

# Russia

	2013	2014		
<b>Internet Freedom Status</b>	<b>Partly Free</b>	<b>Partly Free</b>	Population:	143.5 million
Obstacles to Access (0-25)	10	10	Internet Penetration 2013:	61 percent
Limits on Content (0-35)	19	22	Social Media/ICT Apps Blocked:	No
Violations of User Rights (0-40)	25	28	Political/Social Content Blocked:	Yes
<b>TOTAL* (0-100)</b>	<b>54</b>	<b>60</b>	Bloggers/ICT Users Arrested:	Yes
			Press Freedom 2014 Status:	Not Free

\* 0=most free, 100=least free

## Key Developments: May 2013 – May 2014

- On December 30, 2013, President Vladimir Putin signed a bill granting the Prosecutor General the authority to place websites on the federal blacklist if the sites contained extremist content or calls for participation in unsanctioned public actions. The law was subsequently used to block access to independent media or opposition websites reporting on the unfolding conflict in Ukraine (see **Limits on Content**).
- Evidence of increased government surveillance of ICTs emerged in the run-up to the 2014 Sochi Winter Olympic Games (see **Violations of User Rights**).
- In May 2014, the government passed a law requiring certain online bloggers or social media users to register with the telecommunications regulator, which effectively limited citizens' ability to anonymously publish ideas and information online (see **Violations of User Rights**).
- Online journalists and bloggers continued to face legal harassment and threats of physical violence. In July 2013, a correspondent for the online media outlet *Caucasian Knot* who had been reporting in Dagestan was murdered, after facing repeated threats (see **Violations of User Rights**).

## Introduction

Russia's environment for internet freedom declined significantly as the government took multiple steps to increase control over the online sphere, particularly in advance of the Sochi Olympic Games in February 2014 and throughout the ongoing crises in Crimea and eastern Ukraine.

At the end of 2013, Putin signed a law allowing for the Prosecutor General's office to direct the telecommunications authority to block websites that contain extremist content or calls for participation in unsanctioned public actions. The law was subsequently used to block access to independent media sites reporting on the unfolding conflict in Ukraine. Additionally, the State Duma passed amendments to the copyright legislation of the Russian Civil Code that allow for new measures to block websites that are suspected of hosting copyright-infringing material before court proceedings take place. In May 2014, the State Duma also passed a law requiring bloggers or social media users with more than 3,000 daily views to register with the government or face the possibility of having their account blocked.

Independent media outlets that were critical of the Kremlin faced increasing obstacles including economic constraints and pressure on their executive staff. Lenta.ru, one of the oldest and most widely read Russian online media sites, received a warning from Roskomnadzor on March 11 for their coverage of the crisis in Ukraine; the next day, the editor-in-chief was fired. In February, the independent TV channel Dozhd came under attack under false pretexts, leading to the majority of networks and internet TV channels to cancel their broadcasts of the station's programming. Having lost the majority of its advertising revenue, the channel was on the brink of collapse and continues to operate almost entirely on crowd-funded donations.

Internet users in Russia faced increasing prosecutions, physical violence, and evidence of growing surveillance over the past year. According to a report published in February 2014 by eLiberator.ru, a project supported by the AGORA Association, there were 24 episodes of violence against bloggers and online journalists in 2013, including the murder of a correspondent for the online news outlet *Caucasian Knot* in July. In November 2013 a well-known blogger who had reported on local corruption was charged with bribery, insulting an official, and misleading the authorities, and was sentenced to 18 months in a labor camp. Surveillance of online communications without sufficient judicial oversight continues (court orders are technically required but ISPs cannot request to see the court order), and evidence of increased surveillance emerged over the past year.

## Obstacles to Access

The internet penetration rate in Russia continued to grow over the past year, though not as rapidly as in previous years. According to the International Telecommunication Union (ITU), the internet penetration rate reached 61 percent by the end of 2013, compared to 53 percent in 2012 and just 27 percent in 2008.<sup>1</sup> According to the Public Opinion Foundation, the number of people 18 years or older who access the internet on a monthly basis reached 66.5 million, or 57 percent of the

---

1 International Telecommunication Union, "Percentage of Individuals Using the Internet," 2013, 2012, 2008, accessed August 2014, <http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>.

population, by the end of 2013, while the daily audience of internet users is estimated at about 53.2 million, or 46 percent.<sup>2</sup>

