The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Russia's Data Storage Push Hits Snag: It Needs Foreign Help

By Reuters

July 05, 2018

Deputy Prime Minister, Maxim Akimov. **Valery Sharifulin / TASS**

Russian telecommunications operators will have to use foreign technology to comply with a law on storing data, two industry sources with knowledge of the matter said, even though Vladimir Putin told his government to ensure local companies produced the equipment.

The law requires operators to store the content of users' phone calls and text messages for six months to aid the security services. President Putin wanted homegrown technology to be used to perform the task, to boost the domestic tech industry and make telecommunications systems less dependent on Western equipment.

But faced with a tight deadline to start storing the vast amounts of information, and in the absence of suitable Russian hardware, operators will have no choice but to use equipment made by foreign firms including Cisco, Hewlett Packard Enterprise and Huawei, according to the sources.

Related article: Russia's 'Big Brother' Law Enters Into Force

In having to resort to buying in hardware from abroad, Russia is encountering the same issues as other countries including the United States: the tech sector is a multinational endeavor and developing sophisticated systems using only homegrown gear is fraught with difficulties.

"It's a good idea in theory to substitute imports, but you need to make a realistic assessment of the capacity of Russian firms," said Irina Levova of Moscow-based independent think-tank the Institute for the Study of the Internet.

"The money spent implementing this law won't stay in the Russian economy but will end up abroad."

Adding to the problems besetting implementation of the law, no Russian telecommunications operator has the necessary infrastructure in place, despite a July 1 deadline to start storing users' data, according to the two telecommunications industry sources.

One of the sources is a senior manager at a Russian telecommunications operator, who declined to be named due to the sensitivity of the matter. The other is the general director of Norsi-Trans, a company that procures hardware for telecommunications operators.

Russia's ministry for digital development and communications did not respond to a request for comment about the use of foreign hardware or about whether telecommunications firms have the necessary infrastructure in place.

Related article: 'I'm Scared I'll Die Working'

A spokesman for Deputy Prime Minister Maxim Akimov, responsible for telecommunications, referred questions to the ministry for industry and trade. The ministry said Russian-made storage equipment had been tested this year and that it would seek to help local manufacturers competing against foreign firms.

There is no legal requirement for telecom operators to use Russian-made hardware to comply with the data rules, which are part of a package of anti-terrorism legislation dubbed the Yarovaya laws after Irina Yarovaya, one of the sponsors in parliament.

Of Russia's biggest operators, Rostelecom, Vimpelcom and MTS declined to comment about whether they would have to use foreign hardware to comply with the law, while Megafon and Tele2 did not respond to requests for comment.

When asked whether they had the necessary infrastructure in place, Vimpelcom, Rostelecom, and Megafon said their systems were still under development. MTS and Tele2 Russia declined to comment.

Putin's Instruction

After signing the Yarovaya legislation into law in July 2016, Putin instructed his government to ensure that production of the equipment to store users' data took place within Russia.

"This needs to be done swiftly. We need to fill up the order books of our own firms, especially since these are good, guaranteed orders," Putin said at the time at a meeting with government ministers.

Related article: 1 in 10 Russians Want to Emigrate — State Pollster

A handful of Russian companies are approved by the domestic intelligence service, the FSB, to provide combined systems of software and hardware that gather and store the contents of phone calls and text messages.

But the systems they are designing in most cases use foreign hardware to store the data, the two sources told Reuters.

"Russia just does not have the capacity to produce, in the quantities needed," the equipment for storing data, said the senior manager at a Russian telecoms operator.

Sergei Ovchinnikov, general director of Norsi-Trans – one of the companies selling the data-gathering and storage systems to telecoms firms – also said foreign equipment was being used.

Ovchinnikov said Russian-made hardware for storing such massive amounts of data were still at the testing stage. He said his own company offered customers the option of using hardware from China's Huawei and other foreign firms to run home-grown software.

"As far as I know, others producers of ... (the technology to lawfully gather users' data) mainly use foreign solutions," he added.

The leader in the small Russian sector for supplying these combined systems is a firm called Citadel, which has a market share of about 50 percent, according to telecommunications industry executives, followed by Norsi-Trans with 20-30 percent.

A Citadel representative declined to disclose to Reuters where the company procures its hardware, citing commercial secrecy. The company tailors solutions to the needs of each client, the representative said.

Related article: Why It Is Our Duty to Free Oyub Titiyev (Op-ed)

Asked about deals with Russian telecommunications firms, U.S. company Cisco said it was "not in a position to comment on other organizations' network infrastructure".

Huawei said it did not disclose commercial information about relations with its clients but it said it was looking into possible cooperation with companies producing equipment used for gathering users data under the law.

U.S. firm Hewlett Packard Enterprise (HPE) said company policy prevented it from commenting on contracts with customers.

Security Concerns

The Yarovaya laws were written by officials in Russia's Security Council, according to four sources in the IT sector and the government. The council, which includes key ministers, sets the strategic direction for Russia's security and defense policies.

The laws were written without consultation with technical specialists, according to business lobby group the Russian Union of Industrialists and Entrepreneurs and the Institute for the Study of the Internet.

The Security Council did not immediately respond to a request for comment about how the laws were written.

A week after Putin signed the law, Deputy Minister of Economic Development Oleg Fomichev said there was not enough data storage equipment available, in Russia or abroad, to meet the terms of the legislation.

Related article: More Foreign Agent Labels Possible With Proposed Law

The laws come against the background of a separate Kremlin drive to curb the use of foreign hardware and software in state digital infrastructure because it says such technology represents a cyber-security risk. Last year Moscow instructed government bodies and state companies not to buy foreign telecommunications hardware.

Russia is not the only country to have such concerns.

A hostile foreign government, counter-intelligence officials say, could adapt technology at the point of manufacture. When it is sold to an overseas buyer, the hostile government acquires a "back door" into the host country's digital networks.

The United States has pressured U.S. companies to not sell products made by China's Huawei or ZTE products, saying they potentially could be used to spy on Americans.

They have also triggered concerns over Western companies such as Hewlett Packard Enterprise and SAP sharing their source code to the Russian authorities as a condition for access to the Russian market.

Asked if their equipment could be exploited by foreign intelligence services, Cisco said it does not work with any government or customer to weaken its products for exploitation.

Huawei said its products underwent a Russian certification process that includes testing to ensure there are no undeclared capabilities or vulnerabilities.

Original url:
https://www.themoscowtimes.com/2018/07/05/russias-telecoms-security-push-hits-snag-it-needs-foreign-help-a62129