prison terms. In addition, the authorities continue to expand their capacity for surveillance of ICTs, including through an update in April 2015 to the SORM surveillance system that incorporates DPI technology, allowing intelligence agents to access and search the content of online communications.

Legal Environment

Although the constitution grants the right to free speech, this right is routinely violated, and there are no special laws protecting online modes of expression. Online journalists do not possess the same rights as traditional journalists unless they register their websites as mass media. Russia remains a member of the Council of Europe and a party to the European Convention on Human Rights and Fundamental Freedoms, Article 10 of which enshrines the right to freedom of expression. However, over the past few years Russia has adopted a set of laws and other acts that, coupled with repressive law enforcement and judicial systems, have eroded freedom of expression in practice. Courts tend to side with the executive authorities, refusing to apply provisions of the constitution and international treaties that protect the basic rights of journalists and internet users.

Over the past year, the government passed amendments to significantly increase the penalties for online incitement to separatism or calls for extremism, with prison terms up to five years, and incitement to hatred, with prison terms up to six years. In addition to the criminal penalties, the mere opening of a criminal case could serve as a basis for the inclusion of the accused on a list of extremists maintained by the Federal Financial Monitoring Service. Individuals on this list, even if they have not been convicted, are restricted from certain professions, and their bank accounts can be frozen.

The law establishes criminal penalties for defamation (Article 128.1 of the criminal code), defamation against a judge or prosecutor (Article 298.1), insulting the authorities (Article 319), calls for terrorism or justification of terrorism (Article 205.1), insulting religious feelings (Article 148), calls for extremism (Article 280), calls for separatism (Article 280.1), incitement of hatred (Article 282), spreading false information on the activities of the Soviet Union in World War II, or insulting "symbols of Russian military glory" (Article 354.1). In addition, administrative prosecutions can be brought against

individuals for displaying Nazi symbols or symbols of organizations deemed extremist (Article 20.3 of the administrative code), the dissemination of extremist materials (Article 20.29), or insult (Article 5.61).

Prosecutions and Detentions for Online Activities

According to the SOVA analytical center, dozens of activists, journalists, and online editors continue to be subjected to administrative and criminal prosecution for content they post online.[34] The majority of cases result in penalties such as fines and suspended sentences. However, the possibility of criminal prosecution even for reposting an item deemed to contain extremist content has had a significant chilling effect, with users apparently more inhibited in discussing political and social issues online.

There were several arrests and sentences over the past year for online activities falling under Article 280 (calls for extremism) and Article 282 (incitement of hatred):

- In December 2014, the chairman of the Tatar Public Center, Rafis Kashapov, was arrested in Kazan on charges of inciting hatred. The arrest was prompted by Kashapov's posts on Vkontakte, which supported Ukraine and the Crimean Tatars while condemning the illegal annexation of Crimea and the actions of Russian authorities.[35] In September 2015, Kashapov was sentenced to three years in prison.[36]

- Krasnodar activist Darya Polyudova was arrested in August 2014 and spent six months in pretrial detention for using Vkontakte to call for a march demanding the federalization of Kuban, which was never held. According to Radio Free Europe/Radio Liberty, Polyudova was charged with promoting separatism and faces up to five years in prison.[37]

- In May 2015, LGBTI activist and environmentalist Konstantin Golava was arrested on charges of incitement and extremism. The arrest stemmed from antigovernment posts on VKontankte that were deemed extremist. He was released pending trial.[38]

- Sergey Reznik, a freelance blogger imprisoned since November 2013, was charged for a second time in July 2014 for allegedly insulting authorities online. The prosecution did not specify which blog posts on his LiveJournal account were being investigated. In January 2015, Reznik was sentenced to an additional three years in prison.[39]

There were a number of other cases related to the dissemination of banned symbols or extremist materials online. More than a dozen users from various regions of Russia were prosecuted in 2014 under Article 20 of the administrative code for circulating a video, originally published in 2011, that

34 Analytical center SOVA, "Illegal anti-extremism" [in Russian], http://bit.ly/1LHEKaX.

35 "Taken to Kazan" [in Russian], *Grani*, December 29, 2014, http://bit.ly/1Ce07Jc.

