

Russia

	2015	2016		
Internet Freedom Status	Not Free	Not Free	Population:	144.1 million
Obstacles to Access (0-25)	10	10	Internet Penetration 2015 (ITU):	73 percent
Limits on Content (0-35)	23	23	Social Media/ICT Apps Blocked:	No
Violations of User Rights (0-40)	29	32	Political/Social Content Blocked:	Yes
TOTAL* (0-100)	62	65	Bloggers/ICT Users Arrested:	Yes
			Press Freedom 2016 Status:	Not Free

* 0=most free, 100=least free

Key Developments: June 2015 – May 2016

- A package of antiterrorist legislative amendments known as Yarovaya's Law was proposed during the coverage period, and signed into law in July. The law undermines the security of encrypted communications and increases authorities' access to user data (see **Surveillance, Privacy, and Anonymity**).
- The past year saw a dramatic hike in arrests of social media users, with the first maximum five-year sentence issued for so-called extremist expression online (see **Prosecutions and Detentions for Online Activities**).
- An unprecedented number of attacks were registered against social media users in the past year, with members of political VKontakte groups targeted with physical violence and suffering property damage (see **Intimidation and Violence**).

Introduction

The Russian government continued to erode user rights, imprisoning social media users, while online activists have been targeted with violence and cyberattacks.

Internet freedom in Russia has deteriorated steadily over the past few years, as Vladimir Putin continues to consolidate power in his third term as president. The authorities have demonstrated a low tolerance for critical expression, readily blocking content critical of Russia's annexation of Crimea and involvement in the conflict in the Donbass region of Ukraine. Anti-extremism laws are widely used as a pretext to block political content, often without judicial oversight. Independent online news outlets continue to face legal and economic pressure from the government, and are often forced to take down politically sensitive content or otherwise face retaliatory action. LGBTI social media groups and websites are also routinely censored, as well as websites run by the political opposition.

The past year saw an unprecedented crackdown on social media users, with the authorities issuing long prison sentences and applying other legal sanctions against users who post or even share material online that contradicts the official Kremlin position on controversial issues. While the coverage period saw the first maximum five-year sentence issued in December 2015 to a social media user under Russia's broad anti-extremism laws, a new law passed in July 2016 increases the maximum sentence to seven years for "inciting" or "justifying" terrorism online, expanding the powers of authorities to target social media users. Social media users who are openly critical of the Russian regime have also faced a targeted campaign of physical violence and acts of intimidation, often perpetrated by unidentified assailants encountered on the street or near their homes.

The Russian government has continued to undermine citizens' privacy and security online, passing laws which grant the authorities greater legal access to personal data and more power over tech companies. Data localization rules, which entered into force in September 2015, may make it easier for the Russian government to access internet users' information. Coupled with new laws passed in July 2016 mandating extensive data retention, conditions are rife for future infringements on users' right to privacy.

Obstacles to Access

Access to the internet is affordable in Russia and connection speeds are high compared to the rest of the region, while internet penetration rates continue to increase. However, the ICT industry is concentrated, with a state-owned ISP dominating the market and planning to expand.

Availability and Ease of Access

Internet access in Russia continues to gradually expand. According to the Public Opinion Foundation, the internet penetration rate reached 57 percent by the end of 2015, compared with 51 percent by the end of 2014.¹ The International Telecommunication Union (ITU) places the figure somewhat

1 Public Opinion Foundation, "Internet in Russia: Dynamics of Penetration. Winter 2015-2016" [in Russian], April 22, 8, 2016 <http://ow.ly/uj5Q300xtdl>.

higher, reporting an internet penetration rate of 73 percent by the end of 2015, compared to 71 percent in 2013 and just 29 percent in 2009.²

The speed of access is also increasing. According to Akamai, Russia was one of 20 countries in the third quarter of 2015 with average connection speeds at, or above, 10 Mbps. This is 12 percent higher than in 2014, and places Russia far ahead of other post-Soviet states. However, connection speeds remain behind top-performing countries such as Sweden, which enjoys a connection speed of 17.4 Mbps.³

According to TNS Russia, 62 percent of Russians living in cities with over 100,000 inhabitants use smartphones to access mobile internet, and 34 percent access the web via tablets. Meanwhile, 59 percent of Russians in this group use home computers and 53 percent use laptops.⁴ According to the ITU, the mobile phone penetration rate reached 160 percent in 2015,⁵ indicating a greater number of subscriptions than inhabitants; for mobile broadband subscriptions, the rate was 65.9 percent.⁶

The average cost of a monthly internet plan in Russia is approximately US\$6 (RUB 400) for 3 Mbps.⁷ Though there is no significant gender divide when it comes to internet access in Russia,⁸ a regional divide persists with respect to internet speed and price. Inhabitants of the subarctic cities of Yakutsk and Novy Urengoy pay the highest prices in Russia, more than double the national average for monthly internet access.⁹

The average cost of internet access makes up approximately 1 percent of an average salary, indicating that access is relatively affordable for most citizens. 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 could not afford to access the internet.¹⁰ The median monthly income of Russia citizens according to the Ministry of Labor and Social Protection was US\$499 (RUB 30,514) in the third quarter of 2015.¹¹

Nevertheless, while people with median and higher incomes can easily afford the internet, 20.3 million Russians—nearly 14 percent of the population—lived below the poverty line as of the end of 2015. This is an increase of 2 million from the previous year.¹²

Restrictions on Connectivity

During the coverage period, there were no government-imposed internet outages or disruptions to communication platforms. However, certain bills currently under discussion may make it easier for the government to do so in the future. In February 2016, *Vedomosti*, a business daily, reported that the Communications Ministry was in the early stages of drafting a bill titled “On the Autonomous Internet System,” which seeks to increase government control over internet infrastructure in Russia by

2 International Telecommunication Union, “Percentage of Individuals Using the Internet,” 2000–2015, <http://bit.ly/1cblxxY>.

3 Akamai, “State of the Internet Q3 2015 Report”, .

4 TNS Russia, “TNS Web Index”, April 2016, <http://ow.ly/pAWV300xrJW>.

5 International Telecommunication Union, “Percentage of individuals using the Internet,” 2015, <http://bit.ly/1cblxxY>.

6 Broadband Commission, *The State of Broadband 2015: Universalizing Broadband*, September 2015, <http://bit.ly/1CdQnO>.

7 Yandex, “Internet in Russian regions” [in Russian], Spring 2016. <http://ow.ly/mGWQ300CBd5>

8 TNS Russia, “TNS Web Index”, April 2016, <http://ow.ly/pAWV300xrJW>

9 Yandex, “Internet in Russian regions” [in Russian], Spring 2016, <http://ow.ly/mGWQ300CBd5>.

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

11 Ministry of Labor and Social Protection, “Per capita incomes in the Russian Federation” [in Russian], December 18, 2015, .

