Internet freedom in Vladimir Putin's Russia: The noose tightens

By Natalie Duffy

January 2015

Key Points

- The Russian government is currently waging a campaign to gain complete control over the country's access to, and activity on, the Internet.
- Putin's measures particularly threaten grassroots antigovernment efforts and even propose a "kill switch" that would allow the government to shut down the Internet in Russia during government-defined disasters, including large-scale civil protests.
- Putin's campaign of oppression, censorship, regulation, and intimidation over online speech threatens the freedom of the Internet around the world.

Despite a long history of censoring traditional media, the Russian government under President Vladimir Putin for many years adopted a relatively liberal, hands-off approach to online speech and the Russian Internet. That began to change in early 2012, after online news sources and social media played a central role in efforts to organize protests following the parliamentary elections in December 2011. In this paper, I will detail the steps taken by the Russian government over the past three years to limit free speech online, prohibit the free flow of data, and undermine freedom of expression and information—the foundational values of the Internet.

The legislation discussed in this paper allows the government to place offending websites on a blacklist, shut down major anti-Kremlin news sites for erroneous violations, require the storage of user data and the monitoring of anonymous online money transfers, place limitations on

bloggers and scan the network for sites containing specific keywords, prohibit the dissemination of material deemed "extremist," require all user information be stored on data servers within Russian borders, restrict the use of public Wi-Fi, and explore the possibility of a kill-switch mechanism that would allow the Russian government to temporarily shut off the Internet.

Changing Times for the Russian Internet

The Internet has, until recently, successfully avoided Putin's attention. Nikolay Petrov, an analyst at the Carnegie Moscow Center, stated in mid-2012: "Two months ago, Putin was saying that the Internet doesn't deserve any real attention, and that it's the place where pornography dominates."[1] At that point, the Internet was still a mostly deregulated and uncensored frontier for the Russian population to obtain information and share ideas. Since early 2012, however, the Russian government's attitude toward the Internet has shifted from a general indifference to an evolving cyberphobia. We have witnessed a government campaign to gain complete control over the Russian population's access to, and activity on, the Internet.[2]

Shortly after the parliamentary elections of December 2011, segments of the Russian population began voicing their disapproval of the election results, citing election rigging in favor of Putin's party, United Russia. On December 10, 2011, tens of thousands of disillusioned Russian citizens congregated in Bolotnaya Square in Moscow; two weeks later, the number of participants swelled to 100,000.[3] These protests were by far the largest antigovernment demonstrations to occur since the dissolution of the Soviet Union in 1991; previous protests had drawn at most 200 individuals.[4]

Social media—including Facebook, VKontakte (the Russian equivalent of Facebook), LiveJournal, and Twitter—was used as a medium to coordinate the times and locations of rallies and demonstrations while also facilitating the collection and distribution of funds that made the demonstrations possible. In addition, social media was an integral catalyst to the protests, as it allowed the Russian population to see electoral fraud and manipulation in favor of—and potentially orchestrated by—the party in power. Dozens of user-generated videos capturing electoral violations were posted online. Some videos depicted carousel voting, in which individuals were bussed between various polling places to cast votes in favor of United Russia

under different names; other videos documented individuals stuffing stacks of ballots, already filled out with votes for United Russia, into ballot boxes.[5] Konstantin von Eggert, a Russian journalist and political commentator who previously headed the BBC Russian Service's Moscow bureau, summed up the role of the Internet in these protests by stating, "For the first time, really, the online presence has transformed offline politics."[6]

These protests sparked a transformation in Putin's attitude toward the network of networks. Since 2011, we have seen an onslaught of laws and initiatives aimed at eliminating Internet freedom and ensuring that the last form of free media in Russia is brought within boundaries dictated by the Russian government. Furthermore, it is likely that in the years to come, should economic sanctions continue to weigh heavily on the Russian economy, the Russian government will continue to expand its controls on the Internet to squash any opposition movements and ensure that the powers-that-be remain just that.

