The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Kremlin Considers Real-time Online Surveillance to Replace Mass Data Storage

By Ed Crowther

September 21, 2016

TASS

The Kremlin is to drop part of its new, controversial anti-terror legislation, which would have seen all online and mobile communications stored for six months.

Russian intelligence agencies are instead looking to implement the law by deciphering and analyzing internet traffic in real time, the Kommersant newspaper reported Wednesday.

The recently-approved law, which was authored by ultra-conservative United Russia lawmaker Irina Yarovaya, required telecom operators to store users' messages, photos and videos for six months.

Metadata, which includes the time and date at which a call was made, will still be stored for 3 years. Companies will also still face fines of up 1 million rubles ($15,700) if they do not decode users' data at the request of Russia's Federal Security Service (FSB).

The law caused a widespread backlash from Russian companies, who claimed that the move would see them forced to spend 2.2 trillion rubles ($33.8 billion), on new infrastructure and maintenance.

Russia's Deputy Minister for Economic Development, Oleg Fomichev, went on to admit in July that the data storage infrastructure needed to put the law into force did not exist anywhere in the world.

The FSB is now working with the government on deciphering and monitoring Russia's internet traffic in real time, Kommersant reported. The plan would see the agency scan online communications for keywords such as "bomb," the paper's government source said.

Decrypting protected HTTPS connections would allow the security services to not just read messages being sent online, but see which sites users accessed, when they were accessed, and what users did on each site, the source said.

Kommersant's sources claim that the FSB is discussing the use of so-called Man in the Middle (MITM) attacks, which secretly relays communication between two parties who believe they are talking in private.

Another method, Deep Packet Inspection (DPI) could to be used to analyze both encrypted and decrypted traffic, Kommersant reported. DPI is already used by many Russian internet operators to block sites which have been banned by the Russian government's media watchdog Roskomnadzor.

Private communications companies may be forced to use Russian-made equipment to implement DPI systems as part of the government's import substitution program, one source said. Several Russian companies are already developing the necessary software for the move, Kommersant reported.

Experts polled by Kommersant said that while the move could be effective in fighting terrorism, they also make it easier for enforcement agencies to abuse citizens' constitutional rights and endanger national security.

Original url: https://www.themoscowtimes.com/2016/09/21/yarovaya-a55416