Additionally, internet access has become less expensive and speeds have increased over the past year. According to a Yandex report, the speed of broadband internet access has significantly increased, while costs have reduced fourfold. A connection speed of 1 Mbps costs an average of US\$0.72 per month, while the residents of Moscow, for instance, pay US\$14 per month for access speeds averaging 51 Mbps.<sup>3</sup>

The mobile phone penetration rate reached 168 percent, or approximately 240 million subscribers, by the third quarter of 2013.<sup>4</sup> According to another report by the research company TNS Russia, approximately 50 percent of internet users access the internet via mobile devices.<sup>5</sup>

The past year witnessed the massive implementation of LTE standard in Russia and access to 4G networks was available in nearly all regional centers. Mobile operators have started to offer economy tariffs for mobile service, allowing users access to the 4G/LTE network for approximately US\$5.50 per month.<sup>6</sup>

In March 2014, new amendments to the law on communications came into effect that established general requirements for providing universal communication services to citizens. According to the amended law, at least one point of collective access to telephone communication services must be installed in every settlement in the country in order to provide free access to emergency services. Settlements with a population of over 250 people must be equipped with at least one access point to the internet, which should provide the ability to transfer data at speeds of more than 10 Mbps.<sup>7</sup> However, according to an official government report, approximately 8 percent of settlements with a population of less than 10,000 (1,343 townships) still have no access to cellular networks or the internet.<sup>8</sup>

The market for broadband internet access remains highly concentrated in the hands of a few companies. According to the most current data available, the six largest providers occupy 77.1 percent of the market: the state-owned provider Rostelecom controls 38.6 percent of the market, while the rest is divided among ER-Telecom, VimpleCom, MTS, Trantelecom and AKADO.<sup>9</sup> The mobile communications market is even less diverse, with the four biggest operators—MTS, Megafon, VimpleCom and Tele2—together controlling 92 percent of the market.

---

2 Public Opinion Foundation, "Интернет в России: динамика проникновения. Осень 2013" [Internet in Russia: Dynamics of Penetration. Fall 2013], January 15, 2014, <http://fom.ru/SMI-i-internet/11288> [In Russian]

3 Internet in Russian regions, [http://company.yandex.ru/researches/reports/2013/ya\\_internet\\_regions\\_2013.xml](http://company.yandex.ru/researches/reports/2013/ya_internet_regions_2013.xml) [In Russian]

4 Advanced Communication & Media, "Cellular Data," accessed 12 March 2014, <http://www.acm-consulting.com/>.

5 TNS Russia. Mobile Internet Research Results. November 21, 2013, <http://en.tns-global.ru/press/news/207039/>

6 Ilya Shatilin. New perspectives of mobile Internet. TelecomDaily, January 9, 2014, <http://www.tdaily.ru/news/top-novo-sti/31770> [In Russian]

7 ICT Ministry official website. Amendments to the Federal Law "On Communications" will provide broadband to all villages of more than 250 residents. February 6, 2014, [http://minsvyaz.ru/ru/news/index.php?id\\_4=44301](http://minsvyaz.ru/ru/news/index.php?id_4=44301).

8 ICT Ministry official website. Results of the survey of communication services in small cities of Russia. January 9, 2014, [http://minsvyaz.ru/ru/news/index.php?id\\_4=44260](http://minsvyaz.ru/ru/news/index.php?id_4=44260).

9 Advanced Communication & Media, "Cellular Data", accessed March 12, 2014

On July 17, 2013 the Ministry of Communications published a concept paper titled, "Theses for the concept of development of multi-service networks for public communication in the Russian Federation,"<sup>10</sup> which would centralize the management of trans-boundary internet traffic. The proposal would grant the right to transmit foreign internet traffic to only a few federal service providers, effectively forcing all other ISPs to buy the traffic from them. The requirements of the federal service provider are so strict that currently only a single state-owned company, Rostelecom, would be able to meet them. If the proposal is approved, it is likely that Rostelecom will control an even greater share of the market.

The ICT and media sector is regulated by the Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications (Roskomnadzor) under the control of the Ministry of Communications and Mass Media and the Government of the Russian Federation. The head of Roskomnadzor, Alexander Zharov, was appointed directly by executive decree on May 3, 2012. The regulatory body has the authority to determine if a website should be blocked based on whether or not the site contains material that is restricted by the law; these decisions do not require prior court approval. Additionally, 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 (see Limits on Content). As a result, Roskomnadzor has become a primary player in the field of controlling and filtering information on the internet.