The Putin Government Declares War on the Open Internet

Since December 2011, Putin has tightened his grip on the Internet via numerous pieces of legislation. These laws were passed in rapid succession, and all used vague language to define the parameters for which sectors of the Internet they apply to and how they are enforced. The rapid implementation of legislation focused on constricting the Internet and the freedom of its users has been referred to as an initiative to create a domestic equivalent to the "Great Firewall of China" around web content in Russia. Putin has faced little resistance in this campaign, as the *Moscow Times* noted, "Russia's government and its loyalist legislature have a track record of passing so-called 'blitzkrieg' bills that impose Internet restrictions within weeks and without consulting the web community or IT industry."[7]

The Censorship Campaign Begins. President Putin's increased interest in the Internet was evident in the implementation of Federal Law No. 89417-6.[8] Formally titled "On the Protection of Children from Information Harmful to Their Health and Development" but more commonly known as the "Blacklist Bill," it was signed on July 28, 2012, less than six months after the protests of late 2011 and early 2012. The law's stated purpose is to block sites related to child pornography, materials on drug abuse or production, and suicide.

The law further states that a blacklist be instituted and maintained by the Federal Division Roskomnadzor, a government regulatory body roughly equivalent to the United States Federal Communications Commission.[9] Under this law, Roskomnadzor notifies sites that they are on the blacklist, and if the offending content is not removed within 72 hours of the notification, the site may be blocked. This law also includes measures that allow Roskomnadzor to essentially censor individual URLs, domain names, and IP addresses. Additionally, it grants Roskomnadzor power to censor websites that would encourage "mass riots" or "participation in unsanctioned events."

The approval of the Blacklist Bill raised numerous concerns from critics on how government regulation would operate within the confines outlined in the bill. On July 10, 2012, as the bill progressed swiftly through the State Duma, many Russian websites went dark in protest. They cited lack of oversight of the government authority appointed to implement the new restrictions. Coupled with the vague language of the bill and the uncertainty about what content would be deemed harmful to children, many believed this law would open the door for the potential of misuse and excessive, unwarranted censorship. Despite protests, the bill was approved by an overwhelming majority within one week.[10]

The Blacklist Bill has been used on several occasions. In the first two weeks after the bill was passed, more than 180 websites were banned; by February 2013, after a mere four months, the number of websites banned under the Blacklist Bill reached 4,000.[11] In March 2014, access to six websites—including those of dissident Alexei Navalny. individuals organizing protests against Russia's annexation of Crimea, and pages of Ukrainian rights groups on Russia's largest social media site—were shut off.[12] A study by Freedom House, an independent watchdog organization, details that from January 2012 to February 2013, the number of websites that were blocked for containing what the Ministry of Justice deemed "extremist" material increased by approximately 60 percent.[13]

On February 1, 2014, Roskomnadzor gained even greater authority. The "Lugovoi Law"—named after the member of the State Duma who sponsored it, who also happens to have been accused of murdering a Kremlin critic in 2006—gave the communications regulator the power to block, without a court ruling, websites deemed extremist or a threat to public order.[14]

Additionally, the Russian government focused on major independent news sites. On March 13, 2014, Russia's prosecutor general published a list that was sent to Russia's Internet service providers (ISPs). The list included several information sites and social media accounts of opposition groups and leaders. It also included the newspaper *Grani*, a popular opposition news portal famous for publishing pieces highly critical of the Kremlin. The ISPs were instructed to shut down servers that deliver the offending content in an effort by the government to prevent unauthorized protests and ensure that house arrest standards were met. [15]

Taking Aim at Russia's Online Civil Society. The next blow to Internet freedom in Russia came in April 2014 with the approval of the two antiterrorism laws. Before this point, the Kremlin had mainly concentrated on regulating access to sites that supported opposition groups or voiced disapproval of the Russian government's policies and friends. The antiterrorism laws, however, target different components of Internet freedom, such as the storage of data and monetary transactions conducted online.

The first law stipulates that owners and operators of websites and services "are obligated to store all information about the arrival, transmission, delivery, and processing of voice data, written text, images, sounds, or other kinds of action."[16] The wording of the law is opaque and does not succinctly define which companies or individuals fall under the umbrella of "owners and operators"—the law simply states that those obligated to archive information are "individuals or legal entities" who "[organize] the dissemination of information and (or) the exchange of information between Internet users." The law's vague language leaves much up to interpretation, thereby allowing Russian authorities greater discretion with which to demand that specific information be stored, ostensibly for the government to access and review.