36 "Tatar Activist Kashapov Gets 3-Year Prison Sentence for Crimea Posts," *Moscow Times*, September 16, 2015, http://bit.ly/1klKSf1.

37 Natalya Dzhanpoladova, "Darya Polyudova: Free pending trial" [in Russian], Radio Svoboda, March 5, 2015, http://bit.ly/1PDNVuH.

38 Front Line Defenders, "Russia—Human rights defender Konstantin Golava facing charges," May 18, 2015, http://bit.ly/1PwMDmd.

39 Committee to Protect Journalists, "Imprisoned Russian journalist sentenced to new three-year jail term," January 22, 2015, http://bit.ly/1W3ltHV.

criticized the ruling United Russia party.[40] The video was deemed extremist in 2013, and the prosecutor's office indicted individuals who "liked" or reposted the video in 2014, with some cases resulting in fines.

Several individuals have also been questioned or fined for posting material that references Nazi symbols. In March 2015, a court in Ulan-Ude fined Mariya Burdukovskaya RUB 1,000 (US$20) for posting an image on VKontakte of a Nazi-style eagle over the phrase "grammar will make you free"—a reference to a joke about "grammar Nazis."[41] Also in March 2015, Readovka.ru correspondent Polina Petruseva was fined RUB 1,000 (US$20) for circulating a photograph on VKontakte of the German occupation of Smolensk during World War II. The photo depicted the house where the journalist is now living with a Nazi flag and swastika.[42]

Surveillance, Privacy, and Anonymity

Over the past year, the Russian authorities have actively tried to limit internet users' ability to remain anonymous online, while simultaneously expanding the government's capacity for surveillance. The July 2014 data localization law, which requires all foreign internet companies to host Russians' data on servers within the country, could facilitate the Russian government's access to user data.[43] In May 2014, Putin had signed a law that considered any website with over 3,000 daily viewers, including blogs and social media accounts, to be "mass media," requiring them to register with the government; among other effects, this decreased the space for users to communicate anonymously online.[44] The measure also contained wording that would require any services hosting such outlets to maintain records of their data on servers located within Russia. As of May 2015, more than 700 popular bloggers were included on the list.

In July 2014, the Ministry of Communications issued an order regarding the new requirements for ISPs to update their equipment for the implementation of SORM, the system used by the security services to carry out surveillance.[45] As of March 31, 2015, ISPs in Russia were required to upgrade to SORM-3, which uses DPI technology, enhancing the ability of the security services to monitor content on all telecommunications networks in Russia.

SORM, or "system for operational investigative measures," has been gradually improved since it was first launched in the late 1990s. Indeed, there is evidence that the Russian government has significantly increased its overall surveillance capabilities over the past few years. Procurement documents revealed the extent to which the government had expanded its domestic surveillance infrastructure, including upgrades to telephone and Wi-Fi networks, ahead of the February 2014 Winter Olympic Games in Sochi.[46] Such technology has been used for political purposes in the past, including the

40 Analytical center SOVA, "Tatarstan continues fight against Navalny's video" [in Russian], December 9, 2014, http://bit.ly/1JTZcFK.

41 Nikita Likhachev, "'Grammar-Nazi' from Buryatiya got a penalty for a picture with the 'Nazi eagle' on VKontake" [in Russian], *TJournal*, March 17, 2015, http://bit.ly/1PDOdlw.

42 Analytical center SOVA, "Smolensk journalist prosecuted for publishing photo of her yard from WW2" [in Russian], March 2, 2015, http://bit.ly/1jRtuy0.

43 Paul Sonne and Olga Razumovskaya, "Russia Steps Up New Law to Control Foreign Internet Companies," *Wall Street Journal*, September 24, 2014, http://on.wsj.com/1wylGQd.

44 Neil MacFarquhar, "Russia Quietly Tightens Reins on Web With 'Bloggers Law,'" *New York Times*, May 6, 2014, http://nyti.ms/1slgNL3.

45 Rublacklist, "SORM-3 shall be implemented by March 31, 2015" [in Russian], October 11, 2014, http://rublacklist.net/8827/.