## Limits on Content

From 2013-2014, the Russian authorities significantly expanded restrictions on online content through the introduction of additional legal grounds for blocking access to websites. On December 30, 2013, Putin signed a bill granting greater authority to the Prosecutor General to block websites without a court order if the websites allegedly contained extremist material or calls for participation in unsanctioned public actions. Up until the end of 2013, the practice of blocking online content in Russia was relatively untargeted—many individual websites or webpages were blocked for containing "harmful" or "extremist" content, but independent news outlets were still largely able to operate online. Indeed, the internet was regarded as a space for freedom of expression and freedom of information that was distinctly separate from—and largely immune to—the firm state control over the print and broadcast media. After this law came into effect on February 1, 2014, however, it was quickly used to crack down on online media outlets with content critical of the Kremlin's policies, particularly regarding the conflict in eastern Ukraine and Crimea.

On March 13, 2014, just three days before 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 the Bolotnaya protestors in 2012; *Ezhednevny Zhurnal* (Ej.ru), a news and opinion site; and Kasparov.ru, the website of former chess champion turned opposition figure, Gary Kasparov.<sup>11</sup> The owners of the websites were not provided with an explanation as to what content had violated the law and caused the Prosecutor General to issue the blocking order. At the same time, the authorities blocked access

---

10 ICT Ministry official website. <http://minsvyaz.ru/ru/discussions/index.php?id=41> [In Russian]

11 Access to a number of online resources calls for unauthorized mass events was blocked. Roskomnadzor official website, March 13, 2014, <http://rkn.gov.ru/news/rsoc/news24447.htm> [In Russian]

to the personal blog of the opposition leader Alexei Navalny and the website of the radio station Echo of Moscow (Ekho Moskv), though these two were subsequently unblocked within a few days.<sup>12</sup>

In the first half of 2014, Roskomnadzor reported blocking 85 websites for containing “extremist content,” based on orders from the Prosecutor Generals’ office.<sup>13</sup> In addition to the new amendments passed in December 2013, websites can still be blocked in accordance with Federal Law 139-FZ if they are placed on the Unified Register of banned sites, operated by Roskomnadzor, for containing illegal or otherwise harmful material such as child pornography, material related to drug abuse, and so forth. According to the official report of Roskomnadzor published on December 13, 2013, the Unified Register contains 3,361 records, including 894 IP addresses. Experts at the RosComSvoboda project claim that this has led to the blocking of more than 50,000 sites in Russia.<sup>14</sup>

On July 17, 2013, the State Duma passed amendments to the copyright legislation of the Russian Civil Code, allowing for new measures to block websites that are suspected of hosting copyright-infringing material. The law allows for the court to grant preliminary injunctions in cases of alleged copyright infringement online, in which case the person responsible for the website where the content is hosted has 24 hours to remove the content after notification, otherwise the website host company will be instructed to restrict access to that website. However, once the court issues the preliminary injunction, the website is blocked while the court waits for the applicant to file the official complaint, potentially before the website owner is even notified of the case.

Russian legislation contains a wide range of prohibited information, including images that offend religious feelings, or content related to suicide or illegal drugs. Thus, in most cases there are no clear criteria for evaluating information, and public authorities, when considering the decision to block content, do not always offer clear rationale for such a restriction. The lack of clear legislation for blocking banned content leads telecom operators, in some cases, to carry out the widest blocking possible so as to avoid fines and or having their license revoked. During 2013, Russian courts issued 429 decisions on the administrative liability of telecom operators for failing to block prohibited information.<sup>15</sup> For example, in September 2013, Roskomnadzor sued at least three ISPs for 30,000 rubles (approximately US\$900) for failing to log in to the register of banned websites. Presumably the ISPs could not be following the blocking orders if they had not checked the list of banned websites, and would therefore be in violation of the law, although the proceedings did not specify whether the ISPs were found to have actually provided access to any of the sites on the list.<sup>16</sup>

Online media outlets also suffer as a result of ISPs’ decisions to block access to more than the prohibited content. For instance, Rostelecom, referring to the technical inability to block single pages in mid June 2013, denied access to the entire websites of *Gazeta.ru* and *Komsomolskaya Pravda* in the Ulyanovsk Region, after the Leninsky court ruled that content about bribery of officials that was

---

12 Steven Wilson, “The logic of Russian Internet censorship,” *The Guardian*, March 16, 2014, <http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/03/16/the-logic-of-russian-internet-censorship/>.