The second law restricts anonymous money transfers and donations on the Internet. These restraints limit the amount of money a donor can give anonymously as well as restrict the ability to track the source providing funds to individuals, organizations, and businesses, including PayPal, Yandex.Dengi, and WebMoney.[17] It limits the amount individuals are able to donate via anonymous transactions online to $450 per month, and single-day transactions are limited to $30. Clearly, these restrictions will hurt any organization that relies on online financial donations, but

it is likely to have the most adverse effect for grassroots or smaller-scale civil society movements or protests.

Limiting Free Speech in the Blogosphere and Social Media. By 2014, laws restricting the Internet were coming in rapid succession. On May 5, 2014, another multipart bill was signed into law. Known as the "Bloggers Law," it requires all web-based writers with posts that exceed 3,000 page views to register with the government, as they are considered to fall under the umbrella of media outlets. At the time of the bill's approval, approximately 30,000 Russian bloggers were included under these new stipulations requiring that they fact check and delete any inaccuracies in their posts or risk their sites' being removed or blocked.[18] This law is notable because it is stricter than a similar Chinese law limiting blogger freedom, which sets the cutoff at 5,000 page views per day. Furthermore, the Bloggers Law does not merely apply to websites that could be classified as blogs or independent sites—it also applies to social media accounts that have posts with over 3,000 daily page views.

The law also implements scanning software that allows the Russian government to review all content posted on the Internet, regardless of daily page hits or classification. The software scans the Internet for undisclosed curse words that, if found, are reason enough for the site to be blocked or taken down.[19] Violators are subject to fines or suspension of business.

Confining Public Commentary. In June 2014, the Russian government passed a law that limits the redissemination of content they believe to be extremist or threatening. Dubbed the "Law against Retweets," this piece of legislation gives the government the right to imprison—for up to five years—any individual deemed a disseminator or redisseminator of "extremist materials"; its main aim is to target and punish "extremist retweeters."[20]

Although the Russian government had a history of arresting individuals for redisseminating antigovernment online material even before the Law against Retweets, this law codifies the pervasive, informal legal procedures that have, for example, imprisoned bloggers and professors.[21]

Further, the law raises concerns regarding the vague nature of its wording. In addition to the undefined notions as to what this law classifies as extremism, questions also remain concerning whether the law's enforcers will wait for proper government approval prior to moving forward with arrests and trials.

Surveillance and Mandated Local Data Storage. Next, a bill related to data retention and data mining was passed on July 4, 2014. The law requires Internet companies—including American technology giants such as Google, Twitter, and Facebook—to locate servers handling Russian Internet traffic inside the country and to store their users' data on these locally based servers for a minimum of six months. Companies have until September 2016 to comply or be blocked by the government.[22]

The law ambiguously defines "users" and can therefore be applied to a vast swath of websites.[23] The Russian government's reasoning behind the creation and approval of this law was centered on the Russian public's alleged desire to keep their data stored within their own borders and not off-site in foreign nations, such as the United States.[24] The motivation behind this law also appears to have roots in the Edward Snowden revelations—a Moscow city councilman, Alexey Lisovenko, stated in his plea to State Duma deputies, "Snowden has confirmed that the largest intelligence-gathering corporation there is—The US' National Security Agency—is monitoring our social media accounts."[25] He urged the lawmakers to pursue greater digital sovereignty for Russia, emphasizing data retention on Russian servers as a crucial component.

While it is alarming that servers in Russia would retain data from users (even non-Russian citizens who are merely surfing Russian websites) for extended periods of time, the concerns surrounding this requirement are amplified by the existence and scope of Russia's System of Operative Investigative Activities (SORM) program. Similar to the National Security Agency's PRISM program in the United States, SORM is able to rapidly filter through vast swaths of user data and information. As the program is not subject to any public oversight, SORM has access to essentially all information that flows through or originates on the Russian Internet.[26]

Access to Public Wi-Fi No Longer Anonymous. On July 31, 2014, a bill was signed that places further restrictions on Internet freedom and prohibits anonymous access to Internet in public spaces.[27] Under this law, Russians must now register with their phone number to use public Wi-Fi. The personal data entered is required to be stored for six months by the companies that control the networks being accessed.[28] It is not clearly defined which companies are required to comply with the law or what enforcement mechanism will be in place to monitor the companies' compliance and ensure that users enter valid information.

