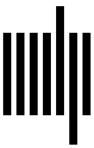
Access Controlled

The Shaping of Power, Rights, and Rule in Cyberspace

Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain

Citation:

Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace
Edited by: Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan L. Zittrain
DOI: 10.7551/mitpress/8551.001.0001
ISBN (electronic): 9780262266031
Publisher: The MIT Press
Published: 2010



The MIT Press

Russia

The absence of overt state-mandated Internet filtering in Russia has led some observers to conclude that the Russian Internet represents an open and uncontested space. In fact, the opposite is true. The Russian government actively competes in Russian cyberspace employing second- and third-generation strategies as a means to shape the national information space and promote pro-government political messages and strategies. This approach is consistent with the government's strategic view of cyberspace that is articulated in strategies such as the doctrine of information security. The DoS attacks against Estonia (May 2007) and Georgia (August 2008) may be an indication of the government's active interest in mobilizing and shaping activities in Russian cyberspace.

Background

Under Vladimir Putin, the federal government of the Russian Federation (RF) has consolidated its power, stripping regional government representatives of some of their

RESULTS AT A GLANCE

Filtering	No Evidence of Filtering	Suspected Filtering	Selective Filtering	Substantial Filtering	Pervasive Filtering
Political			•		
Social			•		
Conflict and security	•				
Internet tools	•				

Other Factors	Low	Medium	High	Not Applicable
Transparency	•			
Consistency	•			

KEY INDICATORS	
GDP per capita, PPP (constant 2005 international dollars)	13,873
Life expectancy at birth (years)	68
Literacy rate (percent of people age 15+)	100
Human development index (out of 179)	73
Rule of law (out of 211)	175
Voice and accountability (out of 209)	166
Democracy index (out of 167)	107 (Hybrid regime)
Digital opportunity index (out of 181)	51
Internet users (percent of population)	27

Source by indicator: World Bank 2009a, World Bank 2009a, World Bank 2009a, UNDP 2008, World Bank 2009b, World Bank 2009b, Economist Intelligence Unit 2008, ITU 2007, Miniwatts Marketing Group 2009.

authority.[1] Putin abolished the principle of electing regional heads by regional parliaments and channeled a number of legal and institutional reforms that demonstrate a gradual tendency to reintroduce a more centralized form of governance over its subjects. These shifts have been felt in all sectors of public life.

Putin's administration after eight years in power brought Russia back to the international scene as a strong global player, and this success has inspired a wave of nationalism fueled by government policies. Putin enjoyed high approval ratings in Russia up to 87 percent (July 2006)[2] largely because of the improved economic indicators of the country. The economy has performed well under his watch, especially in comparison to the period between 1991 and 1999. It has been growing steadily, bolstered by high global energy prices. The growing popularity for Putin, however, was coupled with a significant drop in political rights and civil liberties.[3] Putin's administration effectively silenced the opposition, cracked down on antigovernment protests, reimposed control over the media, and concentrated power in the presidency. The policy line introduced by Putin remains largely unchallenged during the first year of Dmitri Medvedev's presidency. Putin and his supporters refer to the current system of governance in Russia as ''sovereign democracy.'' International observers disagree, describing the established system of government as an increasingly authoritarian state, albeit one that is supported ''with the consent of the governed.''[4]

As President, Putin strengthened state control over major outlets, focusing especially on media owned at the time by Russian oligarchs. As a sanction for unpaid debts, Putin took away owners' shares in television channels and placed the media under state control. This action sharply influenced the flow of information and the management of the outlets. Major federal television channels are either directly or indirectly controlled by the government, with the sole exception of RenTV, which openly criticizes the government but, ironically, is owned by a Kremlin supporter, Vladimir Potanin.[5] Print me-

dia are the least controlled part of the Russian media, but their influence may not be as strong as that of other media. The control on the media tightened particularly during and after the 2004 ''Beslan Crisis,'' in which 1,100 students were taken hostage in Beslan in the North Caucasus by terrorists demanding an end to the second Chechen war.[6]

The Russian government has deliberately created mechanisms to centralize power in the Kremlin and influence major information outlets. This policy has been expanded to reach the Internet through a range of approaches from censorship to propaganda, resulting in self-censorship.

Although Putin admittedly has never sent an e-mail in his life,[7] his administration has been increasingly interested in regulating the Internet. Under Medvedev's presidency (since May 2008), Putin, now as the prime minister, continues to have significant influence over the internal and foreign politics of the state.

Dmitri Medvedev has demonstrated familiarity with Internet communications. During the election campaign, he addressed questions about the Russian blogosphere, promising clement conditions for its development. In October 2008, Medvedev launched his own video blog.[8] However, no significant changes have been introduced to promote media freedom and freedom of expression in Russia. Nonetheless, Russian media have surmised that Medvedev's involvement has led to the removal of the restrictions on foreign participation in ISPs, which were envisioned in the Draft Bill for Amendments to the Law ''On the Order of Foreign Investment in Companies and Organizations Having Strategic Importance for National Security.''

Internet Infrastructure

Internet use grew in Russia in the 1990s with a regime unprepared to deal with new information and communication technology (ICT) challenges. The post-Soviet government seemed to prefer to have strong control over the Internet, similar to the way it already controlled traditional media, but left it alone for lack of viable approaches. Internet penetration in Russia was low during this period, and access was difficult, factors that may explain why the Internet was not a major government concern.[9]

With the election of President Putin came a new focus on regulating the Internet. He issued the Information Security Doctrine in 2000, which outlined Russia's desire to encourage development of the information space amid growing security concerns. This document regulates traditional media but also indirectly positions the Internet at the core of national security policies.[10] Within a few years, the majority of other CIS countries adopted laws similar to Russia's Information Doctrine.