12 Georgy Peremitin, “The number of the poor in Russia increased by more than two million in 2015” [in Russian], *RBC*, December 10, 2015, .

transferring control of traffic exchange points and .ru and .рф domains to the government. Further, the bill seeks to control international internet traffic in Russia by requiring operators of autonomous systems to set up SORM, the system Russia uses to conduct state surveillance¹³ (see Surveillance, Privacy, and Anonymity).

In May 2016, the Ministry of Telecommunications and Mass Communications published amendments to its state program “Information Society”, aiming to bring 99 percent of Russian internet traffic within Russian borders by 2020, compared to 70 percent in 2014.¹⁴ The ministry plans to establish a system for monitoring the connectivity and network stability in the Russian segment of the Internet, claiming that these changes will bring increased stability to internet, safeguarding it from foreign interference or disconnection. However, observers such as Alexey Platonov, director of the “Technical Center Internet,” which provides technical support for domain infrastructure in Russia, have suggested that the changes resemble a move towards the Chinese Firewall model. The move may increase the authorities’ ability to block international traffic and potentially cut Russia’s network off from the rest of the world.¹⁵

ICT Market

The communications market in Russia is still relatively concentrated among a few companies. State-owned Rostelecom controls 37 percent of the broadband internet market, followed by ER-Telecom with 9 percent, MTS with 9 percent, and Vimpel Communications (Beeline) owning 7 percent. The remaining market share is split among smaller, local ISPs.¹⁶ Rostelecom plans to expand further, and will spend approximately US\$163 million (RUB 10 billion) on mergers and acquisitions to sustain and grow its market share.¹⁷ The market for mobile phone access is similarly concentrated. In the first quarter of 2016, four major companies—Mobile TeleSystems, Megafon, Vimpel Communications, and Tele2—controlled 99 percent of the market.¹⁸

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 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. In addition to conducting its own monitoring of the internet, Roskomnadzor receives

13 Anastasia Golitsyna, Elizabeth Sergina Peter Kozlov “The government wants to control the internet traffic in the country” [in Russian], *Vedomosti*, February 11, 2016, <http://ow.ly/ZTJt>. Under the bill, domain name systems would be associated with IP address assignment, and a traffic monitoring system would be introduced.

14 Pavel Kantyshev, Anastasia Golitsyna “Russian internet will be completely isolated in 2020” [in Russian], *Vedomosti*, May 13, 2016, <http://ow.ly/3eHq300CCja>.

15 Alyona Sukharevskaya, ““Hints of China”: whether it is possible to turn off Russia from the global Internet” [in Russian], *RBC*, February 11, 2016, <http://ow.ly/ZTKs9>.

16 ICT Online, “TMT Consulting” published the rating about broadband Internet in Russia in 2015 [In Russian], February 16, 2016, <http://ict-online.ru/news/n128614/>.

17 Vladislav Novy, Denis Skorobogatko, Anna Balashova, “Rostelecom is going shopping,” *Kommersant*, November 20, 2015, <http://www.kommersant.ru/doc/2211111>.

18 Advanced Communication & Media, “Cellular Data, Q4 2014,” accessed July 14, 2016, http://www.acm-consulting.com/news-and-data/data-downloads/doc_download/140-1q-2015-cellular-data.html.

complaints about online content from the public, the courts, and other official bodies such as the General Prosecutor's Office.¹⁹ Roskomnadzor is also in charge of implementing the so-called "Bloggers' Law," requiring bloggers with more than 3,000 daily readers to register with the regulator.

Limits on Content

The Russian authorities censor a wide range of topics online, most often under the pretext of anti-extremism measures. Content subject to blacklisting or removal includes LGBTI expression, the conflict in Ukraine, and political opposition. The authorities have also pressured international platforms, such as Wikipedia, into removing select pages. Online outlets are subject to political and economic pressure to publish Kremlin-friendly content, while the government actively manipulates public opinion through state-controlled media and paid commentators.

Blocking and Filtering

Within the coverage period, Russian authorities have continued to use anti-extremism legislation to restrict access to content related to radical Islam, political opposition, nationalism, the conflict with Ukraine, and other topics. According to the SOVA Center for Information and Analysis, a Moscow-based nonprofit, many websites continue to be blocked without proper justification.²⁰

From 2012 to 2013 the Russian government enacted legal amendments that gave several agencies—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 the following types of content without a court order: 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 order, provided that the court finds the content illegal.

According to the nonprofit organization RosComSvoboda, which conducts ongoing monitoring of blocked content, the following were blocked by the end of May 2016:

- 1,587 sites for extremism and calls for protests (by orders of Prosecutor General's Office)
- 9,982 sites containing drug-related content (by orders of the Federal Drug Control Service)
- 228 sites containing suicide propaganda (by orders of the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing, or Rospotrebnadzor)
- 5,253 sites for the distribution of child pornography (by orders of Roskomnadzor)
- 9,593 sites for the publication of various prohibited information (based on court decisions)
- 1,465 sites for copyright infringement (based on decisions of Moscow City Court)

¹⁹ Daniil Turovsky, "How Roskomnadzor operates" [in Russian], *Meduza*, March 13, 2015,

²⁰ Marya Kravchenko, Alexander Verhovsky, "Misuse of anti-extremism legislation in Russia in 2015" [in Russian], *Sova Center*, March 2, 2016 <http://www.sova-center.ru/misuse/publications/2016/03/d33946/>.

- 6,313 sites for information about gambling (by orders of the Federal Tax Service).²¹

Ukraine and Crimea remain areas of particular sensitivity for Russian authorities, with numerous Ukrainian websites blocked from within Russia. Ukrainian news websites Korrespondent.net, Bigmir.net, and Liga.net were blocked without a court order for quoting Refat Chubarov, the leader of the Crimean Tatar national movement in Ukraine, as saying that Crimea should be returned to Ukraine.²² In May 2016, Krym.Realii (“Crimea.Realities”), a project of Radio Free Europe/Radio Liberty, was blocked within Russia and Crimea by Roskomnadzor after Crimea’s de facto Prosecutor-General called for the website’s closure for allegedly inciting inter-ethnic hatred and extremism.²³ Additionally, the website of the Consumer Rights Defenders Society was blocked for several months until September 2015, after the group posted an article recommending that Russian travelers to Crimea enter through Ukraine, a statement seen by some as undermining Russia’s sovereignty in Crimea. Roskomnadzor blocked the site on extremism grounds according Federal law 398, known as “Lugovoi’s law,” which allows authorities to block websites for extremism on the orders of the Prosecutor General Office without a court order.

