The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

What Russia's New Draconian Data Laws Mean for Users

The Moscow Times took a look at how the laws will affect users and companies.

By Matthew Bodner

July 13, 2016

Life-Of-Pix / Pixabay

After three years of relative silence, NSA whistle-blower Edward Snowden spoke up: "[President Vladimir] Putin has signed a repressive new law that violates not only human rights, but common sense. Dark day for Russia." For the man who fled to Russia after blowing the lid off the NSA's unprecedented Internet surveillance program, it seemed to be too much to swallow.

"Signing the Big Brother law must be condemned. Beyond political and constitution consequences, it is also a $33 billion [or more] tax on Russia's Internet," Snowden wrote on

Twitter on July 7.

But Snowden is not alone in his criticism of the new laws. Despite the scores of dire warnings from leading Russian Internet and technology figures about the technological impracticality of the laws, Putin signed them into action last week. Championed publicly by State Duma deputy Irina Yarovaya, there has been speculation that the initiative came from the security services, with Putin's blessing.

While the new laws cover a wide spectrum of draconian policies, three areas of the legislation are of particular concern to the Russian Internet.

First, the imposition of a nationwide dragnet. Telecom companies, as well as the vaguely described "organizers of information distribution" — a term that applies to any website or application — will be required to store copies of all data to pass through their servers for six months beginning July 1, 2018. All metadata must be stored for three years, although websites need only store one year's metadata.

Second, cooperation with the authorities. Considering that most communications traffic is encrypted in one form or another, companies will be obligated to provide the Federal Security Service (FSB) with keys to the encryption, and back doors have been essentially mandated. The third, but closely related point, is that the FSB will soon have access to any user's messaging data without court order.

The Moscow Times took a look at how the laws will affect users and companies.

Encrypted Messaging, Internet Browsing

Russian Internet users are concerned about the future of their Internet security. Following Snowden's NSA surveillance revelations four years ago, demand has surged for encrypted messaging apps. So too has the demand for secure Internet browsing, facilitated either through anonymous browsers like the Tor Network or Virtual Private Network (VPN) services.

Depending on the type of encryption used, compliance with the new laws is either impractical or impossible.

Take for example WhatsApp, the world's most popular messaging service. Earlier this year, the company began to wrap all forms of communication facilitated by their services in a form of encryption known as end-to-end. This encryption ensures that no one — other than the two devices in communication — have the keys to the code. When the FSB asks WhatsApp to provide keys to message encryption, it is asking for something the company cannot access.

"The Russian approach here is a bit outdated," says Andrei Soldatov, co-author of "The Red Web" and an expert on Russian electronic surveillance efforts. "It is based on the assumption that there is no such thing as end-to-end encryption, and that encryption is hardware, rather than software based." In this vein, Russia is hoping to force companies like Apple to sell phones in Russia that have end-to-end encryption disabled. "But this cannot work because they can't prevent you from downloading an encrypted messenger

service onto your phone." Encryption is done by the app, not the iPhone.

While it is conceivable that Russian authorities could pressure Apple into restricting encrypted messenger apps from the Russian App Store, "this could only work when everyone believes you will deliver on the threat," Soldatov says, "and this is questionable given Russia's obvious failure to punish global firms for being reluctant to move servers to Russia last year." But while the threat may not be credible, it is real. The question remains how far Russia will take this.

The bigger risk for Russian Internet users is that encryption-based services, including providers of Virtual Private Networks (VPNs) simply leave the Russian market rather than deal with working around the new legislation. This happened on July 11, when a VPN service known as Private Internet Access (PIA) announced that it was completely withdrawing from the Russian market after discovering evidence that "some of our Russian Servers (RU) were recently seized by Russian authorities, without notice or any type of due process."

A VPN is one of the best options available for secure Internet, and if the Russian legislation drives these services completely out of the market, only the consumer can suffer. The government is also taking huge risks with Russian data. If companies are forced to build back doors for the FSB to access, then anyone else could exploit them. At the other end of the data collection process, the government's data storage facilities will become attractive targets for governments and cyber criminals.

Internet Companies

The burden forced on companies in Russia is no less dramatic. Already, major Russian Internet firms like Yandex and Mail.ru have joined forces to speak out about the legislation. As "organizers of information distribution," they will have to shoulder the burden of copying all their data, decrypt the encrypted data, and pass it along to the FSB.

All of this requires significant investment on the part of the company, and it applies to both large tech giants like Yandex, and small start-ups like CourseBurg, an Internet marketplace for offline educational courses. Alexander Alkhov, CourseBurg's co-founder and CEO, says the new laws are "very destructive" to the Russian online business community.

"It will be particularly difficult for young companies like ours, since it will worsen the investment climate in the Russian segment of the Internet, and it can put an end to many of the innovative projects that have only just started to appear in Russia. Or, we will have to go to the West and set up our companies there," Alkhov says.

"So much has been done to support innovative projects in this country in recent years, it would be a pity if one set of bills negates all of it," he added.

Telecoms, Infrastructure

Russia's so-called "big four" telecommunications companies have all predicted that service costs will rise two to three times as a result of the new requirements, the RBC news agency reported on June 29. Compliance costs for telecom operators have been estimated at around

2.2 trillion rubles – or twice the combined annual revenue of MTS, Megaphone, VimpelCom and Tele2.

The companies will need to invest heavily in data storage capacity to store the required six months of data, and three years of all metadata that travels through their networks. They will also need to invest in communications infrastructure to facilitate the transfer of all that extra data.

Vladimir Gebrielyan, the CTO of one of Russia's largest Internet companies, Mail.ru, wrote in a column published by RBC on June 23 that Russia simply does not have the data storage capacity to store so much data. "The storage dimensions required for this are unprecedented: It would take all the data-storage factories in the world producing systems for years just for Russia."

Considering that it takes three to four years to build a data center, that there isn't enough power generation in the European part of Russia to support the centers, and that some 5 trillion rubles would need to be spent upgrading communications lines to facilitate the increased traffic, the Yarovaya laws are not feasible, Gebrielyan wrote.

And while Russian companies and users will assume the massive burden of compliance with the laws, "it is the equipment suppliers that will be the only ones to benefit," noted CourseBurg's Alkov. The great irony here is that suppliers for large data-storage and telecom infrastructure are all foreign.

Russia's Culture Ministry has become a surprising voice of reason amid the Yarovaya debate. There are so many complications that even Communications Minister Nikolai Nikiforov, said on June 29, "there will be serious issues with the application of this law. We are confident it will require a number of amendments."

Original url:
https://www.themoscowtimes.com/2016/07/13/what-russias-new-draconian-data-laws-mean-for-users-a54552