As of December 2008, the number of Internet users in Russia had reached 38 million.[11] Internet penetration is growing notably, though it remains predominantly two-tiered, with much higher Internet and PC penetration rates in Moscow and

St. Petersburg than in the rest of the country. The ''e-readiness'' standing of Russia as measured by the Economist Intelligence Unit[12] is 59th out of 70 countries surveyed in 2008.[13] The Ministry of Education and Science has initiated national programs for providing Internet access to all general educational institutions in the country.[14] Fifty thousand schools were connected to the Internet by the end of 2007.[15] Moreover, the government has announced its plans to install open-source software on every school computer by 2009.

The majority of Russian Internet users are connected by broadband (40 percent), followed by dial-up (27 percent), and ADSL (23 percent). Seven million PCs were sold in Russia in 2006, of which 1.9 million were laptops, representing a 62 percent annual increase from the year before.[16]

A significant portion of the telecom market has remained under state control. Telecommunication Investment Joint Stock Company SvyazInvest is one of the largest telecommunications holding companies in the world. It was created during the market transition by a regulation providing for the merger of a majority of the regional state telecommunications enterprises.[17] About 89 percent of the Russian telecommunications infrastructure now belongs to SvyazInvest,[18] with the remaining 11 percent divided among several other operators.[19] The main shareholder of SvyazInvest is the Russian government through the Federal Property Agency (75 percent minus 1 share), and Comstar-UTS owns 17.31 percent plus 1 share. Some of the main regional ISPs are SvyazInvest's subsidiaries: Central Telecommunication Company, North-West Telecom, VolgaTelecom, Southern Telecom, Uralsvyazinform, Sibirtelecom, Dalsvyaz, and Central Telegraph.[20]

Rostelecom is another large telecommunications operator and ISP. Despite strong international pressure for privatization, SvyazInvest continues to hold 51 percent of Rostelecom shares. Historically, Rostelecom has been the primary long-distance and international telephone operator, collecting mandatory intermediary fees from other providers. Before the adoption of the new regulatory framework on communications, Rostelecom had a monopoly over the provision of international long-distance services. Under the new regime, providers of long-distance services may offer their services directly to users without paying intermediary charges, provided certain prerequisites apply. These include that the providers ''are in technical conformity with the local and long-distance network operators, with a point of presence in every Russian administrative region, and are operationally ready to provide long-distance services to any local network subscriber.''

Russia has more than a dozen main first-tier ISPs, which have independent connections to foreign networks, and several other influential ISPs. First-tier ISPs in the Russian Federation are Rostelecom,[21] GoldenTelecom,[22] TransTeleCom,[23] Makomnet,[24] TeliaSonera,[25] Comstar-Direct (previously MTU-Intel),[26] Metrocom,[27] Corbina,[28] ER-Telecom, CentrTelecom,[29] RTComm,[30] RETN.net,[31] and RiNet.[32] The major ISPs in

Russia either are state owned or include significant state participation. State participation is either direct or through a state-controlled entity.

There are hundreds of ISPs throughout the country functioning on a divided market of well-connected big cities and underdeveloped infrastructure in towns and villages. The established fixed-line providers have been traditionally the largest ISPs, though many small ISPs have started to emerge. Under a regulation that entered into force at the beginning of 2006, all companies that control more than 25 percent of the capacity of communication traffic need to publish a list of prices for interconnection and data transmission within 20 days for the inspection and approval of the regulatory agency.[33]

There are several Internet exchange points (IXP) in Russia. The main ones are Moscow IX,[34] independent, comprising various locations in Moscow;[35] SPB-IX in St. Petersburg, jointly with the MSK-IX; SAMARA-IX in Samara; NSK-IX in Novosibirsk; and KRS-IX in Krasnoyarsk. Other IXPs are the North-West Internet Exchange based in St. Petersburg and Ural-IX in Ekaterinburg and Perm.

The cable television market and broadband Internet access market significantly increased penetration to around 40 percent in 2007.[36] Broadband connections are growing as operators invest in modernized networks. However, broadband is emerging mainly in large urban areas (ADSL, cable, and FttH/FttB-based services). A large portion of residential areas use Ethernet local area networks (LANs), followed by dial-up (27 percent), and ADSL (23 percent). Wireless broadband networks have become popular mainly in large tourist cities, especially St. Petersburg and Moscow, and some operators have announced plans to launch Wi-Fi coverage on a large scale. Also, IPTV services have been launched.[37]

In remote regions, satellite connection is very attractive to the Russian population, in comparison to fixed-line charges. Two main educational networks in Russia (Radio-MSU and the university network RUNET) are supported by satellite.

There are about 250 mobile operators on the Russian market. The mobile market represents about 40 percent of telecom revenue. As of September 2006, the market was divided as follows: MTS, 34 percent; Vimpelcom, 32 percent; Megafon, 19 percent; and others, 15 percent. According to studies, some 40 percent of the population does not have a mobile phone. Russia's three biggest operators were issued 3G licenses in 2007.

The importance of the blogosphere to Russians is increasing rapidly. The Russian-language part of the Internet, or the RUNET, is an active and vibrant environment. As a Russian-language platform, the RUNET has grown as the center of modern culture connecting Internet users from Russia and the rest of the CIS region, and ethnic Russians in Germany, Israel, and the United States. It brings together people sharing the same language and similar history and culture, and is a self-sufficient online environment with its own search engines, Web portals, free e-mail services, and social network

Web sites (most of them modeled after U.S. services). The most popular blog servers are LiveJournal.com and LiveInternet.ru. The Russian site of LiveJournal has more than 2 million[38] registered users, while the site's readership amounts to nearly 10 million people, according to Anton Nossik, one of the RUNET pioneers.[39]

The Russian blogosphere operates within an environment where the state directly competes with other actors for influence. During election times, the Kremlin maintains a network of supportive bloggers and online media experts, similar to China's so-called *fifty cent party*. This squadron of Kremlin bloggers has engaged in public discussions, trying to keep the level of political criticism low, to nurture nationalism, and to flood the Russian blogosphere with blogs that favor the regime during times of oppositional protests.[40] Instead of giving publicity to its efforts to control the Internet through direct censorship, the government has turned to these soft approaches to combat undesired content.