The authorities continue to censor information online on political opposition, including the website of opposition leader Garry Kasparov which was originally blocked in 2014 by Roskomnadzor for containing calls to illegal activity.²⁴ Two websites—srywvyborow.blogspot.ru and activism.win—were blocked by Roskomnadzor in July 2016 for posting calls to boycott upcoming legislative elections. A Roskomnadzor spokesman described the websites as pure propaganda.²⁵ Roskomnadzor also temporarily blocked the website of the Communist workers movement, work-way.com, after it posted articles related to an upcoming truck-drivers’ strike.²⁶

In cases where websites employ the HTTPS protocol, which prevents ISPs from blocking individual pages within the domain, ISPs are often forced to block entire platforms in order to comply with Roskomnadzor’s instructions to block a single page. For example in June 2015, the Internet Archive, a platform which allows users to view webpages that have been modified or removed, was blocked in its entirety after Roskomnadzor banned a saved webpage called “Solitary Jihad in Russia.”²⁷ Similarly, ISPs temporarily blocked all of Wikipedia and Reddit in August 2015 after an order from Roskomnadzor banning articles related to recreational drug use.²⁸

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 block-

21 RosComSvododa, “Distribution of blocked sites across departments” [in Russian]. Accessed on July 18, 2016, <https://reestr.rublacklist.net/visual/>.

22 SOVA Center for Information and Analysis, “Chronology of the Internet filtration in Russia” [in Russian], February 29, 2016, <http://www.sova-center.ru/misuse/publications/filtr/2016/01/d33687/>.

23 TASS, “Online media “Crimea.Realities” is banned in Russia” [in Russian], May 16, 2016, <http://special.itar-tass.com/politika/3274509>.

24 “Russia blocks internet sites of Putin critics,” Reuters, March 13, 2014, <http://www.reuters.com/article/us-russia-internet-idUSBREA2C21L20140313>.

25 SOVA Center for Information and Analysis, “Chronology of the Internet filtration in Russia” [in Russian], July 8, 2016, <http://www.sova-center.ru/misuse/news/elections/2016/07/d35001>.

26 SOVA Center for Information and Analysis, “Chronology of the Internet filtration in Russia” [in Russian], February 29, 2016, <http://www.sova-center.ru/misuse/publications/filtr/2016/01/d33687/>.

27 Kevin Rothrock, “Russia Bans the Internet Archive’s ‘Wayback Machine,’” *Global Voices*, June 25, 2015, <http://ow.ly/ZVex2>.

28 Shaun Walker, “Russia briefly bans Wikipedia over page relating to drug use,” *Guardian*, August 25, 2015, <http://bit.ly/1hbjdvn>; Andrew Griffin, “Reddit banned in Russia because of one thread,” *Independent*, August 13, 2015, <http://ind.pn/1PvYKzY>.

ing 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. According to RosComSvoboda, 93 percent of accidental blockings occurred due to blocking orders carried out on the basis of IP addresses.²⁹

The head of Roskomnadzor, Alexander Zharov, announced in December 2015 that the regulatory body is in the process of launching an automated online content analysis and filtering system. The technology, which will assist Roskomnadzor in identifying content to be blocked, has been test-launched in 19 regions across the country.³⁰ Some regions, such as Tatarstan, have separately introduced automated content monitoring systems.³¹

Providers of public internet access, including libraries, cafes, and educational institutions, are responsible for ensuring that the content available to their users is filtered in compliance with Article 6.17 of the administrative code on protecting children from harmful information.³²

Content Removal

Roskomnadzor typically receives orders from government bodies, including the Prosecutor General's Office and Federal Drug Control Service, to enforce the censorship of content deemed illegal and, in some cases, Roskomnadzor itself identifies illegal content. Roskomnadzor must then instruct the hosting provider to issue a warning to the website. Website owners have the right to appeal the restriction in court, but are often given a short window of time to do so. As a result, website owners quickly delete the banned information, rather than risk having the entire site blocked. If the content is not removed, the page is then included on a blacklist and must be blocked by ISPs within 24 hours after receiving a warning from Roskomnadzor. ISPs face fines for failing to block websites included on Roskomnadzor's blacklist.

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. “Open Russia,” an online portal launched by opposition figure Mikhail Khodorkovsky, was urged to delete an article about a demonstration in the memory of murdered opposition leader Boris Nemtsov.³³ Similarly, *The New Times*, a Moscow-based publication that

29 RosComSvoboda, “Distribution of blocked sites across departments” [in Russian]. Accessed on July 18, 2016, <https://reestr.rublacklist.net/visual/>.

30 Vladimir Zykov, “Roskomnadzor tests a monitoring system to analyze online media” [in Russian], *Izvestia*, December 25, 2015, <http://ow.ly/ZTVLX>.

31 Official site of the prosecutor's office of Tatarstan, “Tatarstan Prosecutor's Office continues to implement large-scale project to counter offenses on the internet,” [in Russian], December 16, 2015, <http://ow.ly/ZTXno>.

32 Sova Center, “Inappropriate enforcement of anti-extremist legislation in Russia in 2015,” June 6, 2016, <http://www.sova-center.ru/en/misuse/reports-analyses/2016/06/d34694/>.

33 SOVA Center for Information and Analysis, “Chronology of the Internet filtration in Russia” [in Russian], January 25, 2016, <http://www.sova-center.ru/misuse/publications/filtr/2016/02/d33930/>.

is critical of the Kremlin, received a warning about an article in February 2016 for failing to mention that the Ukrainian ultra-nationalist group Right Sector is banned in Russia. Interestingly, *the New Times* received this warning on the same day it published an investigative article about President Putin's daughter, raising speculation that the warning was retaliation for publishing about Putin's secretive family.³⁴

In August 2015, Wikipedia was temporarily blocked in Russia for less than a day after Russian authorities were unsuccessful in removing a single Wikipedia article about "charas," a form of cannabis, due to Wikipedia's HTTPS protocol. Though access to Wikipedia was promptly restored, some have speculated that this could be part of a wider strategy to threaten platforms such as Wikipedia with bans over single pages in order to, ultimately, force them to give up on HTTPS, allowing the authorities to conduct targeted blocking.³⁵ Roskomnadzor had reportedly failed to provide Wikipedia with the appropriate warning prior to blocking.³⁶ Wikipedia's community of authors voted to remove the offending content in order to safeguard Wikipedia in Russia, and the article was ultimately edited so as to comply with Russian law.³⁷

Russian authorities continue to target LGBTI groups on social media. In September 2015, Roskomnadzor ordered VKontakte to block five accounts of LGBTI groups on the social media platform, after a court in Barnaul found that the pages constituted illegal "gay propaganda." The most prominent of these groups was Children-404, a support group for Russian LGBTI teenagers. VKontakte complied with the order, claiming that Roskomnadzor would have otherwise blocked the social media platform in its entirety.³⁸

Foreign companies do not always comply with the demands of Russian authorities. According to a transparency report from Twitter, Russian authorities submitted 1,735 requests for content removal between July and December 2015—a 25-fold increase on the previous year. Twitter found that only 5 percent of these requests constituted a violation of the company's rules.³⁹ In July-December 2015, Facebook complied with 56 requests issued by Russian authorities to restrict content, up from 28 in the prior six months.⁴⁰ Meanwhile, Google received 1,570 requests from the Russian government to restrict content from July-December 2015, complying in more than 75 percent of cases. Russia accounted for 32 percent of the total requests Google received in this period.⁴¹

In July 2015, President Putin approved a law on "the right to be forgotten," requiring search engines to remove links to false or outdated information about an individual.⁴² The petitioning individual must prove that the information warrants removal, though a court order is not required. Russia's search engine, Yandex, had voiced opposition to the law, highlighting that altering search results vi-

34 Alec Luhn, "Russian magazine cyber-attacked and fined after article on Putin's daughter," *The Guardian*, February 1, 2016, <http://ow.ly/ZYfGY>.