Further, the law does not specify what constitutes a "public area." Citing security as the motive for the law, the deputy chair of the State Duma's information technology committee, Vadim Dengin, asserted, "An information war is under way. Anonymous access to the Internet in public areas allows illegal activities to be carried out with impunity."[29]

Perhaps the most worrisome component of this measure is the fact that purchasing SIM cards for mobile phones in Russia requires that you provide your passport information. Therefore, every time users log in to public Wi-Fi with their mobile phone number, they are essentially providing their passport information (along with what content they access and for how long), which will be stored and can be accessed by the government for six months.[30]

A Kill Switch for the Russian Internet? Most recently, a meeting convened by Russia's Security Council on September 22, 2014, discussed the practicality of a government "kill switch" for the Russian Internet in case of crisis. Essentially, if a government-defined disaster arose, the government would be able to temporarily shut down portions of the Internet hosted in Russia and redirect all domestic Internet traffic to servers within the country.

What would constitute a crisis is ill-defined but is believed to include times of war or large-scale civil protests.[31] Utilizing the kill switch would give the government control over Russian servers, require all websites with .ru in their IP addresses to host their users' content in Russia, and prevent foreign IP addresses from accessing Russian networks.[32]

Though the Security Council had made no concrete decision regarding the Russian kill switch at the time of this publication, such an idea is very much feasible in Russia because of its Internet infrastructure. Russia has very few Internet exchange points—the physical infrastructure points via which ISPs exchange information and Internet traffic between their networks.[33] The few exchange points Russia does possess are controlled by national long-distance operators, which are closely intertwined with Russian authorities. For example, Rostelecom, Russia's leading long-distance telephone company, whose majority shareholder is the state, controls several of Russia's Internet exchange points. Popular Russian blogger Anton Nosik that commented, "Putting a block on the worldwide Internet doesn't present technical challenges and is only a matter of political will."[34]

The discussion of a kill switch for the Internet reflects Putin's growing desire to ensure that the Russian government has sole authority over the networks within the country. In a press conference in September 2014, Putin's spokesman Peskov stated, "Taking into account the complete unpredictability of the United States and the European Union, Russia is taking measures to ensure its own security. . . . This is a question for other countries, first and foremost the United States. Considering the unpredictability of their actions we should be ready for anything."[35] Peskov's statement highlights how heavily invested Putin has become in finding a solution to Russia's dependence on American technology and digital infrastructure.

No Longer Just Protecting the Children: Strict Filtering on All Content. As I have detailed, the Russian government initially cited the "protection of children from harmful content" as the seemingly valiant motivation for filtering and removing content from the Internet. At the time of this writing, however, the Kremlin is debating new legislation to filter all Russian Internet content before publication. Artyom Kozlyuk, head of Rublacklist.net, a watchdog organization that focuses on Internet freedom, explained that "such pre-filtering, so-called 'state white-listing,' would be a whole new level of Internet censorship and restriction of net freedoms."[36]

If implemented, the filtering mechanism (the exact details concerning the operation of which are still unclear) would be incredibly costly, with estimates hovering in the billions of dollars. In addition to the bill's vague language, the treatment of the bill in the Duma has been secretive; the

bill has, for example, been absent from the online State Duma database of legislation. It is supported by state-affiliated web morality watchdog the League of Safe Internet, an organization whose founder, Konstantin Malofeyev, is currently on a European Union blacklist, alleged of facilitating communication between pro-Russian separatists in Eastern Ukraine and the Kremlin.

The Consequences of Pursuing Complete Control and Digital Isolation

The new laws and regulations I have described clearly reflect the psychology of a government that has become increasingly paranoid and West-averse. The Internet in Russia has so wholly transformed from a vehicle of freedom of expression to another instrument of the state that, by April 2014, Putin began referring to it "as a special project [of the CIA]."[37]

The Putin government has blatantly flouted the very foundations of the Russian Constitution that ensures the Russian Federation remains a democratic state in which freedom of speech, thought, and idea are able to flourish. The ease and speed with which Putin has been able to implement comprehensive control over the Russian Internet and the ability of both foreign and domestic companies, institutions, and individuals to freely use the Internet without censorship or fear illustrates that the future of the Russian Internet is oppressive and grim.

The deleterious effects of Putin's digital isolation pursuits are apparent in Russia's standing in freedom of speech rankings. A 2014 Freedom House report on Internet freedom revealed that Russia had slid six percentage points year-on-year in the direction of "less free" and was now one point away from moving from the "partly free" category to the "not free" category. Russia ranks among the most oppressive nations with regards to Internet freedom, on par with historically repressive nations such as Kazakhstan and Egypt.[38] As Putin continues to tighten his grip on Internet censorship, Russia continues on a path to becoming one of the most restricted countries in the world.