Recently, the Russian government has implemented an unprecedented, and so far surprisingly effective, initiative to engage with political dissent in order to weaken it. A number of pro-Kremlin blogs have been created; in number, they overshadow blogs not favoring the regime, and they were especially prevalent toward the end of 2007, when national political campaigns were under way for parliamentary and presidential elections. This strategy could also be intended to drown out the voices of opposition blogs.

Effective strategic blogging has been seen to have an impact. In April 2007, for example, an opposition movement held a march in Moscow. To interfere with the information about the march, blogger Pavel Danilin, a Putin supporter, together with his team, started blogging about a smaller pro-Kremlin march being held the same day. European Digital Rights noted, ''they blogged so much and linked to each other so effectively, that they crowded out all the items about the opposition march from the very influential top-five blog post listing on the Yandex Web portal.''[41] A consistent and motivated group of supporters is likely to channel the Kremlin's message to large online communities. According to Masha Lipman, a political expert at the Moscow Carnegie Center, ''The Kremlin has lots of sites under its control, financed by businesses associated with the Kremlin or otherwise, which create an environment in which those more independent ones are easily dissolved. This [dissolution of independent sites] . . . is one thing that the Kremlin is using to counter or neutralize the potentially stirring effect.''[42] The blogs are not based on simple propaganda, and some of the bloggers are not even necessarily loyal; ''they may be critical themselves, but this will be criticism that the Kremlin itself sort of oversees.''[43]

Legal and Regulatory Frameworks

The Constitution of the Russian Federation guarantees free speech and prohibits any restraint on the freedom of expression (Article 29). The constitution recognizes the

rights to privacy and data protection, the right to information, and secrecy of communications (Articles 23, 24, and 25).

The Law on Communications of 2003[44] further protects the secrecy of communications and guarantees that restrictions on individual privacy are allowed only after a court order, unless otherwise envisioned by federal law.[45] To meet its obligations as a member of the Council of Europe, Russia adopted the Law on Personal Data in 2006.[46] Although the law guarantees the privacy of the individual, it provides for broad exemptions to the government in processing personal data. Also in 2006, Russia modified its information law, adopting the new Law on Information, Information Technologies, and Protection of Information.[47] The new laws, together with the Labor Law, establish a legal framework for handling personal data, including employee data. Russian experts claim that even though the new law on information guarantees citizens' access to public information held by federal or regional authorities, not more than 23.6 percent of the relevant information is publicly available.[48]

A presidential decree titled ''Measures Providing Information Security to the Russian Federation in the Information Exchange Area,'' signed in May 2004, restricts the access of officials' computers to the Internet.[49] The decree prevents computers and communication networks from connecting to the Internet if they hold (have on their servers) state and official secrets, as well as other classified information.

The Internet in Russia is largely seen as an extension of media space. The mass media regime carries certain responsibilities, such as registration, necessary attestation, and others. The Internet escaped regulation in the Law on Mass Media, No.2124-1,[50] as the Law entered into force in 1991. However, it is held that the Internet should be regulated under this law anyway. Article 2 of the law states that it shall cover ''other forms of periodic distribution of mass information'' as purported by officials.[51] This interpretation has given grounds for detaining and prosecuting Web site owners and bloggers by authorities on the grounds of violation of media laws. Officials view Internet proliferation as increasing the government's responsibility for regulating the Internet space and ensuring that users act in accordance with legal and ethical norms of society. In at least one instance, the court included an online forum in the definition of mass media, setting a precedent for prosecution under mass media provisions.

On several occasions, the authorities have expressed interest in subjecting content on the Internet, specifically online media, to media law. Federation Council member Vladimir Slutsker initiated amendments to the Law on Mass Media: one of the amendments provides that Web sites visited more than 1,000 times a day should be subjected to registration as mass media outlets.[52] However, it was deemed impossible to find all applicable sites and force Web site owners to register. For this reason, unofficially, it was agreed that the Web sites would register only voluntarily as mass media.[53]

According to its supporters, the envisioned proposal would give official recognition to the registered Web sites and would be important for controlling child pornography and defamatory materials, and even for providing information about terrorist and

extremist organizations. There are incentives for Web sites to register as mass media outlets, including an official stamp of legitimacy and permission to attend press conferences, request information from authorities, and be present at sites of emergencies or mass protests. Another push for registration came in 2004 when the head of the Federal Agency for Print and Mass Communications, Michail Seslavinski, called for ''important'' Web sites to register as mass media.[54] In 2004, there were 1,296 registered Web sites, a figure which had increased to nearly 20,000 registered Web sites by 2009.[55]

There have been several proposals to introduce ISP liability for content found on their servers.[56] In March 2008, a new initiative was suggested by the Russian prosecutor general's office to hold ISPs jointly liable with extremists for extremist content posted online.[57] However, currently no draft law is known to have been proposed.

The ICT sector does not have an independent regulatory authority. Until 2007, the regulation of the sector was managed by the Ministry of Communications and Informatization through RosSvyazNadzor (the Federal Service on the Supervision of Communications), which reported directly to it. After the Russian Television and Radio Broadcasting Network (RTDN) lodged complaints in court against RosSvyazNadzor that the control it was exercising exceeded the limits provided by law, the agencies were reorganized. RosSvyazNadzor merged with another regulatory agency, the Federal Service on the Supervision of the Mass Media and the Protection of Cultural Inheritance. In addition to current responsibilities, the newly formed agency will also be responsible for protecting personal data and monitoring the processing of such data.