13 Roskomnadzor blocks 85 websites with extremist content in 2014 so far,” *Kyiv Post*, April 23, 2014, <http://www.kyivpost.com/content/ukraine/roskomnadzor-blocks-85-websites-with-extremist-content-in-2014-so-far-344760.html>.

14 “The Register Monitoring” [in Russian], <http://reestr.rublacklist.net/>

15 Statement by Alexander Zharov, Roskomnadzor website, December 24, 2013, <http://rkn.gov.ru/news/rsoc/news23315.htm> [In Russian]

16 “Russian Internet Service Providers Fined for Ignoring Site Blacklist,” RIA Novosti, September 2, 2013, <http://en.ria.ru/russia/20130902/183126055/Russian-Internet-Providers-Fined-for-Ignoring-Site-Blacklist.html>

previously featured on the websites “undermined the authority of the government.”<sup>17</sup> Access to the sites was restored on June 26 after the prosecutor clarified the blocking order.<sup>18</sup>

Self-censorship among average internet users is not a pervasive trend in Russia, aside from categories of speech that are prohibited by law. However, bloggers and editors of online media outlets have faced increasing government pressure over the past year, which may have had a chilling effect on online freedom of expression more broadly. Additionally, recent government efforts to restrict anonymous communication online may also have an impact on what internet users feel comfortable expressing online (see Violations of User Rights).

Over the past year a number of independent media outlets found themselves under the threat of closure or were forced to change their editorial policy. On March 11, 2014, one of the oldest and most widely read Russian online media sites, Lenta.ru, received a warning from Roskomnadzor in connection with the publication of an interview with one of the leaders of the Ukrainian movement “Pravy Sector” (“The Right Sector”), who took an active part in the confrontation with Berkut forces during the Euromaidan protests in Kyiv. The next day, prominent businessman Alexandr Mamut, who controls part of the media company that owns Lenta.ru, dismissed editor-in-chief Galina Timchenko without explanation and replaced her with a government relations specialist, Alexey Goreslavskay. It is unlikely that the dismissal of the editor could be explained by financial motives, as Lenta.ru, with 20 million unique visitors in February,<sup>19</sup> was bringing in 15 to 20 percent of the total profit for media holding company Afisha-Rambler-SUP.<sup>20</sup> In response to the dismissal, 77 correspondents and members of the editorial staff posted an open letter on the website stating that the dismissal of Timchenko amounted to government censorship and a violation of the law on mass media. Thirty-nine of these staff members additionally resigned in protest.

VKontakte, Russia’s leading online social network, has also reportedly come under increasing pressure from the government over the past year. Beginning in December 2013, Pavel Durov, the founder and CEO of VKontakte, reported that the Federal Security Service (FSB) had sent him requests to hand over the private data related to the accounts of several Euromaidan activists. Durov refused to comply with this request. Previously, the FSB had issued orders for VKontakte to block the pages associated with Alexei Navalny, the anti-corruption and opposition figure. In April, Durov announced that he was resigning due to this ongoing pressure and was leaving the country. In September 2014, the email provider Mail.ru, owned by Kremlin-friendly businessman Alisher Usmanov, officially took control over VKontakte.

Other forms of pressure on internet outlets have also been used in the past year, as Roskomnadzor continued to issue warnings to the media. At least four editorial boards (for the websites Grani.ru, Obeschaniya.ru, Sibkray.ru, and Polit.ru) received warnings from the court in Novosibirsk in June 2013 for publishing one of the banned icons associated with the punk-protest group Pussy Riot. Other websites, including Neva24.ru, KM.ru, the information agency “Novyi Region,” and Regions.

---

17 Gazeta.ru has been blocked in Ul’yanovsk, Gazeta.ru, June 25, 2013, <http://www.gazeta.ru/social/2013/06/24/5391777.shtml> [In Russian]

18 Index on Censorship, “Russia: We know what you blocked this summer,” October 1, 2013, <http://www.indexoncensorship.org/2013/10/russia-censored-summer-2013/>.