46 Shaun Walker, "Russia to monitor 'all communications' at Winter Olympics in Sochi," *Guardian*, October 6, 2013, http://bit.ly/196oL5B.

targeting of opposition leaders. In a Supreme Court case in November 2012 involving Maksim Petlin, an opposition leader in the city of Yekaterinburg, the court upheld the government's right to eavesdrop on Petlin's phone conversations because he had taken part in "extremist activities," namely antigovernment protests. Online surveillance represents somewhat less of a threat in the major cities of Moscow and St. Petersburg than in the regions, where almost every significant blog or forum is monitored by the local police and prosecutor's office. Most of the harassment suffered by critical bloggers and other online activists in Russia occurs in the regions.

Under current legislation, in order to receive an operating license, ISPs are required to install equipment that allows security services to monitor internet traffic. ISPs that do not comply with SORM system requirements are promptly fined, and may have their licenses revoked if problems persist. Russian authorities are technically required to obtain a court order before accessing an individual's electronic communications data; however, the authorities are not required to show the warrant to ISPs or telecom providers, and FSB officers have direct access to operators' servers through local control centers. Experts note that there is no information about any government efforts to punish security officers who abuse tracking methods.[47] ISPs and mobile providers are required to grant network access to law enforcement agencies conducting search operations, and to turn over other information requested by the prosecutor's office, the Interior Ministry, the FSB, or the Investigative Committee.

There are currently no explicit restrictions on the use of circumvention tools or anonymizers, though such tools may be banned in the near future. Russian officials have periodically proposed the idea of prohibiting the use of anonymizers and proxy servers, and in August 2013 it was reported that the FSB was developing a package of laws to block access to Tor and foreign proxy servers for Russian users.[48] In April 2015, a court issued a decision to block the website of RosKomSvoboda, which provided instructions on how to use circumvention tools. The ruling stated that the website "is an anonymizer," which is incorrect, and anonymizing tools are not currently banned in any case.[49]

Presently, identification is needed to sign a contract for internet access or mobile service. In addition, owners of public Wi-Fi facilities are required to use content filters to protect children from potentially "harmful" information. This requirement may force owners to implement age checks for users. As of April 2015, according to the Department of Information Technology in Moscow, identification was required for use of all public Wi-Fi networks in the city.[50]

Intimidation and Violence

Impunity flourishes in Russia, and perpetrators of attacks on online activists and bloggers continue to avoid prosecution.[51] The failure of the authorities to protect activists and uphold international human rights standards have set dangerous precedents that foster a climate of intimidation.[52] Investigations into past attacks, such as the 2011 murder of *Chernovik* founder Gadzhimurad Kamalov and

47 Aleksey Alikin, "SORM in public" [in Russian], *Russkaya Planeta*, July 29, 2013, http://rusplt.ru/policy/policy_3890.html.

48 "FSB conducts the law against anonymity on the net" [in Russian], *Izvestia*, August 16, 2013, http://izvestia.ru/news/555552.

49 Tetyana Lokot, "Did Russia Just Effectively Outlaw Internet Anonymizers?" Global Voices Advocacy, May 28, 2015, http://bit.ly/1XhpplM.

50 Rublacklist, "There will be no anonymous access to public Wi-Fi in Moscow" [in Russian], March 2, 2015, http://bit.ly/1GnG-1DK.

51 Index on Censorship, "Russia: End the cycle of impunity," November 2, 2014, http://bit.ly/1J7VOXL.

52 "A New Power Struggle in Dagestan?" Radio Free Europe/Radio Liberty, December 19, 2011, http://bit.ly/1Srp0ui.

the 2013 murder of *Caucasian Knot* journalist Akhmednabi Akhmednabiyev, have been suspended or remain ineffective.[53]

In August 2014, Timur Kuashev, a blogger for *Kavkazkaya Politika* (Caucasian Politics), *Caucasian Knot*, and *Dosh*, was found dead on the outskirts of Nalchik.[54] Kuashev's writings criticized the actions of local government and law enforcement officials.[55] In January 2015, Sergey Vilkov, a journalist for the independent news website *Obshchestvennoye Mneniye* (Public Opinion), was assaulted in Saratov. The attack was apparently motivated by Vilkov's investigative reports on government corruption and organized crime in the region.[56] Vyacheslav Starodubets, a Dagestan-based blogger and founder of *My Derbent*, a website reporting on local corruption, was kidnapped, badly beaten, and hospitalized in April 2015.[57]