The Federal Law on Communications of 2003 provides a simplified licensing regime for ISPs. In order to conduct business in Russia, operators need to obtain two licenses: one for data transfer and another for ''telematic'' (data transmission and storage) services. In 2005, the Ministry of Communications introduced a licensing regime for VoIP services. Any VoIP service must be processed through a licensed long-distance telephone operator.

Libel incurred through the media is a crime regulated by the Criminal Code. It is also addressed in the Law on Mass Media. Articles 43 through 45 of the law describe the circumstances for publishing a refutation in libel suits when the information spread through the mass medium does not correspond to reality and denigrates honor and dignity.[58] Registered Web sites and producers of online content can be liable for defamation for published information under the Criminal Code and in the Law on Mass Media. In at least one instance, the court included an online forum in the definition of mass media, setting a precedent for prosecution under mass media provisions.[59]

In December 2007, the Russian Supreme (Arbitrazh) Court upheld the seizure of media archives. According to the Internet outlet Regnum.ru, the court did not apply Article 57, which provides a media libel exception for published information.[60] This precedent establishes that Internet outlets do not receive the protection of the law,

since they are not treated as mass media outlets, thus leaving the door open to any potential defamatory claims.

At present, the Criminal Code includes numerous provisions that may be grounds for criminal charges in connection with Internet activities. Article 278, for example, criminalizes ''forced assumption of and retention of authority.'' The Criminal Code provides for government officials to prosecute individuals for posting objectionable content online. The text against terrorist activities in Article 282, in the section ''Crimes against the Government,'' can be applied to online activities. The text states, ''incitement of national, racial, or religious enmity, abasement of human dignity, and also propaganda of the exceptionality, superiority, or inferiority of individuals by reason of their attitude to religion, national, or racial affiliation, if these acts have been committed in public or with the use of mass media'' are punishable by fines equaling up to two years of salary and up to two years imprisonment. This broad language leaves space for open interpretation of the statute, as it can apply to anything ranging from commentary on the infamous Danish cartoons,[61] to racial slurs and hate speech. Insulting a government official is an aggravated crime covered in Article 319, which may bring a fine of up to one month of salary or corrective labor of up to one year.[62]

The government and private individuals can and do attempt to find broad interpretations of the laws in order to silence independent Web sites. For example, the content provider Bankfax was charged under Article 282 with insulting a group of people by referring to them as ''oligarchs.''

The government has adopted the Law against Extremist Activities.[63] Under this law, effectively any Web site hosting a forum section is vulnerable. An individual needs only to post hate or extremist (or other objectionable) speech in a forum and report it to the authorities before a moderator notices it to kick off legal prosecution. Violations are not uniformly prosecuted—most reported content does not lead to penalties, making the Internet a source of information that is not found in print media. If such speech is detected, however, owners risk closure of their Web sites or fines.[64]

Censorship has not been legally introduced in the country, though informally it has been applied as a tool for use during a national crisis. Internet censorship has occurred or been discussed in several other ways—for example, interference with the work of oppositional and independent Web sites and restrictions imposed by a court.

Russia's government officials are sensitive to offensive speech posted online. The Criminal Code and the Law against Extremist Activities establish individual liability for a broad range of ''illegal'' content. A special enforcement agency, Department ''K,'' was established within the Ministry of Internal Affairs to monitor for compliance with the regulations in cyberspace. Department ''K'' has branches in various regions and is mandated to investigate crimes in the sphere of information technologies, including online hate speech and defamation. Aside from monitoring for possible defamation of

officials online, the ''cyber police'' deal with unauthorized access to computer systems and networks, and the distribution of pirated software.

An example of the activities of this cyber police department was the September 2007 case involving the sports site hc-rodina.ru.[65] The ISP of the sports Web site stopped maintaining service following an order from Department ''K.'' The reasons for this censorship were ''inaccurate'' comments about representatives of the government posted on the Web site's forum section. In another example, a blogger was sentenced to a year in jail for posting a caricature of Putin depicted as a skinhead.[66]

On several occasions, Russian politicians have proposed establishing a legal framework that would directly control the Internet. At the end of January 2007, the Federation Council Commission on Information Policy discussed the possibility of introducing a law regulating the Internet in order to establish a ''safe'' online environment to protect people against the growing cases of illegal activities.[67]

In July 2007, Putin spoke of making Russia ''a global information technology powerhouse.'' Following his statement, the Kremlin announced plans to create a Cyrillic Web for Russia and the rest of the CIS and Bulgaria. The Russian Federation is the only country other than China that has decisively announced plans to launch a self-contained and independent language Web parallel to the World Wide Web. At the end of June 2008, ICANN spoke in favor of proposals to establish Cyrillic and Chinese language-based domains. Although this idea moves toward further development of the Internet, there are shared fears that this step might also lead to the division of the Internet and facilitate state censorship through the registration and management process. If the administration of Russian Web sites is concentrated in the hands of a government agency, it could have chilling effects on independent-minded online media and bloggers.

In the past few years, Russia's government has recognized the need to develop a favorable environment for information technology by providing legal and tax incentives for companies in this market. The development of the ICT sector has risen to become a national policy priority. Yet, while the government is hoping to attract foreign investment, it is not ready to abandon centralized decision making and end its monitoring of ISPs.

Surveillance

The Russian government has been advancing justifications for surveillance, ostensibly to aid in the investigation of crimes and the prevention of terrorism. The Law on Systems for Operational Investigation Activity (SORM)[68] of 1995 authorized the FSB monitoring of telecommunication transmission. In 1999, formulated as an amendment to SORM, SORM-II was enacted to allow for the monitoring of Internet traffic. SORM-II is still effective and ''reinforced,'' and in April 2008, Leonid Reiman, the Min-

ister of Communications, signed an order that essentially restated the obligations of ISPs under SORM-II to allow monitoring of users' Internet activities.