19 *Sultan Suleimanov*. Retro: That’s all. TJournal.ru. March 14, 2014 [In Russian]

20 “Thank you, colleagues.” Vedomosti. March 14, 2014, <http://www.vedomosti.ru/opinion/news/23959221/spasibo-kollegi#-sel=11:51,11:51> [In Russian]

ru — also received warnings for publishing links to video of punk-prayer by Pussy Riot. Given that media outlets can be forced to close if they receive two court warnings within a 12 month period, most of the outlets chose to remove the images.

Russian authorities continue to use the assistance of paid commentators to influence online content. An investigation conducted by journalists at *Novaya Gazeta* showed that some members from the pro-Kremlin youth movements “Nashi” and “Molodaya Gvardiya” organized paid campaigns in social networks.<sup>21</sup> In January 2014, the editors of the German newspaper *Die Zeit* reported a wavelike increase in the number of anti-Western comments, believed to be propaganda, on the paper’s website at the time of the Euromaidan protests in Ukraine.<sup>22</sup> Other media outlets, including *Forbes* and the *Guardian*, reported similar flooding of “insulting, combative” comments on any articles posted online related to Russia or Ukraine.

Pressure from the government has also made it more difficult for independent media outlets to maintain their economic viability. The independent media outlet Dozhd TV, which also broadcasts online, does not receive government funding and exists solely on advertising revenue. The editorial policy of the channel is very different from state-controlled television; for example, Dozhd TV was the only Russian TV channel that broadcasted live from Kyiv during the early stages of the Euromaidan protests. Beginning in early 2014, Dozhd TV came under fire from the government after it aired a debate in January asking whether Leningrad should have surrendered during the 900-day-long siege in World War II.<sup>23</sup> Within a month, the majority of the largest satellite broadcasting operators and cable networks, and internet TV providers such as NTV-plus, AKADO, Dom.ru, Rostelecom and TricolorTV, simultaneously refused to broadcast the channel, in what some attributed to a coordinated government crackdown on independent media. Dozhd reportedly lost nearly 90 percent of its audience, leading to a catastrophic reduction in advertising revenue—some companies reportedly left because of the loss in viewership, others because of direct government pressure. Additionally, in March 2014, the company that owns the building where Dozhd operates announced that it was refusing to renew Dozhd’s lease for the following year, forcing the media outlet to relocate. Faced with these developments, Dozhd was on the verge of collapse and has had to ask for financial support from viewers. Currently, Dozhd continues to function due to the success of these crowdfunding efforts.

Despite government pressure against independent media outlets, the online sphere in Russia remains relatively diverse, particularly content on blogs or forums. Social networks like VKontakte, LiveJournal, and Facebook continue to be a significant tool for mobilization and communication between citizens and activists. In 2011, opposition activists in Moscow used Facebook to organize street protests in reaction to the December 2011 State Duma elections, although local platforms like Vkontakte are more popular tools for political mobilization in other regions.<sup>24</sup> Organizers of subsequent protests, such as those related to Putin’s inauguration in May 2012 and the January 2013 “March Against Scoundrels” protesting the bill banning American’s adoption of Russian children, have

---

21 Alexandra Garmazhapova, “Where the trolls live. How internet-provocateurs work in Saint-Petersburg and who rules them,” *NovayaGazeta.ru*, September 9, 2013, <http://www.novayagazeta.ru/society/59903.html> [In Russian]

22 Annika von Taube, “Russische Botschaft,” *Zeit Online*, January 27, 2014, <http://www.zeit.de/index> [In Russian]

23 Tikhon Dzyadko, “Triumph of the will: Putin’s war against Russia’s last independent TV channel,” *The Guardian*, April 10, 2014, <http://www.theguardian.com/commentisfree/2014/apr/10/putin-war-dozhd-russias-last-independent-tv-channel>.

