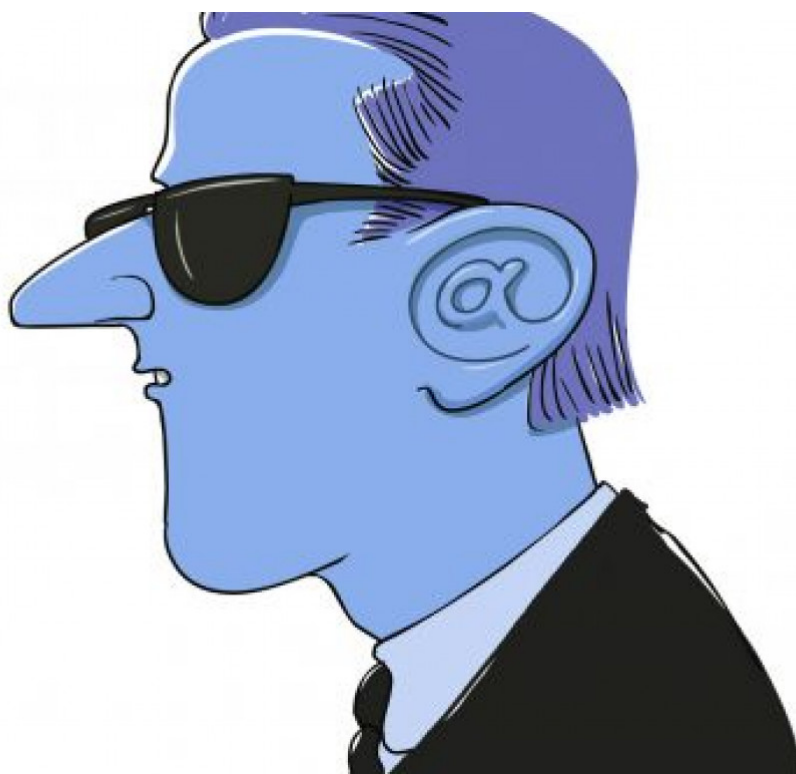


Russia's Spying Craze

By [Andrei Soldatov](#)

October 30, 2013



It came as a shock to many observers when VimpelCom, one of Russia's largest telecommunications companies, publicly criticized the government's plans to legalize the interception of telephone and e-mail communications. VimpelCom sent a letter to the Communications and Press Ministry criticizing the plan as unconstitutional.

But this type of espionage is not all that new. The principles governing that system were established and first implemented back in the 1990s. Every few years since then, the requirements placed upon Internet providers and phone companies have been updated in accordance with the latest technologies and the ever-growing appetite of Russia's intelligence agencies.

After the FSB
announced its
plans to gain
direct access to
phone calls and

e-mails without a court warrant, other Russian agencies said they want in on the spying game.

For example, the new spying program requires that phone operators and Internet providers make it possible for intelligence agencies to intercept correspondences that users sent through companies such as Gmail and Yahoo, along with ICQ instant messages and even obligates the companies to store the information for 12 hours at a time until it is retrieved by the authorities. These requirements would expand the authorities' surveillance capabilities to intercept correspondences that are passed through foreign Internet providers.

The number of telephone calls and e-mail messages that the Federal Security Service has intercepted has doubled over the past six years, from 265,937 in 2007 to 539,864 in 2012. These figures were based on the number of court sanctions issued to approve the government's surveillance of private communications, according to the Supreme Court. What's more, other federal agencies have followed the example of the FSB by legalizing their own communications interception programs. These include the Federal Drug Control Service, the Interior Ministry and the Federal Penitentiary Service.

The interception system was designed to avoid any outside control. The same reasons that prompted the U.S. National Security Agency to create its PRISM system also motivated Russia to create a legal interception system it called SORM that has enabled the authorities to remotely access information from phone operators and Internet providers. For this purpose, the provider must install a SORM black box that is connected by a cable to a command center at FSB headquarters. By using this equipment, FSB agents can monitor all phone conversations, e-mail correspondence, instant messages, Internet searches and so on.

Notably, Russian telecommunications and Internet companies have not publicly complained about the practice for many years. The last instance was in 1998, when the first initiative was introduced mandating the installation of Internet surveillance equipment. But the providers did not complain about the violations of Russians' civil and privacy rights, but only about the fact that they would be forced to pay for the SORM equipment.

Today's situation is different in that communications giant VimpelCom is upset not only about the requirement that it must bear all of the expenses of installing the government's surveillance equipment, but that such a law would violate citizens' constitutional right to confidential correspondence.

Of course, National Security Agency leaker Edward Snowden's revelations might have played a key role in mobilizing public opinion against electronic eavesdropping, but it is also possible that the sheer speed with which the government has been encroaching on Internet privacy is what prompted VimpelCom to become such an outspoken opponent of such measures.

The same day that VimpelCom openly criticized the FSB surveillance program, another government agency requested the right to intercept information. Oddly enough, it was not

an intelligence agency but the Central Bank that made the request. The bank prepared amendments to the law on insider trading that would give it access to private telephone conversations and correspondence in an effort to identify potential abusers of inside information on financial markets.

The Central Bank has already leveled fines against Rambler.ru and Mail.ru, Russia's two largest such providers, for refusing to provide correspondence information without a court order. According to the Central Bank, collecting "metadata" — general information about who is corresponding with whom without actually reading the content of those correspondences — does not violate the constitutional rights of Internet users, but the e-mail providers argue that it is technically impossible to obtain that information without actually opening the letters themselves.

According to those companies, the efforts of the Central Bank to gain access to such information and its use of heavy fines to force compliance has inspired other government agencies with no connection to fighting terrorism or crime to make similar demands for information on their clients — and all without a court order. Everyone wants in on this spying game.

There are already eight siloviki agencies that have the right to monitor the correspondence and phone conversations of anyone they choose. The key question is: How many will be listening alongside them one year from now?

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/2013/10/30/russias-spying-craze-a29105>