Under SORM-II, ISPs are required to provide the FSB with statistics on all Internet traffic that passes through their servers. In addition, ISPs are required to install monitoring devices on their servers and route all transmissions in real time through the FSB's local offices, which would allow the FSB to track all users' transactions, e-mail communications, and online browsing. Even though the FSB still needs to obtain a warrant to read the contents, many doubt that they would obtain the warrant beforehand consistently, since there is no mechanism to prevent the FSB from having unauthorized access. Providers must also provide the FSB with information on users' names, telephone numbers, e-mail addresses, one or more IP addresses, key words, user identification numbers, and users' ICQ number (instant messaging client), among others.

Under Putin, Minister of Communications Reiman entered an order stating that the FSB officials shall not provide information to the ISPs either on users who are being investigated or regarding the decision on the grounds of which such investigations are made.[69] Consequently, this Order offered a ''carte blanche'' to the Special Services to police the activities of Internet users without supplying any further information to the provider or any other interested party.

Only a few days after assuming office, President Putin expanded the list of state agencies that can monitor communications under SORM to include the tax police, Ministry of Internal Affairs, Border Guards, Kremlin Security Service, Presidential Security Service, parliamentary security services, and Foreign Intelligence Service.

SORM places the substantial financial burden of installing routers on the FSB servers on the balance sheets of ISPs, with minimal benefit to them for the technology. The cost of equipment at the time the regulation was adopted was close to USD 25,000.[70] This expense has caused many small and independent ISPs to shut down. In one recorded case a small regional ISP in Volgograd, Bayard-Slaviya Communications, resisted the new law and refused to install the required equipment. As a result, the Ministry of Communications suspended the provider's license. However, when the ISP brought the question to court, the ministry renewed its license.

SORM-II drastically expanded the ability of the FSB to carry out surveillance of operators and individuals. Some reports reveal that ISP owners prefer to negotiate their own confidential agreements with the FSB office rather than take on the cost of complying with SORM-II or risk losing their licenses.[71]

In reality, however, many doubt that the FSB possesses the capability of monitoring all Internet traffic.[72] Increased Internet traffic renders ubiquitous surveillance practically impossible. Unless the authorities know ahead of time what they are searching for, random surveillance is unlikely to produce any meaningful results.[73] Nevertheless, as there is no independent authority that controls or supervises the FSB, their activities are not publicly known.

ONI Testing Results

The OpenNet Initiative tested from different locations and several access points on a number of main ISPs in the major cities and regions. The ONI tested on the following ISPs: AltaiTelecom, ASN-Yartelecom, Comstar, Corvette, Metrocom, North-West Telecom (ASN SPBNIT), Rosnet, RiNet, St. Petersburg State University (ASN-SPBGU), and Wiland. The ONI found first-generation filtering that targeted erotic and pornographic content. Second-generation filtering methods were largely undetected by the ONI, as they occur only during significant political events. The ONI did not monitor the 2007 parliamentary or 2008 presidential elections, during which numerous instances of second-generation and third-generation controls were reported in the Russian and foreign press.

Conclusion

Control of media has a long-established history in Russia. As the Internet has proliferated, the government has moved to design suitable control mechanisms. Compared to other countries, the Russian approach represents a notably different method of controlling Internet activity. Instead of utilizing Chinese-style filtering to control Internet access, the Russian government prefers to employ second- and third-generation techniques such as legal and technical instruments and national information campaigns to shape the information environment and stifle dissent and opposition.

As many countries around the world struggle with Internet regulation, it is likely that this Russian model will be emulated by other governments, in the CIS and beyond.

Notes

1. Helen Womack, ''Russia's Governors Reluctantly Accept Putin Curbs on Power,'' *The Independent*, July 27, 2000, http://www.independent.co.uk/news/world/europe/russias-governors-reluctantly-accept-putin-curbs-on-power-707944.html; Nikolay Petrov and Michael A. McFaul, ''How Much Has Federal Power Increased Under Putin?'' Carnegie Endowment for International Peace, September 8, 2004, http://www.carnegieendowment.org/events/index.cfm?fa=eventDetail&id=747.

2. Centre for the Study of Public Policy (University of Aberdeen) and Levada Center (Moscow), ''Russia Votes,'' January 22, 2009, http://www.russiavotes.org/president/presidency_performance_trends.php#190.

3. Freedom House sets Russia's country status as ''nonfree'' for 2006 and 2007.

4. Clifford J. Levy, ''Is Russia's Economy a Threat to Putin's Power?'' *The Seattle Times*, February 1, 2009, http://seattletimes.nwsource.com/html/nationworld/2008694591_worldweek01.html?syndication=rss.

5. Only one radio station, Echo Mosckvy, is considered independent, but it actually belongs to the state-owned company Gazprom, which itself implies that any criticism of the government broadcast over its networks is ''pre-approved.'' In a recent interview, the editor in chief Alexei Venediktov admitted that ''The Kremlin is our real stockholder.'' See Alexi Venediktov: '''The Kremlin is our real stockholder.''' *Novaya Gazeta*, April 17, 2008, http://en.novayagazeta.ru/data/2008/25/08.html.

6. The federal TV channels did not report the tragedy, and it was only through print media and the Internet that the Russian population obtained information. See Organization for Security and Cooperation in Europe, *Report on Russian Media Coverage of the Beslan Tragedy: Access to Information and Journalists' Working Conditions*, September 16, 2004, http://www.osce.org/documents/rfm/2004/09/3586_en.pdf; Stephen Dalziel, ''Russia 'Impeded Media' in Beslan,'' *BBC News*, September 16, 2004, http://news.bbc.co.uk/1/hi/world/europe/3662124.stm.

7. Adi Ignatius, ''A Tsar is Born,'' *Time*, http://www.time.com/time/specials/2007/personoftheyear/article/0,28804,1690753_1690757_1690766-1,00.html.

8. Weblog of Dmitri Medvedev, President of the Russian Federation, http://blog.kremlin.ru/.

9. For an analysis of the development of the Internet in the Russian Federation in the early and mid-1990s and services provided by the main e-mail provider, please consult Chapter 2 in this volume.