35 Shaun Walker, "Russia briefly bans Wikipedia over page relating to drug use," *The Guardian*, August 25, 2015, <http://ow.ly/ZVcpb>.

36 Stanislav Kozlovky, a message on Facebook to the author, March 23, 2016.

37 Shaun Walker, "Russia briefly bans Wikipedia over page relating to drug use," *The Guardian*, August 25, 2015, <http://ow.ly/ZVcpb>.

38 "Access to Children 404 group blocked for VKontakte users in Russia," *Russia Beyond the Headlines*, September 25, 2015, https://rbth.com/news/2015/09/25/access_to_children-404_group_blocked_for_vkontakte_users_in_russia_49555.html.

39 Twitter transparency report, <http://ow.ly/ZVeSB>.

40 Facebook, "Report on governmental requests" [in Russian], <https://govtrequests.facebook.com/country/Russia/2015-H2/>.

41 Google, "Transparency Report--Russia," <https://www.google.com/transparencyreport/removals/government/RU/?hl=en>.

42 Tetyana Lokot, "President Putin Signs Russian 'Right to Be Forgotten' Into Law," *Global Voices*, July 17, 2015, <http://ow.ly/ZVkr3>.

olates the constitutional right to seek, obtain, produce, and spread information,⁴³ in addition to raising concerns regarding the added burden placed on the company to make decisions about which content to remove. Though “right to be forgotten” laws exist in other jurisdictions, Russia’s law fails to provide limits in cases where the information relates to the public good or pertains to public figures.⁴⁴ In March 2016, three months after the law had been enacted, Yandex released data showing it received 3,600 removal requests, 51 percent of which were requests to remove truthful, but outdated information, often related to crimes. Yandex approved 27 percent of the requests it received.⁴⁵

Search engines and news aggregators such as Google News and Yandex.Novosti (Yandex News) will be placed under additional pressures once an amendment to the Law on Information, Information Technology and Data Protection, passed in June 2016, enters into force in January 2017.⁴⁶ The new law will require aggregators with over one million daily users to prevent the dissemination on their platforms of terrorist content, pornography, cruelty, the disclosure of state secrets, and other content, facing fines if they do not comply.⁴⁷ News aggregators will also be responsible for the accuracy of some of the information disseminated through their platforms with some exceptions, such as direct quotes from the media.⁴⁸ Russian news aggregators like Yandex and Mail.ru have strongly pushed back against the amendments, calling the measures excessive and arguing that it may become impossible to provide their services under the new regulations.⁴⁹

Media, Diversity, and Content Manipulation

As the space for independent print and broadcast media in Russia shrinks, online publications and social networks become increasingly important platforms for critical expression and social mobilization, with 48 percent of Russians now turning to the internet to find trustworthy news sources.⁵⁰ However, 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. 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, corruption, war with Ukraine, the annexation of Crimea, violations of civil rights, religion, and the LGBTI community.

Several online media outlets that were originally blocked in March 2014 remain restricted, including Grani.ru, Kasparov.ru, and Ej.ru. 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

43 Yandex, “Right to forget about search,” [in Russian] June 5, 2015, <http://ow.ly/ZVklE>.

44 Article 19, “Legal analysis: Russia’s right to be forgotten,” September 16, 2015, <https://www.article19.org/resources.php/resource/38099/en/legal-analysis-russia-s-right-to-be-forgotten>.

45 Yandex, “About the implementation of the right to be forgotten,” [in Russian] March 25, 2016, <http://ow.ly/ZVlfr>.

46 Consultant Plus, Act 208, June 23, 2016, http://www.consultant.ru/document/cons_doc_LAW_200019/.

47 Ekaterina Bryzgalova, “Deputies satisfied demands of the Internet industry” [in Russian], *Vedomosti*, June 13, 2016, <https://www.vedomosti.ru/technology/articles/2016/06/14/645179-novostnim-agregatoram>.

48 “The draft law about news aggregators passed Duma,” [in Russian] *BBC Russian*, June 10, 2016, http://www.bbc.com/russian/news/2016/06/160610_duma_news_agregator.

49 Anastasia Golitsyna, “Mail.Ru Group may close its news service,” [in Russian] *Vedomosti*, April 21, 2016, <http://ow.ly/cWou300CNGQ>.

50 Public Opinion Foundation, “News on the internet”, January 25, 2016, <http://ow.ly/ZYd7X>.

individuals are still able to use circumvention 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 some circumvention tools, all blocked resources have reported a significant reduction in traffic.

Online outlets continue to face government pressure to publish news in line with the Kremlin's views. 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.⁵¹

One of the few independent major media outlets, RBC, owned by Russian billionaire Mikhail Prokhorov, sacked its key managers and reporters in May 2016, reportedly under the pressure from Kremlin.⁵² RBC was renowned for its critical investigatory journalism exposing corruption, often targeting Putin and his inner-circle. The RBC website alone had 11,765,000 monthly readers in Russia in April 2016, and was the only major media outlet in Russia to report on Putin's links to the Panama Papers revelations. Elizaveta Osetinskaya stated that the publication had become a "red rag" for the Kremlin because of its critical coverage of the Panama papers, though the Kremlin denied any involvement in the sacking of RBC's top editors.⁵³

Russian authorities continue to use the assistance of paid commentators to influence online content. 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 the harassment of opposition activists. Media outlets including *Forbes* and *the Guardian* have reported increases in anti-Western user comments on any comments related to Russia or Ukraine.⁵⁴ The issue of progovernment trolling gained significant attention in Russia in May 2015 when the Internet Research Agency, a "troll factory" located in St. Petersburg, was sued by a former employee to bring the activities of the agency to public attention, a case which received much media attention domestically and internationally.⁵⁵ In an attempt to counter the prevalence of government manipulation in the media, Alexey Kovalev, a former employee of state-friendly media outlet RIA Novosti (now Rossiya Segodnya), created an online platform called Noodle Remover, which aims to debunk false or misleading news published in the Russian media.⁵⁶

Authorities have continued to introduce onerous regulatory requirements and restrictive laws affecting online media, pushing some outlets to downsize, sell, or exit the market altogether. On January 1, 2016, new amendments to the Law on Mass Media came into force, prohibiting foreign citizens and organizations from owning more than a 20 percent stake in Russian media. As a result, foreign media holdings are leaving Russia and, in some cases, ownership is being transferred to Russian entities.⁵⁷ For instance, German publishing house Axel Springer sold its assets, including *Forbes* (the

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

52 Ksenia Boletskaya, "RBC is not approved for reading," [in Russian] *Vedomosti*, May 13, 2016 <http://ow.ly/E9yx300CFxU>.