24 Tom Balmforth, “Russian Opposition ‘Likes’ Facebook,” *Radio Free Europe / Radio Liberty*, May 18, 2012, <http://www.rferl.org/content/russian-opposition-likes-facebook/24585388.html>.

also made use of social networking platforms to call attention to events. Additionally, crowdfunding websites such as RosUznik.org, which raises money for and coordinates the legal defenses of civil activists charged in the Bolotnaya Case, have emerged as a way for opposition activists to organize support efforts online.<sup>25</sup>

## Violations of User Rights

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, during 2013 and early 2014, Russia adopted a complex set of laws and other acts, which, coupled with repressive law enforcement and judicial practices, have reduced the constitutional guarantees of freedom of speech. Additionally, surveillance and detentions of online activists have increased. Courts tend to side with public authorities, refusing to apply directly applicable provisions of the constitution and international treaties of the Russian Federation.

In July 2012, the State Duma passed amendments to the criminal code that recriminalized defamation, after having just decriminalized it less than a year earlier. Revisions to Article 129 of the code officially make defamation a criminal offense, with penalties including a fine of up to RUB 5 million (approximately US\$138,000). Over the past year there were more criminal charges for illegal activity on the internet, and punishments for posting extremist content (which often refers to criticism of the authorities) were also increased.

During 2013 there were more than 200 cases of criminal prosecution against internet users for the dissemination of information online.<sup>26</sup> The majority of these criminal cases were connected to right-wing publications on social networks. The usual penalty for these crimes is correctional work, probation or fines. In addition to these cases, however, there were also prosecutions launched against politicians, activists, and journalists. One of the more troubling cases of politically-motivated prosecution involved Sergei Reznik, a well-known blogger who reported on alleged corruption involving local officials. In November 2013, a court sentenced Reznik to 18 months in a labor camp on charges of bribery, insulting an official, and misleading the authorities.<sup>27</sup>

In March 2013, Mikhail Afanasyev, the editor-in-chief of the online media outlet *Novy Fokus*, was charged with criminal defamation for publishing an opinion piece online in which he accused a police officer of lying about him in court. Previously, Afanasyev had been arrested on charges of hooliganism for attempting to video record an arrest, though these charges were later dropped. On September 6, 2013, Afanasyev was acquitted of the criminal defamation charges.

---

25 "Arrest extension validated for Moscow riot participants," Russian Legal Information Agency, August 8, 2012, [http://rapsin-ews.com/judicial\\_news/20120806/264133072.html](http://rapsin-ews.com/judicial_news/20120806/264133072.html).

26 AGORA Association, February 4, 2014, Openinform.ru, <http://openinform.ru/news/pursuit/04.02.2014/29343/>

27 "Opposition blogger sentenced to jail in Russia," Committee to Protect Journalists, November 26, 2013, <https://cpj.org/2013/11/opposition-blogger-sentenced-to-jail-in-russia.php>.

## Russia

Opposition leader and prominent blogger Alexei Navalny has faced prosecution multiple times over the past few years. On April 22, 2014, Navalny was found guilty of libeling a district councilor on Twitter and was fined US\$8,400. Under house arrest at the time of the alleged Twitter post, Navalny denied posting the tweet, as his house arrest precluded him from using the internet. His spokesperson stated that the case was politically motivated and was intended to move Navalny from house arrest to pretrial detention.<sup>28</sup>

Privacy and anonymity are key concerns for many online users in Russia. On May 5, 2014, Putin signed a law that considers any website with over 3,000 viewers, including blogs and social media accounts, to be "mass media."<sup>29</sup> The law requires these outlets to register with the government, thus decreasing the space for these users to communicate anonymously online. Additionally, the new measure contained wording that would require any services hosting such platforms to maintain records of these users' data on servers located within Russia, a provision which was further substantiated by a broader data localization law passed in July 2014 that requires all foreign internet companies to host Russians' data on servers within the country.<sup>30</sup>

There are currently no restrictions on the use of circumvention tools or anonymizers, although 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 is developing a package of laws to block access to Tor and foreign proxy-servers for Russian users.<sup>31</sup> Presently, identification is needed for signing a contract for internet access or cellular services. Additionally, owners of public Wi-Fi spots are required to use content filters to protect children from potentially accessing "harmful" information (Article 6.17 of the code of administrative offenses). This requirement may force owners to implement age checks for users.