Cyber idealists once predicted that the Internet would be immune to the efforts of authoritarian governments to control speech. The apparent success of Putin's campaign of oppression, censorship, regulation, and intimidation over online speech suggests those predictions were overly optimistic. Should this trend continue, Internet freedom in countries all over the world

will be in jeopardy, and the potential for these restrictions and censorship to spread to areas outside of the Internet and further threaten personal freedom will be great.

About the Author

Natalie Duffy (Natalie.Duffy0@gmail.com) was an intern in the Center for Internet, Communication, and Technology Policy at AEI in Fall 2014 and is currently pursuing her master's degree in European and Eurasian Studies at the Elliott School of International Affairs, George Washington University.

Notes

1. Jackie Northam, "Russian Activists Turn to Social Media," NPR, January 13, 2012.
2. Emily Parker, "Putin's Cyberphobia," *Foreign Policy*, September 24, 2014.
3. Markku Lonkila, "Russian Protest On- and Offline," Finnish Institute of International Affairs 98 (2012): 1–9, www.isn.ethz.ch/Digital-Library/Publications/Detail/?lng=en&id=137720.
4. Alissa De Carbonnel, "Insight: Social Media Makes Anti-Putin Protests Snowball," Reuters, December 7, 2011, www.reuters.com/article/2011/12/07/us-russia-protests-socialmedia-idUSTRE7B60R720111207.
5. Ibid.
6. Tom Balmforth, "Russian Protesters Mobilize via Social Networks, as Key Opposition Leaders Jailed," Radio Free Europe, Radio Liberty, August 12, 2011.
7. Alexey Eremenko, "Russia to Make Internet Providers Censor Content–Report," *Moscow Times*, December 2, 2014.
8. President of Russia, "Amendments to the Law on Protecting Children from Information Harmful to Their Health and Development," news release, July 31, 2012, http://eng.kremlin.ru/news/4246.
9. Marianna Mao, "Censorship Law in Russia Raises Grave Concerns for Internet Freedom," Herdict Blog (Harvard Law School), November 14, 2012, www.herdict.org/blog/2012/11/14/censorship-law-in-russia-raises-grave-concerns-for-internet-freedom/.
10. Katrina Kaiser, "Passing of the Internet Blacklist Bill Spells Bad News for Freedom of Expression in Russia," Electronic Frontier Foundation, July 24, 2012, www.eff.org/deeplinks/2012/07/blacklist-bill-spells-bad-news-for-freedom-expression-russia.
11. Miriam Elder, "Censorship Row over Russian Internet Blacklist," *Guardian*, November 12, 2012, www.theguardian.com/world/2012/nov/12/censorship-row-russian-internet-blacklist; "Registry Monitoring: State Agencies Shocked on February 23rd (and Banned 92 IP [Addresses])," Rublacklist.net, February 27, 2013, http://rublacklist.net/4445/.
12. Ilya Khrennikov and Anastasia Ustinova, "Putin's Next Invasion? The Russian Web," *Bloomberg Businessweek*, May 1, 2014, www.businessweek.com/articles/2014-05-01/russia-moves-toward-china-style-internet-censorship.
13. Parker, "Putin's Cyberphobia."
14. Tom Parfitt, "Russian MPs Tighten Control over Internet Data Storage," *Telegraph*, July 5, 2014, www.telegraph.co.uk/news/worldnews/europe/russia/10948202/Russian-MPs-tighten-control-over-internet-data-storage.html; Victor Davidoff, "Putin's Brave New Russia," *Moscow Times*, March 17, 2014, 17.
15. "Restricted Access to a Number of Online Resources," Roskomnadzor News Roskomnadzor, March 13, 2014; Eva Galperin and Danny O'Brien, "Russia Blocks Access to Major Independent News Sites," Electronic Frontier Foundation, March 13, 2014, www.eff.org/deeplinks/2014/03/russia-blocks-access-major-independent-news-sites.
16. "Law No. 428884-6," Russian State Duma, January 15, 2014; Kevin Rothrock, "Russia's Parliament Prepares New 'Anti-Terrorism' Laws for Internet," Global Voices, January 16, 2014, http://globalvoicesonline.org/2014/01/16/russias-parliament-prepares-new-anti-terrorist-laws-for-internet/.
17. Ibid.
18. Khrennikov and Ustinova, "Putin's Next Invasion?"
19. Lauren C. Williams, "Russia Declares War on Bloggers with Sweeping New Censorship Law," ThinkProgress. May 7, 2014, http://thinkprogress.org/world/2014/05/07/3435292/what-its-like-to-use-the-internet-in-russia/.