53 Max Seddon, "Editors at Russia's RBC media group sacked after Putin article," *Financial Times*, May 18, 2016, <http://ow.ly/iJX3300CG5T>.

54 Annika von Taube, "Russische Botschaft" [in German], *Zeit Online*, January 27, 2014, <http://bit.ly/1GQIUJ7>.

55 Adrian Chen, "The Agency," *The New York Times*, June 2, 2015, <http://ow.ly/ZYdJu>.

56 Kevin Rothrock, "One Man's Revenge Against Russian Propaganda," *Global Voices*, November 3, 2015, <http://ow.ly/ZUduA>.

57 Anastasia Bazenkova, "Foreign publishers quit Russia over media ownership law," *Moscow Times*, September 9, 2015, <http://ow.ly/ZYf2C>.

magazine and the website Forbes.ru), to Alexander Fedotov, the owner of Artcom Media Group. Sanoma Corp, a Helsinki-based media group, sold its share of the company that produces *Vedomosti*, a business daily and news portal (Vedomosti.ru), to Demyan Kudryavtsev, the former publisher of business media outlet *Kommersant*. Many observers regard the new local ownership requirements as an attempt by the Kremlin to secure greater influence and editorial control over these high-reach news outlets.⁵⁸ Furthermore, in May 2015, a new law on “undesirable organizations” introduced bans on disseminating information from blacklisted organizations, silencing many civil society voices. Individuals and smaller, independent outlets have been targeted by the “Bloggers’ Law.” Introduced in May 2014, the law requires sites with 3,000 or more daily visitors to register as a mass media outlet, which means bloggers can no longer remain anonymous and are held responsible for the accuracy of the content posted on the website, including comments made by third parties.

In response to the increasingly restrictive environment for independent online commentary, some publications choose to operate overseas. Perhaps the most notable example is Meduza.io, a critical online news outlet launched in Latvia. Meduza targets Russian audiences, reaching approximately 4 million monthly visitors,⁵⁹ and also publishes some content in English.

Another legislative development likely to curb online media diversity came in the form of a data localization law (Federal Law No. 242-FZ). The law entered into effect in September 2015, and requires companies to store personal data pertaining to Russian citizens on servers located in the country. In addition to surveillance and privacy concerns, the law is likely to force foreign tech companies out of Russia, with Spotify already reversing plans to enter the Russian market partly due to its inability to comply with data localization requirements as a cloud-based service.⁶⁰

Digital Activism

Despite continued government pressure, the internet remains the most versatile and effective tool for activism in the country, with frequent efforts to confront state propaganda, fight corruption, and organize protests. Videos exposing corruption on prominent activist Alexey Navalny’s YouTube channel frequently receive millions of views. A 2015 video exposing links between general prosecutor Yuri Chaika and the Tsapok gang, the criminals behind a notorious massacre in the town of Kushevskaya in southern Russia,⁶¹ has been viewed over 5 million times. The Chaika investigation has had a notable impact on the Russian public, with a study by *Kommersant* finding that 38 percent of Russians have at least heard of the YouTube video, and 78 percent believe it to be accurate.⁶²

Individuals are also creating online platforms and organizations to expose and scale back restrictions imposed on the internet in Russia. In December 2015, IT professional Leonid Volkov launched the Society for Defending the Internet (OZI), an organization working to defend internet freedom.⁶³ OZI has launched an online crowdfunding campaign to support its efforts to challenge the legality of SORM, technology used by the FSB to conduct surveillance online, ultimately aiming to create a so-

58 Peter Hobson, “Russian Owner Wants Modernised Moscow Times, Not Kremlin Stooge,” *The Moscow Times*, May 4, 2015, <http://bit.ly/2dtd3ok>.

59 Ilya Krasilchik, Facebook post [in Russian], April 1, 2016, <http://ow.ly/tLku300CNxt>.

60 Darya Luganskaya, “Spotify changed its mind to enter the Russian market,” [in Russian] *RBC*, February 2, 2015, <http://ow.ly/ZVnA3>.

61 FBK, “Chaika” [in Russian], December 1, 2015, <http://ow.ly/ZUbtn>.

62 Andrey Pertsev, “Almost half of Russians know about the film ‘Chaika’ about the family of general prosecutor,” [in Russian] *Kommersant*, December 23, 2015, <http://ow.ly/ZUcuh>.

63 Kevin Rothrock, “ISPs Take Kremlin to Court Over Online Surveillance,” *Global Voices*, February 3, 2016, <http://ow.ly/ZUdkp>.

called “people’s ISP” that would then sue the FSB once it is required to install SORM technology.⁶⁴ By July 2016, the activists had successfully obtained the necessary license to operate as an ISP.⁶⁵

Ruslan Leviev, an activist and programmer, established Conflict Intelligence Team (CIT), an online platform which publishes investigations into the actions of Russian troops in Ukraine and Syria, often using information sourced from social networks.⁶⁶ Leviev’s team was the first to reveal evidence of the deployment of Russian soldiers in ground operations in Syria, using the geolocations of photos found on social media.⁶⁷ CIT aims to bring more transparency to the Russian government’s involvement in foreign conflicts.⁶⁸

Violations of User Rights

Over the past year, Russian authorities substantially restricted user rights by passing laws which increase penalties for expression online while expanding the government’s access to personal data. More social media users than ever before faced arrests for voicing their criticism, and many face lengthy prison sentences. The authorities have taken steps to undermine the security of encrypted communications, passing a law in July 2016 that will compel encryption providers to grant access to authorities, a move which is likely to expose more netizens to legal sanction for their activities online.

Legal Environment

Although the constitution grants the right to free speech, this right is routinely violated, and there are no special laws protecting online 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, 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.

In July 2016, the Russian government introduced some of the harshest legislative amendments in post-Soviet Russia, collectively known as “Yarovaya’s Law,” amending nearly a dozen laws with wide ramifications for internet freedom.⁶⁹ The laws introduce prison terms of up to seven years for publicly calling for or justifying terrorism online.⁷⁰ The harsh penalties and broad wording of the law opens the door to abuse, namely the targeting of legitimate, nonviolent expression online.