10. Security Council of the Russian Federation, *Information Security Doctrine of the Russian Federation*, 2000, http://www.scrf.gov.ru/documents/5.html.

11. Miniwatts Marketing Group ''Internet World Stats: Russia,'' 2009, http://www.internetworldstats.com/europa2.htm#ru.

12. Economist Intelligence Unit, ''e-Readiness Rankings 2008: Maintaining Momentum,'' http://a330.g.akamai.net/7/330/25828/20080331202303/graphics.eiu.com/upload/ibm_ereadiness_2008.pdf.

13. Political Intelligence and Internews, *Russia*, 2006, http://ec.europa.eu/information_society/activities/internationalrel/docs/pi_study_rus_ukr_arm_azerb_bel_geor_kaz_mold/2_russia.pdf.

14. Russian Ministry of Education, ''Ensure All Russia's Schools Access to the Internet,'' http://mon.gov.ru/pro/pnpo/int/.

15. *C News*, ''Bum: Glava ''Moego Banka'' Stroit WiMax-set'' [BUM: The Head of 'My Bank' Is Building a WiMAX Connection], May 2006, http://www.cnews.ru/news/top/index.shtml?2009/06/05/349841.

16. Paul Budde Communication Pty., Ltd., ''Russia—Internet, Broadband and Convergence Overview and Statistics,'' November 8, 2007.

17. SyvazInvest, ''Investor Relations,'' http://eng.svyazinvest.ru/investor-relations/fdir/.

18. By the end of 2003, the five largest ISPs (54 percent) have been the SvyazInvest interregional companies. RTComm.ru, a branch of Rostelecom and SvyazInvest that took over Rostelecom's wholesale ISP business, has become an undisputed leader with 28 percent market share.

Transtelecom came second with 18 percent, and interregional companies had 17 percent. Golden Telecom and MTU-Intel had 11 and 9 percent, respectively.

19. There are several groups besides SvyazInvest that own large shares of the telecommunications business and to a large extent influence the development of Russia's telecom industry: AFK Sistema, Alfa Group/Altima, and Telecominvest.

20. SyvazInvest, ''Investor Relations,'' http://eng.svyazinvest.ru/investor-relations/fdir/.

21. It is one of the leading operators. The company ''owns and operates a 150,000 km nationwide fiber optic backbone network'' as well as satellite connection. Rostelecom provides services in many regions of Russia but is focused on major cities. It owns a 31.59 percent significant share of RTComm and provides service for second-tier operators. See Rostelecom, ''General Information,'' http://www.rt.ru/en/about/info/ and Rostelecom, ''Rostelecom at a Glance,'' http://www.rostelecom.ru/en/serv-operators/info/.

22. It is the largest of the alternative fixed-line operators and one of the largest ISPs in Russia, offering access in over 60 locations, including Moscow, St. Petersburg, and the CIS region (Kiev, Tashkent, Almaty, etc.). GoldenTelecom is connected to all the mobile and fixed telephony service providers in the Russian Federation. It has many international points of presence including London, Stockholm, New York, Frankfurt, and Hong Kong. In March 2008, VimpelCom (under the trade name Beeline) acquired GoldenTelecom (http://msk.b2b.beeline.ru). The ISP announced further plans to invest USD 1.5 billion in Russia aiming to build a new broadband Internet network serving 65 Russian cities by 2010.

23. TransTeleCom is a backbone telecommunications provider with a 50,000 km network of communication lines stretching through all 11 zones of the country. It connects to the Euro-Asian telecommunication route, going through Western Europe and Asia. The network is based on the communication lines of the Russian railroad systems. TransTeleCom mostly provides service for second-tier ISPs. The operator is owned by the state-run JSC Russian Railways.

24. Makomnet possesses an internationally linked fiber-optic network. In November 2006, it put into operation its fourth international 100 Mbps Moscow-Stockholm cable. The operator provides more than 1 Gbps capacity to Frankfurt (MCI/UUNet), New York (MCI/UUNet), Helsinki, and Stockholm (TeliaSonera). It maintains a total capacity of more than 4 Gbps with leading Russian ISPs via MSK-IX and direct connections. Shareholders include state-owned Moscow Metro and Moseleset. See Macomnet, ''Internet Access,'' http://www.macomnet.com/services/internet and Macomnet, ''4th International Main 100 Mbps Moscow-Stockholm Was Put into Operation,'' November 1, 2006, http://www.macomnet.com/press/news/text?newsid=47.

25. TeliaSonera is an international ISP operating in Russia and connected to the Russian Internet Exchange MSK-IX. It has the largest communication network in Europe and connects Russian networks with European and American operators. See ISP Review, ''TyeliaSonyera Intyernyeshinal Kerriyer Rasha'' [TeliaSonera Russian International Carrier], http://www.ispreview.ru/company1109.html.

26. MTU-Intel was renamed Comstar-Direct in December 2006 after it grew to become one of the largest ISPs in Moscow and the largest broadband ISP in Moscow. It provides a 30 Gbps channel

Moscow-Europe and is connected to more than 200 Western ISPs at a couple of European Internet exchanges. Comstar-Direct is a subsidiary of Comstar, one of the largest telecoms in Russia. For international Internet connection, see http://www.comstar-uts.com/ru/services/internet/. Also see http://www.comstar-direct.ru.

27. Metrocom operates predominantly in the northwest of Russia. It is owned in majority by the city of St. Petersburg and closed joint stock company MST.

28. Corbina is one of the largest Russian ISPs. It has coverage in more than 20 regions, but it operates mostly in the Moscow region. Corbina does not have its own independent network and is connected to foreign networks through TeliaSonera's and GoldenTelecom's lines. The controlling shareholder is GoldenTelecom. See Corbina ISP, http://home.corbina.ru/news/2007/05/29/1653.html.

