PONARS Eurasia
NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

The Clampdown on Internet Activities in Russia and the Implications for Western Policy

PONARS Eurasia Policy Memo No. 350
September 2014

Mark Kramer
Harvard University

One of the most worrying recent trends in Russia has been the government's clampdown on Internet access and activities. When the World Wide Web emerged in the mid-1990s, the Russian government initially did not try to prevent Russian citizens from having unhindered access to the Internet. After Vladimir Putin became president of Russia nearly fifteen years ago and began methodically re-imposing state control over all national television, the Internet became the medium of choice for urban, highly-educated Russians. Although regular Internet use was low in Russia until around 2008, the rate of daily use has grown very sharply since then. State-controlled national television remains the dominant source of news for the vast majority of Russians (roughly 85-95 percent, according to the Levada Center's periodic surveys), but the Internet is now a crucial source of information about politics for a small but influential segment of intellectuals and elites.

That is why the recent moves to assert much greater control over Russians' use of the Internet are so disturbing. In China, the government has long maintained a "firewall" (a dense set of blocking and filtering technologies and legal regimes) that prevents Internet service providers (ISPs) in China from giving access to a great deal of content, including all content related to particular topics as well as whole categories of websites. In North Korea, the regime has gone much further, banning all access to the Internet. The approach used in Russia until recently had been less heavy-handed. In 1998 the Federal Security Service (FSB) gained legal authority to compel ISPs in Russia to turn over all information and records concerning specific users and to permit the FSB to monitor those users' online activities. Although a Constitutional Court ruling in 2000 stipulated that ISPs did not have to turn over information about users unless the police displayed a valid warrant, the reality is that providers in Russia have come under heavy pressure to furnish detailed information to the FSB regardless of whether a warrant has been obtained.

The FSB's Internet surveillance powers, carried out via the System for Operational-Investigative Measures (Sistema operativno-rozyskikh meropriyatii, or SORM), were sufficient at the time to keep track of individual opposition activists and groups, but as the number of users in Russia rapidly multiplied in the late 2000s and Internet technology rapidly evolved (including the emergence and huge popularity of social network sites), the FSB pushed for a major expansion of its control techniques and regulations. The Russian government readily complied. A series of laws adopted in 2012, 2013, and 2014 established a wide-ranging legal framework to accomplish several goals:

1) block access to selected websites, including those linked with political opposition, human rights, and election monitoring;
2) set burdensome requirements for opposition bloggers and make it prohibitively difficult for them to function properly; and
3) compel certain content providers, particularly foreign companies responsible for social network sites (SNS), to store all personal data about Russians on servers located on Russian territory.

Compliance with the last regulation, which takes effect in September 2016 (well before Putin will be seeking reelection in March 2018), will require foreign SNS operators to establish separate servers in Russia, where any information they store about Russians will potentially be subject to FSB monitoring.

The impetus for the crackdown dates back to 2011, a year that witnessed mass unrest in the Arab world and the outbreak of protests in Russia after widespread fraud marred the country's December 2011 parliamentary elections. The role of SNS in the protests in both the Arab world and Moscow was probably much less important than some observers initially argued, but the key thing is what the Russian authorities believed. Putin and his aides concluded that "hostile" SNS, abetted and instigated by the West, were creating subversive networks committed to the overthrow of authoritarian regimes, including Putin's. In the wake of the unrest, Russian officials began using bilateral meetings and regional forums such as the Collective Security Treaty Organization and the Shanghai Cooperation Organization to promote coordinated efforts against "Western-inspired color revolutions." The prospect of renewed mass unrest in Russia, which the authorities want to avoid at all costs, has been the major force shaping Putin's policies over the past two years both at home and abroad. The recent clampdown on Internet activities has to be understood in that light.

The Legal Thicket

In July 2012, two months after Putin returned as president, the Russian parliament adopted Federal Law 139FZ, which took effect in November 2012. Under the law, the Federal Service for Oversight in the Sphere of Mass Media and Communications

(Roskomnadzor) is responsible for compiling a "unified registry" of prohibited websites, to which all ISPs in Russia must block access. The unified registry, known informally as the "black list," is provided to all ISPs but is not made publicly available. Ostensibly, the 'black list" pertains to websites that promote child pornography, illegal drug use, or suicide, but notifications to opposition-oriented websites over the past two years make clear that Roskomnadzor is also targeting outlets that are critical of the Putin regime.

This law, together with "anti-extremism" legislation adopted in 2012 and 2013 (which provides for the compilation of a Federal List of Extremist Materials), has been invoked against websites featuring such disparate content as Pussy Riot videos, Jehovah's Witnesses texts, exposés of corruption in the Russian Orthodox Church, and reports about high-level corruption and police abuse. The same laws were invoked in March 2014 to shut down nearly a dozen opposition websites such as Alexei Navalny's blog, Ekho Moskvy, Ezhednevnyi Zhurnal, Kasparov.ru, and Grani.ru shortly before a "referendum" was staged in Crimea on March 16, 2014, a ban that has remained partly in effect. Other websites, especially those associated with human rights and freedom of expression, were blocked after mass unrest began in Ukraine in November 2013.