64 Interview with Leonid Volkov conducted in March 2016.

65 Leonid Volkov, “The People’s ISP: Step 2” [in Russian], *leonidvolkov.ru*, July 5, 2016, <http://www.leonidvolkov.ru/p/147/>.

66 Darya Luganskaya, “Inside Big Brother: How Russians Created the ‘Red Web,’” *Global Voices*, November 17, 2015, <http://ow.ly/ZUefL>.

67 “Russian soldiers geolocated by photos in multiple Syria locations,” *Reuters*, November 8, 2015, <http://www.reuters.com/article/us-mideast-crisis-syria-russia-idUSKCN0SX0H820151108>.

68 Interview with Ruslan Leviev conducted in Moscow on March 26, 2016.

69 Consultant Plus, Act 375, Amendment to the Russian Criminal Code, Introducing Additional Counterterrorism Measures and Ensuring Public Safety, <http://bit.ly/2dt782G>.

70 Consultant Plus, Act 375, Amendment to the Russian Criminal Code, Introducing Additional Counterterrorism Measures and Ensuring Public Safety, <http://bit.ly/2dt782G>.

Penalties for extremist had been raised only a couple of years previously, with the passage of a series of amendments to the criminal code in 2014. The amendments significantly increased the penalties for online incitement to separatism or calls for extremism,⁷¹ with prison terms up to five years, and incitement to hatred, with prison terms up to six years.⁷² 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 are restricted from certain professions and their bank accounts can be frozen, even if they have not been convicted.

Russia's anti-extremism law is particularly broad as, according to Andrei Richter, Senior Advisor at OSCE Office of the Representative on Freedom of the Media. Richter noted Russia penalizes expression which is not necessarily abusive or discriminatory in nature.⁷³ Moreover, the interpretation of extremism in Russian has gradually expanded to include not only incitement of national, racial or religious enmity, humiliation of national dignity, but also propaganda of exceptionalism, superiority or inferiority of citizens on grounds of their religion, nationality or race, and public justification of terrorism.

Russian users may also be prosecuted under a host of older laws in the criminal code that may be applied to online speech. The Russian law establishes 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 (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 (Article 354.1), 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

Criminal charges are widely used in Russia to stifle critical discussion online. According to the SOVA Center for Information and Analysis, more journalists, activists, and online editors were subject to administrative and criminal prosecution within the past year. Individuals have been targeted for their posts on social media, including reposts, and many individuals prosecuted were targeted for posts related to Russia's conflict with Ukraine. Most arrests within the coverage period fell under Article 282 ("actions aimed at inciting hate or enmity") and Article 280 ("public calls to extremist activity"). Prison terms issued during the coverage period have also been lengthier than in the past.

The first non-suspended sentence for promoting extremism on social media under Article 282 of the Criminal Code was given to Oleg Novozhenin from the Siberian town of Surgut.⁷⁴ Novozhenin was sentenced in December 2015 to one year in a penal colony for posting audio and video files on so-

71 Criminal Code of the Russian Federation, Article 280.1 "Public calls to separatism," http://www.consultant.ru/document/cons_doc_LAW_10699/8b38952a3e743c7996551cbfe4b32d4d336a35ad/; Criminal Code of the Russian Federation, Article 280, "Public calls to extremist activity," http://www.consultant.ru/document/cons_doc_LAW_10699/c10532ab76df5c84c18ee550a79b1fc8cb8449b2/.

72 Criminal Code of the Russian Federation, Article 282, "Incitement to hatred," http://www.consultant.ru/document/cons_doc_LAW_10699/d350878ee36f956a74c2c86830d066eafce20149/.

73 Written comment provided by Andrei Richet via LinkedIn on March 27, 2016.

74 Igor Lesovsky, "A Russian court assigned a first real imprisonment for propaganda of extremism on social networks," [in Russian] *Kommersant*, December 1, 2015, http://ow.ly/ZVgUB_.

cial media which, according to the court, contained propaganda for Ukrainian nationalist party Right Sector and the Ukrainian Azov Battalion.⁷⁵

Soon after, in another precedent setting case, the first maximum sentence was issued under Russia's anti-extremism provisions. Vadim Tyumentsev, a blogger from the city of Tomsk, was sentenced to five years in prison in December 2015 for posting hate speech and calls to extremism online.⁷⁶ Tyumentsev had uploaded videos of himself calling on local citizens to participate in a rally against high bus fares and criticizing Russia's involvement in eastern Ukraine, suggesting that Ukrainian refugees should be expelled from Russia.⁷⁷

In December 2015, Krasnodar activist Darya Polyudova was sentenced to two years in a penal colony for public calls to separatism and extremism⁷⁸ after posting on VKontakte claims that Kuban is an ethnically Ukrainian region.⁷⁹

In May 2106, mechanical engineer and Tver resident Andrei Bubeev was sentenced to two years imprisonment for reposting material critical of Russia's actions in Crimea as well as an image of a toothpaste tube captioned "Squeeze the Russia Out of Yourself." According to the court's ruling, Bubeev's reposts amounted to public incitement of extremism and calls for the violation of the territorial integrity of the Russian Federation. Bubeev reportedly had only 12 friends on VKontakte.⁸⁰

Russian authorities have also targeted LGBTI expression, using a law against propaganda of non-traditional sexual relationships among minors to prosecute members of the LGBTI community. In December 2015, Sergey Alekseenko of Murmansk was found to have distributed "homosexual propaganda" among minors on the internet after he posted a supportive message in the VKontakte page of an LGBTI nonprofit. Alekseenko was fined RUB 100,000 (approximately US \$1,300).⁸¹

The Russian government continues to display a low tolerance for expression undermining the Russian Orthodox Church. In September 2016, Ruslan Sokolovsky, a blogger from Yekaterinburg, was sentenced to house arrest for incitement to hatred and insulting religious feelings after he uploaded videos of himself playing PokemonGo in a Yekaterinburg church.⁸²

A prominent blogger, Anton Nossik, was fined for inciting hatred after he posted a blog piece calling on President Putin to "wipe Syria off the map". Nossik was fined RUB 500,000 (US \$8,000).⁸³

75 Tetyana Lokot, "Russia Sees Its First Real Prison Sentence for 'Promoting Extremism' on Social Media," *Global Voices*, December 1, 2015 <http://ow.ly/ZVh6E>.

76 Freedom House, "Russia: Blogger Sentenced to Five Years Imprisonment", December 30, 2015, <http://ow.ly/ZVhFp>

77 "Russian court jails blogger for five years for 'extremist' posts," *Reuters*, December 30, 2015, <http://uk.reuters.com/article/uk-russia-blogger-idUKKBN0UD16O20151230>.

78 Tetyana Lokot, "Russian Activist Gets Two-Year Sentence for 'Calls to Extremism' on Social Networks," *Global Voices*, December 21, 2015, <http://ow.ly/ZVhq0>.