29. CentrTelecom is one of the largest ISPs operating in the central part of Russia. It currently provides broadband connection, including xDSL, to more than 120,000 users. CentrTelecom is state run, and the majority shareholder is SvyazInvest. European Communications, ''Russian Operator Center Telecom Selects Italtel for Implementation of Broadband and VoIP,'' July 3, 2007, See http://www.eurocomms.com/online_press/111822/Russian_operator_Center_Telecom_selects_Italtel_for_implementation_of_broadband_and_VoIP_.html.

30. RTComm was founded by SvyazInvest and Rostelecom; now it is now part of the Sinterra group, which is part of PromSvyazCapital, a private investment and media holding company. See RTComm, http://www.rtcomm.ru/geo/net/.

31. RETN.net operates a network joining Russian and Western ISPs. It serves over 140 national and foreign companies having some 500 direct connections between the Russian and international ISPs. It has points of presence in New York, London, Amsterdam, Stockholm, Helsinki, and Frankfurt, as well as in Moscow, St. Petersburg, and other Russian cities. RETN.net is connected to Internet exchanges in New York, London, Washington, D.C., Amsterdam, and Moscow. See RETN.net, ''About Company,'' http://www.retn.net/about.

32. RiNet is owned by Sibirtelecom, http://www2.sibirtelecom.ru.

33. Order No. 127 on the Organization of Activities Concerned with the Consideration of Telecommunications Carriers' Requests Concerning the Issues of Telecommunication Networks Interconnection and Interaction issued by the Minister of Information Technologies and Communications on November 10, 2005.

34. Moscow Internet Exchange, http://www.msk-ix.ru/; Russia IP Traffic Exchange, http://www.ripn.net:8080/ix/.

35. Moscow Internet Exchange, http://www.msk-ix.ru/; graphs of traffic at http://www.msk-ix.ru/network/traffic.html.

36. PMR IT & Telecoms in Russia, http://www.ictrussia.com.

37. J'son and Partners, ''Forecast about IPTV Development in Russia (2007–2010),'' *Rumetrika*, June, 16, 2007, http://rumetrika.rambler.ru/publ/article_show.html?article=3221.

38. See http://ru-news.livejournal.com/.

39. Galina Stolyarova, ''Working the Net,'' *Transitions Online*, June 14, 2007, http://www.tol.cz/look/TOL/article.tpl?IdLanguage=1&IdPublication=4&NrIssue=222&NrSection=3&NrArticle=18778.

40. Anna Polyanskaya, Andrei Krivov, and Ivan Lomko, ''Commissars of the Internet: The FSB at the Computer,'' *Vestnik Online*, April 30, 2003, http://www.vestnik.com/issues/2003/0430/win/polyanskaya_krivov_lomko.htm.

41. European Digital Rights, ''Putin wants Control of Russian Internet,'' November 7, 2007, http://www.edri.org/edrigram/number5.21/putin-russia-internet.

42. Global Integrity, ''Russia: Integrity Indicators Scorecard,'' 2007, http://report.globalintegrity.org/Russia/2007/scorecard/7.

43. Ibid.

44. Russia Federal Law on Communication, N 126-FZ, July 7, 2003, http://minkomsvjaz.ru/5878/7687.shtml.

45. The text of the law is at http://www.rg.ru/oficial/doc/federal_zak/126-03.shtm (in Russian). A few amendments were introduced in 2006: http://www.rg.ru/2006/07/27/svyaz.html.

46. Federal Law No. 152-FZ of July 27, 2006. See the text of the law at http://www.rg.ru/printable/2006/07/29/personaljnye-dannye-dok.html (in Russian). The law follows the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and incorporates it into national law. The Russian law provides for the establishment of a data protection authority, which, instead of being independent, is envisioned as an agency within the Ministry of Communications.

47. Federal Law No. 149-FZ of July 27, 2006. See the text of the law at http://www.rg.ru/2006/07/29/informacia-dok.html.

48. Ivan Pavlov, ''Access to Information is Obstructed in Russia,'' Robert Amsterdam Blog, March 29, 2007, http://www.robertamsterdam.com/2007/03/ivan_pavlov_access_to_informat.htm.

49. No. 611 of May 12, 2004.

50. Federal Law on Mass Media No. 2124–1of 1991 with amendments of 1995, 2000, 2001, 2002, 2003, 2004, 2006, 2007. See http://www.rg.ru/1991/12/27/smi-zakon.html (in Russian).

51. Elena Kupriyanova, ''Saity, kak Sredstva Massovoi Informatsii'' [Sites as Means for Mass Information], *smi.ru*, February 12, 2008, http://www.smi.ru/08/02/12/908335250.html.

52. This number was determined based on the legal provision requiring registration for print media with a distribution of 1,000 or more copies per day.

53. *GZT.ru*, ''Klevetnikam Rossii'' [Slanderers of Russia], February 11, 2008, http://gzt.ru/society/2008/02/11/220201.html.

54. GIPP, ''M. Seslavinskyi: 'Serieznyie Rossiiskie Internet Saityi Doljnyi Registrirovat Sebya kak Sredstva Massovoy Informacii','' ['M. Seslavinskyi: 'The Serious Russian Internet Sites Must Regis-

ter Themselves as Mass Media Outlets' ''], September 28, 2004, http://www.gipp.ru/opennews.php?id=3686.

55. As estimated by Rosokhrankultury. See Rosokhrankultury, ''Intyernyet: Svobodniy i byez Ryegistratsii'' [Internet: Free and Without Registration], March 3, 2008, http://www.finmarket.ru/z/nws/hotnews.asp?id=794793. Quoting the increased rate of voluntary registration, Rosokhrankultury (the regulatory federal agency) reasons against the proposed bill because it is not prepared to meet a large number of registrations. Rosokhrankultury, ''Rossvyaz' Ohrankool' toori protiv Ofitsial'noy Ryegistratsii Saytov kak SMI'' [Rosokhrankultury Against the Official Registration Sites as Media], March 12, 2008, http://www.rian.ru/society/20080312/101150561.html.