In July 2013, members of the State Duma sent a request for clarification to Roskomnadzor regarding the fact that the service Google Translate allows users to open websites that are blocked in Russia. The members reported their intent to resolve this method of circumvention; however, no further steps have been taken to date.<sup>32</sup>

The electronic surveillance system in Russia, known as the "system for operational investigative measures," or SORM, was launched in the late 1990s, and recent evidence suggests that the Russian government has significantly increased its surveillance capabilities over the past few years. Records of government procurement documents revealed the extent to which the government had expanded its domestic surveillance infrastructure, including upgrades to telephone and Wi-Fi networks, allowing the government to extensively monitor and filter all communications during the

28 Andrey Ostroukh, "Alexei Navalny Found Guilty in Libel Case," *The Wall Street Journal*, April 22, 2014, <http://online.wsj.com/articles/SB10001424052702303825604579517402175983832>.

29 Neil MacFarquhar, "Russia Quietly Tightens Reins on Web With 'Bloggers Law,'" *New York Times*, May 6, 2014, <http://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html>.

30 This broader data localization law was passed outside of the coverage period for this report. See: Paul Sonne and Olga Razumovskaya, "Russia Steps Up New Law to Control Foreign Internet Companies," *Wall Street Journal*, September 24, 2014, <http://online.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920>.

31 "FSB conducts the law against anonymity on the Net," *Izvestia.ru*, August 16, 2013, <http://izvestia.ru/news/555552> [In Russian]

32 "Google Translate can be used to open website which is blocked in Russia," *RG.ru*, July 31, 2013, <http://www.rg.ru/2013/07/31/google-site-anons.html> [In Russian]

Winter Olympic Games in Sochi.<sup>33</sup> Such surveillance technology has been used for political purposes in the past, including the targeting of opposition leaders. In a Supreme Court case in November 2012 involving Maxim 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 so-called "extremist activities," namely antigovernment protests.

Online surveillance represents somewhat less of a threat in the major cities of Moscow and Saint 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 license 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. At the same time, experts note that there is no information about government efforts to bring to account security officers who abuse tracking methods.<sup>34</sup> ISPs and mobile operators are required to provide network access to law enforcement agencies in conducting search operations, as well as provide other information requested by the prosecutor's office, the Interior Ministry, the FSB and the Investigative Committee.

In addition to surveillance, violence against online journalists escalated over the past year. There were at least 24 cases of violence or threats documented in 2013.<sup>35</sup> On July 9, 2013, Akhmednabi Akhmednabiyev, a journalist for the online news site *Caucasian Knot* and the deputy editor of the independent news outlet *Novoye Delo*, was shot outside of his house in Dagestan. Colleagues believe the murder was politically motivated, given that Akhmednabiyev frequently reported on sensitive topics such as government corruption, arbitrary detentions, and protests.<sup>36</sup> Akhmednabiyev had survived a previous assassination attempt six months earlier.

There has also been an increase in the number of cyberattacks on independent media, blogs, and news portals. Websites that suffered DDoS attacks include 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 *Blogger51.ru*, and the websites of *Novaya Gazeta* and the TV channel *Dozhd*.

According to a Kaspersky Lab report, 2013 was marked by a 20-fold increase in power of DDoS attacks in the Russian online sphere (RuNet). The most powerful attack to date was organized against the website of *Novaya Gazeta* and amounted to 60 Gbps, compared to the maximum attack

---

33 Shaun Walker, "Russia to monitor 'all communications' at Winter Olympics in Sochi," *The Guardian*, October 6, 2013, <http://www.theguardian.com/world/2013/oct/06/russia-monitor-communications-sochi-winter-olympics>.

34 Alexei Alikin. SORM in public. *Russkaya Planeta*. July 29, 2013, [http://rusplt.ru/policy/policy\\_3890.html](http://rusplt.ru/policy/policy_3890.html)

35 AGORA Association, February 4, 2014, *Openinform.ru*, <http://openinform.ru/news/pursuit/04.02.2014/29343/>

36 Committee to Protect Journalists, "Akhmednabi Akhmednabiyev," July 9, 2013, <http://cpj.org/killed/2013/akhmednabi-akhmednabiyev.php>.

power reflected in 2012 of 2.9 Gbps.<sup>37</sup> On January 31, 2014, *Novaya Gazeta* reported that the police investigative department in Saint Petersburg had opened a criminal investigation into the attack; this case remains the only official response to the cyber threat to independent media.

---

37 "The Power of DDos Attacks in Russian Has Grown 20 Times," TheRuNet.com, July 3, 2013 <http://therunet.com/news/1189-moschnost-ddos-atak-v-runete-vyroslo-v-20-raz> [In Russian]