The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

FSB Will Welcome Russia's Internet Server Law

By Andrei Soldatov

July 09, 2014



A little more than two years ago, in March 2012, Sergei Smirnov, first deputy director of the Federal Security Service, presented a policy paper about the threat to state power posed by social networks.

The venue he chose, a meeting of the Regional Anti-Terrorist Structure, an outgrowth of the Shanghai Cooperation Organization, was no coincidence. The organization's members — Kazakhstan, Kyrgyzstan, China, Russia and Tajikistan — have begun to use their meetings to discuss and plan countermeasures against the types of social networks that played such an important role in the Arab Spring.

In essence, Smirnov said that Western intelligence agencies use the blogosphere to overthrow political regimes and that the Federal Security Service, known by its Russian acronym FSB, was going to "cleanse" the Internet of their influence. At the same time, Smirnov was forced to admit that the FSB had "not yet developed" those countermeasures. In other words, the FSB was still at a loss as to how to cope with the social networks.

The reason for their difficulties was immediately apparent: The FSB only understood how to combat the influence of social networks located on Russian territory. Under Russian law, all communications operators and hosting providers are required to install surveillance and interception equipment, otherwise known as a "back door."

This requirement is part of Russian intelligence agencies' famous SORM, or System for Operative Investigative Activities. As one FSB employee told me in 2012, "Why should we put pressure on social networks when we can use SORM to gather information from servers without their knowledge?"

And so at the time of Smirnov's report, Russian intelligence agencies had just one problem — how to deal with networks with servers physically located beyond Russia's borders.

Now two years later, the FSB has found a solution. The new law that the State Duma passed last Friday prohibits the storing of Russians' personal data anywhere but in Russia.

There is some irony in the fact that Russian intelligence agencies justify the expansion of their powers with the argument that they are protecting the personal data of Russian citizens.

In fact, nobody asked Russia's Duma deputies to protect their personal data. In contrast to the people of Brazil, whose outrage over U.S. National Security Agency spying led to a similar draft law, Russians were not especially shocked by recent revelations about Washington's global cyber espionage. On the contrary, Russian civic organizations strongly opposed the law. Nonetheless, Putin is fully expected to sign it.

Critics of the law argue that its enforcement will make it impossible for Russians to buy air tickets online, reserve hotel rooms in foreign countries, or order consumer items from abroad. This is because some foreign companies with little Russian business will choose not to relocate their servers, as doing so would cost more than the profits they expect to make from Russian clients.

However, Russian officials have no intention of applying the law across the board.

Russia's approach to controlling the Internet works differently than countries like China that operate stringent firewalls to prevent access to censored content.

In essence, Russian censorship consists of a set of laws that are worded as broadly as possible. These broadly worded laws, formulated two years ago when Russia first introduced nationwide Internet filtering, enable the security services to easily block Internet services they accuse of noncompliance. The laws are particularly dangerous in that they do not include any written reference to specific technical measures they can or cannot use toward those ends. Once passed into law, the bill on web servers will become part of this censorship system.

By relocating servers to Russia, foreign Internet companies will be more vulnerable to Russian laws, forcing them to consult with the Kremlin in an effort to learn exactly what is required of them. Russia's legal system is not a guidebook that defines the rules of the game for all of the players, but a large club with which the government silently threatens everyone, coercing companies to ask what is permitted in order to avoid getting hit. This approach is effective because it is flexible, allowing leaders to change how the law is implemented any time they

want.

This system is also technologically superior to establishing a censorship bureau because Google and Twitter obviously know better than government officials how to sanitize their own content. It is also inexpensive because companies pay for all server relocation costs themselves, sparing the federal budget.

The new law will come into force in two years: on Sept. 1, 2016. The law's authors believe that provides enough time for Internet companies to open data centers based in Russia. In fact, officials will use those two years to negotiate with the key players to whose data they want to gain access. These key players most likely include the social networks Facebook and Twitter, as well as Google's email service, Gmail.

It remains to be seen how international NGOs devoted to defending freedom of speech on the Internet will use these next two years. But they should not spend their time idly. Other countries wanting to control their own cyberspace are more likely to copy the Russian approach than that used in China.

Andrei Soldatov is an intelligence analyst at Agentura.ru and co-author of "The New Nobility: The Restoration of Russia's Security State and The Enduring Legacy of the KGB."

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2014/07/09/fsb-will-welcome-russias-internet-server-law-a37175