20. Kevin Rothrock, "Russian Bureaucracy's Race to Police the Web," RuNet Echo, June 23, 2014, http://globalvoicesonline.org/2014/06/23/russia-bureaucracy-police-internet-censorship-law/.
21. Antesla, "Alright, Now I'm Officially an Extremist," LiveJournal, November 6, 2013, http://antesla.livejournal.com/3974.html; "Regional Bloggers Targeted for 'Extremism' by Russian Police," Global Voices, November 10, 2013, http://globalvoicesonline.org/2013/11/10/regional-bloggers-targeted-for-extremism-by-russian-police/.
22. Max Smolaks, "Russian Government Will Force Companies to Store Citizen Data Locally from 2016," TechWeekEurope, July 4, 2014, www.techweekeurope.co.uk/workspace/russian-government-will-force-companies-store-citizen-data-locally-148560.
23. Kevin Rothrock, "Everything You Need to Know about Russia's Internet Crackdown," Global Voices, July 5, 2014, http://globalvoicesonline.org/2014/07/05/russia-internet-censorship-laws-crackdown/.
24. Denis Chrissikos, "Russia's Internet Censorship: What Role for Civil Society?" Republic of the East, July 17, 2014.
25. Kevin Rothrock, "A Russian Gulag for American Social Networks' Data?" Global Voices, April 5, 2014.
26. Matthew Bodner, "Russians' Internet Increasingly Subject to Control," *Moscow Times*, September 19, 2014, www.themoscowtimes.com/business/article/russians-internet-increasingly-subject-to-control/507449.html.
27. "Russia Demands Internet Users Show ID to Access Public Wifi," Reuters, August 8, 2014, www.reuters.com/article/2014/08/08/us-russia-internet-idUSKBN0G81RV20140808.
28. Darren Pauli, "Anonymous Wifi the Latest Casualty of Russia Net Neurosis," Register, August 11, 2014, www.theregister.co.uk/2014/08/11/anonymous_wifi_the_latest_casualty_of_russia_net_neurosis/.
29. "Russia Demands Internet Users Show ID to Access Public Wifi."
30. Olga Razumovskaya, "Fear and Loathing over Russia's Anonymous Wi-Fi Ban," Digits, August 8, 2014, http://blogs.wsj.com/digits/2014/08/08/fear-and-loathing-at-russias-anonymous-wi-fi-ban/.
31. Bodner, "Russians' Internet Increasingly Subject to Control."
32. Jeff Stone, "Kremlin Mulls Internet 'Kill Switch' to Knock Russia Offline During Emergencies," *International Business Times*, September 23, 2013, www.ibtimes.com/kremlin-mulls-internet-kill-switch-knock-russia-offline-during-emergencies-1693840.
33. Luke Harding, "Putin Considers Plan to Unplug Russia from the Internet in 'Case of Emergency,'" *Guardian*, September 19, 2014, www.theguardian.com/world/2014/sep/19/vladimir-putin-plan-unplug-russia-internet-emergency-kremlin-moscow.
34. Ilya Khrennikov and Henry Meyer, "Russia Plans to Break from Global Web as U.S. Rift Deepens," Bloomberg, September 19, 2014, www.bloomberg.com/news/2014-09-19/russia-seeks-to-safeguard-itself-from-u-s-internet-regulation.html.
35. Anna Smolchenko and Olga Rotenberg, "Putin Is Considering Unplugging the Internet in Russia During Protests or War," *Business Insider*, September 19, 2014.
36. Eremenko, "Russia to Make Internet Providers Censor Content–Report."
37. Olga Razumovskaya, "Russian Parliament Approves New Law Restricting the Internet," *Wall Street Journal*, April 29, 2014, www.wsj.com/articles/SB10001424052702304163604579531460215555456.
38. "Freedom of the Net 2014," Freedom House, December 5, 2014, https://freedomhouse.org/report/freedom-net/freedom-net-2014#.VIHDv9LF98G.