The threat of harassment, violence, or criminal prosecution has forced some activists and bloggers to flee the country. In November 2014, Altai activist Andrey Teslenko, accused of provoking hatred online, was granted asylum in Ukraine.[58] Teslenko had reposted an article on VKontakte that criticized Russia's call for Ukraine to crack down on protesters during the Euromaidan protests. In an earlier case, Maksim Yefimov, a human rights defender and journalist, was granted asylum in Estonia in 2012. He is currently being investigated under Article 282.1 of the criminal code over an editorial he published that condemned corruption within Russia's Orthodox Church.[59]

In August 2014, eight journalists were violently attacked or otherwise obstructed in Pskov, apparently in connection with their investigations into the burials of paratroopers who were allegedly killed in eastern Ukraine, despite the Russian government's denial that any troops were deployed there. In one incident, four journalists—Vladimir Romensky of TV Dozhd, Ilya Vasyunin of *Russkaya Planeta*, Nina Petlyanova of *Novaya Gazeta*, and Irina Tumakova of the website Fontanka.ru—were attacked by unidentified assailants.[60] The group was visiting the site of the secret burials when the attackers attempted to break their car's windows and slit its tires.[61] The assault was documented on video, and an investigation was launched following pressure from the Russian Council for Civil Society and Human Rights.

Technical Attacks

Cyberattacks against independent media, blogs, and news portals continue to inhibit Russian internet users' ability to access such sites. In September 2014, Google notified several of its Russian users

53 "At UN HRC session, 'Article-19' demands that Russian authorities reopen inquiry into Akhmednabiyev's killing" [in Russian], *Caucasian Knot,* September 2014, http://eng.kavkaz-uzel.ru/articles/29361/

54 "Timur Kuashev found dead in Kabardino-Balkaria" [in Russian], *Caucasian Knot*, August 1, 2014, http://bit.ly/1GfZWoe.

55 Orhan Dzemal, "The investigation of Timur Kuashev's murder" [in Russian], *Orhan Dzemal Blog*, *Caucasian Politics*, December 23, 2014, http://bit.ly/1M4TNgU.

56 Committee to Protect Journalists, "Russian journalist beaten in Saratov, second from same site in five months," January 14, 2015, http://bit.ly/1HYK1to.

57 "Journalist in Daghestan Beaten, Hospitalized," Radio Free Europe/Radio Liberty, April 6, 2015, http://bit.ly/1ChklBU.

58 Kseniya Gogitidze, "Ukraine grants asylum to Russian activist" [in Russian], BBC, November 17, 2014, http://bbc.in/1J4lnJi.

59 Front Line Defenders, "Russian Federation: Update – Supreme Court of Kareliya due to hear human rights defender Mr. Maxim Efimov's appeal," August 20, 2013, http://bit.ly/1Gg0kmQ.

60 "Human Rights Council asks Bastrykin to investigate attack on journalists at graveyard near Pskov" [in Russian], *Novaya Gazeta,* August 26, 2014, http://bit.ly/1Gg0r1D.

61 Elena Milashina, "Journalists investigating deaths of Russian soldiers are threatened and attacked," Committee to Protect Journalists (blog), September 22, 2014, http://bit.ly/1GmSgtK.

that anonymous hackers from an unnamed state were trying to access their accounts.[62] The news portal Kasparov.ru, which had already been blocked for internet users within Russia in March 2014, reported two massive distributed denial-of-service (DDoS) attacks against its website in May 2015.[63]

In previous years, websites that suffered DDoS attacks included the internet project Demokrator.ru, Saint Petersburg news portals Zaks.ru and Lenizdat.ru, the website of the SOVA Center for Information and Analysis, the website of the daily newspaper *Moskovsky Komsomolets*, the Murmansk-based portal Bloger51.ru, and the websites of *Novaya Gazeta* and TV Dozhd.

62 Irina Yuzbekova and Roman Dorokhov, "Google notified its Russian users about an attack" [in Russian], *RBC*, September 9, 2014, http://bit.ly/1LAZa1X.

63 "Kasparov.ru under second DDoS attack" [in Russian], *Grani*, May 28, 2015, http://bit.ly/1OPYQku.