79 "Russian Activist Faces Trial On Separatism Charges," *Radio Free Europe*, September 3, 2015, <http://ow.ly/ZVhmd>.

80 Daniil Turovsky, "A trial for other people's words: a Tver resident is sentenced to two years in prison for the repost," [in Russian] *Meduza*, May 6, 2016, <http://ow.ly/Hw5Z300CXuc>.

81 "Russian LGBT activist fined for propaganda of homosexuality online," *Global Voices*, January 22, 2016, <https://globalvoices.org/2016/01/22/russian-lgbt-activist-fined-for-propaganda-of-homosexuality-online/>.

82 Sova Center, "Criminal case launched against blogger for playing PokemonGo in church," September 2, 2016, <http://www.sova-center.ru/misuse/news/persecution/2016/09/d35335/>.

83 "Russian blogger fined for call to 'wipe Syria off the map,'" *Al Arabiya*, October 4, 2016, <http://english.alarabiya.net/en/media/digital/2016/10/04/Russian-blogger-fined-for-call-to-wipe-syria-off-the-map-.html>.

Surveillance, Privacy, and Anonymity

Over the past couple of years, Russian lawmakers have enacted legislation which gives authorities ever-increasing powers to conduct intrusive surveillance online. Most recently, “Yarovaya’s Law,” a package of antiterrorism legislative amendments passed in July 2016, represents a bold attack on fundamental privacy safeguards on the internet. The new laws mandate that online services which provide encryption must assist the FSB with decoding encrypted data. Though this is an impossible task for many service providers—for example, due to the use of end-to-end encryption by many platforms—“organizers” that fail to cooperate could face a RUB 1,000,000 fine (USD \$15,000). The Electronic Frontier Foundation has suggested that the impossibility of full compliance is a deliberate feature of the law, ensuring that some service providers are de-facto breaking the law and thus giving Russian authorities great leverage.⁸⁴ Yarovaya’s Law also gives the authorities’ greater access to user data by requiring telecoms, ISPs, and “organizers of information” to store the content of users’ online communication—including text, video, and audio communication—for up to six months, while metadata must be stored for up to three years. Russian authorities will have access to this data without requiring a court order.⁸⁵ Following the passage of these antiterrorism amendments, 100,000 citizens signed a petition calling for the laws to be repealed.⁸⁶

Though the new data retention rules have not yet come into effect, the authorities have reportedly started taking measures to intimidate companies into compliance. Private Internet Access, a VPN provider, claimed in July 2016 that authorities raided their Russia office and seized some of their servers. The company believed the raid was linked to the fact that they do not log any user data. Private Internet Access decided to exit the Russian market as a result of the incident.⁸⁷

In what appears to be part of a wider effort to control user data, a data localization law was enacted in September 2015, requiring foreign companies which have personal data of Russian citizens to store their servers on Russian territory, potentially enabling easier access for security services.⁸⁸ Some foreign companies such as Uber⁸⁹ and Viber⁹⁰ have reportedly moved to comply with the law. Facebook and Twitter have declined to make public statements on the matter.

The Russian government employs SORM, or “system for operational investigative measures,” for its online surveillance activities, and must be installed by all ISPs. The current version, SORM-3, uses DPI technology, enhancing the ability of the security services to monitor content on all telecommunications networks in Russia. SORM has been used for political purposes in the past, including the 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 eaves-

84 Electronic Frontier Foundation, “Russia asks impossible in its new surveillance laws,” July 2016, <https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws>.

85 Elizaveta Archangelskaya, Alyona Sukharevskaya, “Yarovaya’s law: what an ‘anti-terrorist’ law means for internet users,” *RBC*, June 24, 2016 http://www.rbc.ru/technology_and_media/24/06/2016/576c0a529a79471bc44d2b57?from=rbc_choice.

86 “100,00 signatures collected calling for Yarovaya’s Law to be repealed,” *Radio Svoboda*, August 13, 2016, <http://www.svoboda.org/a/27919682.html/>.

87 Private Internet Access, “We are removing our Russian presence,” July 11, 2016, <https://www.privateinternetaccess.com/forum/discussion/21779/we-are-removing-our-russian-presence>.

88 Vladimir Prokushev, “Journalists Andrei Soldatov and Irina Borogan: the internet is for the enlightened,” [in Russian] *Horizontal Russia*, February 26, 2016, <http://ow.ly/ZVHMP>.

89 “Uber agreed to move the personal data of Russians to Russia” [in Russian], *Lenta.ru*, July 19, 2015, <https://lenta.ru/news/2015/07/10/uber/>.

90 Vladimir Zykov, “Viber moved its servers to Russia” [in Russian], *Izvestia*, December 19, 2015, <http://izvestia.ru/news/593438>.

drop on Petlin's phone conversations because he had taken part in "extremist activities," namely anti-government protests.

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.⁹¹ 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.

Use of circumvention tools is on the rise, with growing numbers of Russians turning to Tor⁹² and VPNs⁹³ to mask their identity online and access blocked content, particularly after Rutracker.org, a popular torrent tracker, was banned in Russia in January 2016.⁹⁴ According to Andrei Soldatov, Russian authorities are unsure of how to tackle this phenomenon,⁹⁵ though it is clear that circumvention tools are viewed with suspicion and regional courts are increasingly targeting these tools. In February 2016, a court in Anapa, a city in southern Russia, issued a verdict against RosComSvododa, a nonprofit monitoring banned content, ruling that an article with instructions on how to use anonymizers to access banned information was illegal.⁹⁶ However, RosComSvododa succeeded in demonstrating to the Ministry of Telecommunications and Mass Communications that the article had not violated any law and the article remains available.⁹⁷ Later in 2016, the Ministry of Telecoms and Mass Communications proposed a draft bill under which ISPs could be fined if websites publish "propaganda" outlining how to use anonymizers.⁹⁸

Intimidation and Violence

While attacks on journalists have been commonplace in Russia in past years, this year saw a dramatic spike in violent attacks against social media users, indicating a possible coordinated campaign to intimidate critical social media users into silence. Human rights organization Agora registered a total of 28 threats and attacks on online journalists and bloggers in 2015.⁹⁹ VKontakte users and group administrators in particular have been victims of intimidation and violence.

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

92 Tor Metrics, "Top-10 countries by directly connecting users," <http://ow.ly/icSE300CWR2>.

93 Alexey Rezanov, "Invasion of anonymous: how the ban on torrents affects the advertising market?" [in Russian] April 14, 2016, *RBC*, <http://ow.ly/NY0F300CWTT>.

94 Interview with Andrei Soldatov conducted in Moscow on March 25, 2016.

95 Interview with Andrei Soldatov conducted in Moscow on March 25, 2016.

96 Elizaveta Surganova, "A site was blacklisted for information about anonymizers," [in Russian] *RBC*, February 10, 2016, <http://ow.ly/ZXaQD>.