56. One such proposal was defeated in 2002, but the idea has resurfaced in a set of proposals known as Kroshennikov's amendments to existing laws.

57. *Lenta.ru*, ''Genprokuratura Predlozhila Provaideram Razdelit' Vinu s Ekstremistami'' [Prosecutor's Office Requested Providers to Share the Blame with Extremists], March 17, 2008, http://lenta.ru/news/2008/03/17/provider1/.

58. Law on Mass Media, translation (without amendments) at http://www.medialaw.ru/e_pages/laws/russian/massmedia_eng/massmedia_eng.html.

59. A moderator of Fontanka.ru took down comments threatening migrants in Russia, saved them, and passed them on to authorities. Records traced the posts to an Internet café, where surveillance tapes made it possible to identify the poster. The poster was subsequently charged with threatening murder or infliction of grave injury under Article 119 of the criminal code. The court ruled that forum activity online is part of media activities and sentenced the poster to 18 months in prison.

60. Regnum, sued by a large dairy producer for defamation, claims that the information they used against the claimant was obtained from a regional authority for consumer protection, and thus protection under the Mass Media Law should be applied. The exception under Article 57 states that a mass media outlet should be absolved from liability when disseminating information that ''does not conform to the reality and denigrates the honor and dignity of private citizens and organizations,'' in cases where inter alia the information was received from a public authority. As the court rejected the defense statement, it upheld censorship over the Internet in practice, according to the information outlet. Regnum, ''Nasilstvennyi Zahvat Vlasti ili Nasilstvennoe Uderjanie Vlasti'' [The Supreme Arbitration Court of Russia Instituted Review Proceedings on the Complaint Regnum], http://www.regnum.ru/news/933514.html.

61. A series of cartoons portraying the Prophet Mohammed were published in a Danish newspaper in late 2005. The cartoons were reprinted in several papers in early 2006, sparking riots throughout the Muslim world protesting the visual representation of Mohammed.

62. Article 319, Russian Federation Criminal Code with latest amendments as of 2007, http://www.rg.ru/2007/11/12/ukrf-dok.html (in Russian). English translation without amendments is available at http://www.russian-criminal-code.com.

63. See the text of the law ''O Protivodeystvii Eksstremistskoy Deyatelnosti'' [Law against Extremist Activities], http://www.rg.ru/oficial/doc/federal_zak/114-fz.shtm.

64. Interview with Sergey Smirnov, director, Human Rights Online, in Moscow, Russia (March 29, 2006); interview with Alexey Simonov, president, Glasnost Defense Foundation, in Moscow, Russia (March 27, 2006).

65. *Pingvinov.net*, '' Bespredel v Runete. Kiberpolitseiskie Zakryvaiut Sportivnye Saity'' [Lawlessness in Ru.net, Kiberpolitseyskie Closes Sports Web Sites], http://pingvinov.net/2007/09/25/Bespredel-v-Runete-Kiberpoliceiskie-zakryvajut-sportivnye-saity.html.

66. *CNews*, ''Za Virtualnoe Oskorblenie Putina Dali Realnyi Srok'' [For a Virtual Offence of Putin Was Given a Prison Sentence], November 1, 2008, http://internet.cnews.ru/news/top/index.shtml?2008/11/01/325760.

67. The text of the bill is published on the oppositional site Forum.msk.ru. See http://forum.msk.ru/material/lenty/433019.html.

68. Federal Law No. 144-FZ of August 12, 1995; amended in 1997, 1998, 1999, 2001, 2003, 2004, 2005, 2007.

69. Order No. 130 in July 2000 of the Ministry of Communications; see http://www.lenta.ru/internet/2000/08/21/sorm.

70. Jeanette Borzo, ''Russian ISP Finds Court Victory Sometimes Is No Victory at All,'' *Wall Street Journal Interactive Edition*, http://www.libertarium.ru/libertarium/14424/def_article_t?PRINT_VIEW=YES.

71. Jeanette Borzo, ''Russian ISP Finds Court Victory Sometimes Is No Victory at All,'' *Wall Street Journal Interactive Edition*, http://www.libertarium.ru/libertarium/14424/def_article_t?PRINT_VIEW=YES; Sharon LaFraniere, ''Russian Spies, They've Got Mail,'' *Washington Post*, March 7, 2002, http://www.washingtonpost.com/wp-dyn/articles/A51550-2002Mar6.html.

72. Interview with Andrei Richter, Director, Media Law and Policy Institute, Moscow State University, in Moscow, Russia (March 28, 2006); interview with Alexey Simonov, President, Glasnost Defense Foundation, in Moscow, Russia (March 27, 2006).

73. Rafal Rohozinski, ''How the Internet Did Not Transform Russia,'' *Current History* (2000) 58, 1: 334–338.

For information about special quantity discounts, please email special_sales@mitpress.mit.edu

This book was set in Stone Serif and Stone Sans on 3B2 by Asco Typesetters, Hong Kong.

Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Access controlled : the shaping of power, rights, and rule in cyberspace / edited by Ronald Deibert . . . [et al.] ; foreword by Miklos Haraszti.
p. cm. — (Information revolution and global politics)
Report from the OpenNet Initiative.
Includes bibliographical references and index.
ISBN 978-0-262-01434-2 (hardcover : alk. paper) — ISBN 978-0-262-51435-4 (pbk. : alk. paper)
1. Cyberspace—Government policy. 2. Internet—Government policy. 3. Computers—Access control. 4. Internet—Censorship. I. Deibert, Ronald. II. OpenNet Initiative.
HM851.A254 2010
005.8—dc22 2009049632

10 9 8 7 6 5 4 3 2 1