In March 2014, the same month the opposition websites were blocked, the Russian authorities also moved to rein in Lenta.ru, the largest and most popular independent news website in Russia. Russian officials pressured the website owner to dismiss the highly respected editor-in-chief, Galina Timchenko, who had worked at Lenta.ru from the time it was founded in 1999. She was replaced by Aleksei Goreslavskii, who had previously been in charge of pro-Kremlin websites and propaganda outlets, prompting most of the staff of Lenta.ru to quit in protest. The ostensible reason for Timchenko's firing was that she had violated "anti-extremism" guidelines when she published an interview with Dmytro Yarosh, the leader of the radical right-wing Ukrainian group Right Sector, but the move in fact was a fairly obvious effort by the regime to curtail the independence of Lenta.ru and to deter other independent news websites (e.g., Slon.ru) from acting too boldly.

The next month, the government also sought to establish stricter control over VK (formerly known as VKontakte), the most popular SNS in Russia. The founder of VK, Pavel Durov, was forced to resign, and the management of the company was placed fully under the control of wealthy executives who are staunchly loyal to Putin. Durov had tried to resist turning over information about VK users to the authorities, whereas the new management has made clear that VK will now comply with all federal requirements. Although VK has not yet been entirely neutered, it can no longer serve as a forum for freewheeling commentary and plans for collective action.

In May 2014, after the reining in of VK, the Russian parliament adopted a law to curb the activities of Russian bloggers. The law, which took effect in July 2014, requires all online writers whose blogs attract more than 3,000 readers to register with Roskomnadzor and to disclose sensitive personal information, rather than remain anonymous under a nom de plume. The same law requires bloggers to comply with the obligations of mass media outlets, including ensuring the accuracy of everything that appears in their postings, and requires service providers, including SNS sites, to store information about readers in Russia and to make the information available to the FSB when presented with a search warrant (though presumably the warrant requirement will fall by the wayside). The legislation is so burdensome and affects such a large swath of the blogosphere in Russia that it was never intended to be enforced comprehensively. Instead, it has been adopted for the selective prosecution of critics of Putin or the FSB or other agencies as well as anyone who falls afoul of authorities at the local or regional level. The impact of the legislation has been strengthened by another law adopted in June 2014, which calls for up to five years in prison for anyone online who spreads "extremist" sentiment or instigates "mass rioting." The legislation is phrased so broadly that it would include such things as re-postings on VK or Facebook and re-tweets on Twitter, thus criminalizing behaviors that are a routine part of online forums.

The latest blow to Internet activities in Russia came in July 2014, when the Russian parliament adopted amendments to earlier anti-terrorism legislation in order to rein in SNS operators based outside Russia. The amendments, long urged by the FSB, require all Internet companies that store data about Russian citizens to keep the data only on servers based in the Russian Federation. Popular SNS operators abroad, such as Facebook and Twitter, as well as many other content providers that want to continue to have Russian customers will be required to build servers on Russian territory at their own expense. Any information about Russian users of the services must be stored on the new servers, which come within the purview of SORM and other legal restrictions on ISPs. If companies decline to establish separate servers, their services can be blocked.

The data-retention legislation, adopted amid some of the worst East-West tension in 30 years, has caused uncertainty and apprehension among Internet users in Russia and foreign SNS operators, who are awaiting clarification of what exactly they will have to do. Even if the requirements are eased somewhat or the law is enforced haphazardly, the combined impact of the legislation adopted over the past two years has dealt a major blow to the use of the Internet in Russia.

Implications for Western Policy

In keeping with the broad authoritarian backlash after Putin returned to the presidency in 2012, the age of Internet freedom in Russia now appears to be over. There is relatively little that Western governments can do to try to ameliorate the situation in the near term, but Western Internet companies and bloggers can and should help their Russian counterparts to remain a vibrant part of the online community. The establishment of mirror sites and systematic repostings will not be a foolproof way of evading some of the new restrictions, but it will certainly magnify the FSB's task of enforcement.

One important issue to consider is how much the Russian public cares about the crackdown on Internet use. Thus far, the outcry in Russia has been limited almost entirely to journalists, pro-democracy activists, and opposition figures like Navalny, Andrei Soldatov, Masha Lipman, and Tanya Lokshina. Opinion polls suggest that among the broader Russian public, the new restrictions have encountered surprisingly little resistance. (Some polls show close to 65 percent supportive of the "black list" and other controls.) Potentially, public attitudes toward the growing censorship will become more negative if popular websites continue to come under official pressure, but, at least for now, the situation is not as remediable as one might hope.

One thing Western governments must avoid doing is creating the impression that free access to the Internet is strictly a "Western value" that can safely be rejected by the officially-sponsored xenophobic campaign in Russia. In promoting free access to the Internet, Western officials, scholars, and Internet companies should work with Russians (to the extent possible) and emphasize how much Russian programmers and scientists have contributed to the online community. A few Russian legislators and advisers to Putin have spoken, rather fancifully, about trying to create a separate "mini-Internet" for Russia that will be directly under the Russian federal government's control, but such ideas are likely to die of their own impracticality. By making clear that Russia has been, and should remain, a vigorous part of the online world, Western officials, universities, and Internet companies can best help those in Russia who are trying to preserve at least a modicum of free speech and free information.

PONARS EURASIA
NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Elliott School of International Affairs
THE GEORGE WASHINGTON UNIVERSITY

© PONARS Eurasia 2014. The statements made and views expressed are solely the responsibility of the author. PONARS Eurasia is an international network of academics that advances new policy approaches to research and security in Russia and Eurasia. PONARS Eurasia is based at the Institute for European, Russian and Eurasian Studies (IERES) at the George Washington University's Elliott School of International Affairs. This publication was made possible by grants from Carnegie Corporation of New York and the John D. and Catherine T. MacArthur Foundation. www.ponarseurasia.org