97 "RosComSvododa found a way to avoid blocking," [in Russian] *RBC* February 12, 2016, <http://ow.ly/ZXaRK>.

98 Alyona Sukharevskaya, "Telecom operators are proposed to be fined for information about anonymizers," [in Russian] May 19, 2016, <http://ow.ly/EkBe300Euuw>.

99 Damir Gaynutdinov, Pavel Chikov, "Internet freedom 2015: the triumph of censorship," [in Russian] *Agora*, February 16, 2016, <https://rublacklist.net/14661/> p.10.

In March 2016, Aleksandr Markov, an administrator of the VKontakte group “Criminal Regime” which is critical of Kremlin policies, was brutally assaulted when two strangers showed up at his Saint Petersburg apartment, pushed him down a staircase, and beat him. In June 2016, another Criminal Regime administrator, Yegor Alekseev, was attacked on the street by two men and suffered a broken nose, a concussion, and a fractured skull. Also in June, a VKontakte employee well known for his antigovernment posts was physically attacked in the street by unidentified men who called him a national traitor, a Jew, and member of the “fifth column”.¹⁰⁰

Social media users have also been subject to arson attacks in the past year. In April 2016, after student Ruslan Starostin posted a satirical image of Putin to his VKontakte page, his wife received a friend request from an unknown user who sent threatening messages related to the Putin post. Starostin’s car was then torched several hours later.¹⁰¹

A number of opposition activists and social media users have been subject to intimidation via VKontakte. In February 2016, Daniel Alexandrov, a political activist associated with the Watchers of Saint Petersburg opposition movement, came across a spoof VKontakte profile whose profile picture was a photo secretly taken of Alexandrov walking his dog.¹⁰²

In March 2016, a group of journalists, including correspondents from online publications *Mediazona* and *The New Times*, in addition to local and international human rights activists brought together by the Committee Against Torture on a tour of the Caucasus, were attacked by a group of masked men armed with batons and sharp objects. The assailants then set the bus on fire¹⁰³ and stole computers and other equipment from the group.¹⁰⁴ The Kremlin and Putin personally reacted to the accident saying that it should be investigated, though little progress has been made so far.¹⁰⁵

Technical Attacks

Cyberattacks against independent media, blogs, and news portals continue to inhibit Russian internet users’ ability to access such sites. In 2015, the human rights group Agora registered 30 hacking attacks against independent media and blogs, as well as hacks of emails and social media accounts.¹⁰⁶ In the past year, dozens of Russian civil society activists and journalists have been notified of attempts to compromise their accounts online, including Telegram and Gmail accounts, suggesting a coordinated campaign to compromise their security and access private information.

In May 2016, activists Oleg Kozlovsky and Georgy Alburov reported that their Telegram accounts were hacked through the messaging app’s SMS login feature. The activists never received an SMS

100 “Violence against Russian web dissidents raises fresh fears for internet freedoms,” *The Guardian*, June 23, 2016, <https://www.theguardian.com/world/2016/jun/23/violence-against-russias-web-dissidents-raises-fresh-fears-for-internet-freedoms>.

101 “People against Putin are beaten and their cars are burned,” *Real Time*, June 14, 2016, <http://www.currenttime.tv/a/27797019.html>.

102 “In St Petersburg, ‘Free Ingria’ activist beaten,” *The Village*, February 9, 2016, <http://www.the-village.ru/village/city/city/231301-alexandrov>.

103 Shaun Walker, “Journalists and activists beaten and bus torched on Chechnya tour,” *The Guardian*, March 10, 2016, <https://www.theguardian.com/world/2016/mar/10/journalists-beaten-and-bus-torched-on-chechnya-tour-say-activists>.

104 Ilya Rozhdestvensky, “The equipment of the journalists and human rights activists beaten in Ingushetia has been stolen” [in Russian], *RBC*, March 11, 2016, <http://ow.ly/ZUjUa>.

105 Maria Bondarenko, “Putin ordered to deal with the attack on journalists on their way to Chechnya.” [in Russian] *RBC*, <http://ow.ly/ZUjE2>.

106 Damir Gaynutdinov, Pavel Chikov, “Internet freedom 2015: the triumph of censorship,” [in Russian] *Agora*, February 16, 2016, <http://ow.ly/ZTWQn>.

notification of the login requests, and later discovered that their mobile phone company, MTS, had switched off SMS delivery for their SIM cards for several hours on the night of the breach. Though it remains unclear who accessed their accounts, Kozlovsky and Albuov strongly suspect that MTS colluded with the FSB to access their private communications.¹⁰⁷

Kozlovsky was targeted again in October 2016 among a group of Russian journalists and activists who received a notification from Google that “government-backed hackers” were trying to gain access to their accounts. At least 16 people received this message within a similar time frame, including journalist Ilya Klishin and Bellingcat researcher Aric Toler.¹⁰⁸

Earlier, in September 2015, two investigative journalists and a spokesperson for opposition leader Alexey Navalny reported that their email accounts had been breached using copies of SIM cards issued by MTS and Vypelcom (Beeline).¹⁰⁹

Independent news sites also continue to be targeted for their work. In June 2015, hackers called “Group SMERSH” published the emails of Elena Myasnikova, the vice president of the independent media group RBC.¹¹⁰ In February 2016, *The New Times*, an independent Moscow-based magazine and online news portal, became inaccessible following the publication of its investigation on Putin’s daughter. The editor-in-chief of *The New Times*, Yevgenia Albats, speculated that the outage was a result of massive distributed denial-of-service (DDoS) attacks.¹¹¹

In previous years, websites that suffered DDoS attacks included the internet project Demokrotor.ru, St 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 TV Dozhd.

107 “Neither pro-Kremlin pundits nor opposition safe from hackers,” *The Moscow Times*, May 4, 2016, <https://themoscowtimes.com/articles/ neither-pro-kremlin-pundits-nor-opposition-safe-from-hackers-52782>.

108 “Google warned Russian activists and journalists of attempts by secret services to access their email,” *Meduza*, October 11, 2016, <https://meduza.io/news/2016/10/11/google-predupredil-rossiyskih-aktivistov-i-zhurnalistov-o-popytkah-spetssluzhb-vzломat-ih-pochtu>.

109 “Novaya Gazeta journalists complained of email hacks,” *TJournal*, September 1, 2015, <https://tjournal.ru/p/novaya-gazeta-sim-violations>.

110 “Hackers posted the correspondence of the RBC vice president Elena Myasnikova,” [in Russian] *Roem*, June 2, 2015, <http://ow.ly/ZU9ib>.

111 Svetlana Reiter, Elizaveta Surganova, Ilya Rozhdestvensky, “The magazine *The New Times* received a warning for the “Right Sector” [in Russian], *RBC*, February 1, 2016, <http://ow.ly/ZU77x>.