**Russia's Surveillance State**


Andrei Soldatov and Irina Borogan



*World Policy Journal* 2013 30: 23

DOI: 10.1177/0740277513506378

THE LUBYANKA

# Russia's Surveillance State

ANDREI SOLDATOV AND IRINA BOROGAN

MOSCOW—In March 2013, the Bureau of Diplomatic Security at the U.S. State Department issued a warning for Americans wanting to come to the Winter Olympics in Sochi, Russia next February: Beware of SORM. The System of Operative-Investigative Measures, or SORM, is Russia's national system of lawful interception of all electronic utterances—an Orwellian network that jeopardizes privacy and the ability to use telecommunications to oppose the govern-

ment. The U.S. warning ends with a list of "Travel Cyber Security Best Practices," which, apart from the new technology, resembles the briefing instructions for a Cold War-era spy:

> Consider traveling with "clean" electronic devices—if you do not need the device, do not take it. Otherwise, essential devices should have all personal identifying information and sensitive files removed or "sanitized." Devices with wireless connection capabilities should have the Wi-Fi turned off at all times. Do not check business or personal electronic devices with your luggage at the airport. … Do not connect to local ISPs at cafes, coffee shops, hotels, airports, or other local venues. … Change all your passwords before and after your trip. … Be sure to remove the battery from your Smartphone when not in use. Technology is commercially available that can geo-track your location and activate the microphone on your phone. Assume any electronic device you take can be exploited. … If you must utilize a phone during travel consider using a "burn phone" that uses a SIM card purchased locally with cash. Sanitize sensitive conversations as necessary.

The list of recommendations ends with the advice to discard the user's phone and SIM card before returning. The instruction might seem like overreaction, but far from it. Anyone who wants to attend the Olympics needs a Spectator pass, which requires registering on the official Sochi 2014 site, a procedure that includes taking a photo. What is curious is that when clicking to take a photo, a MacBook immediately warns the user that the site "is requesting access to your camera and microphone. If you click Allow, you may be recorded."

But the Russian surveillance effort is not limited to the Sochi area, nor confined to foreigners. For years, Russian secret services have been busy tightening their hold over Internet users in their country, and now they're helping their counterparts in the rest of the former Soviet Union do the same. In the future, Russia may even succeed in splintering the web, breaking off from the global Internet a Russian intranet that's easier for it to control.

## INTERCEPT TELECOM

Over the last two years, the Kremlin has transformed Russia into a surveillance state—at a level that would have made the Soviet KGB (Committe for State Security) envious. Seven Russian investigative and security agencies have been granted the legal right to intercept phone calls and emails. But it's the Federal Security Service (FSB), the successor to the KGB, that defines interception procedures, and they've done that in a very peculiar way.

In most Western nations, law enforcement or intelligence agencies must receive

*Andrei Soldatov and Irina Borogan are Russian investigative journalists who cover the operations of Russian security services. They are co-founders of the website Agentura, which chronicles the services' activities. They also co-authored* The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB *(Public Affairs, 2011).*

a court order before wiretapping. That warrant is sent to phone operators and Internet providers, which are then required by law to intercept the requested information and forward it to the respective government agencies. In Russia, FSB officers are also required to obtain a court order to eavesdrop, but once they have it, they are not required to present it to anybody except their superiors in the FSB. Telecom providers have no right to demand that the FSB show them the warrant. The providers are required to pay for the SORM equipment and its installation, but they are denied access to the surveillance boxes.

The FSB has control centers connected directly to operators' computer servers. To monitor particular phone conversations or Internet communications, an FSB agent only has to enter a command into the control center located in the local FSB headquarters. This system is replicated across the country. In every Russian town, there are protected underground cables, which connect the local FSB bureau with all Internet Service Providers (ISPs) and telecom providers in the region. That system, or SORM, is a holdover from the country's Soviet past and was developed by a KGB research institute in the mid-1980s. Recent technological advances have only updated the system. Now, the SORM-1 system captures telephone and mobile phone communications, SORM-2 intercepts Internet traffic, and SORM-3 collects information from all forms of communication, providing long-term storage of all information and data on subscribers, including actual recordings and locations.

Over the last six years, Russia's use of SORM has skyrocketed. According to Russia's Supreme Court, the number of intercepted telephone conversations and email messages has doubled in six years, from 265,937 in 2007 to 539,864 in 2012. These statistics do not include counterintelligence eavesdropping on Russian citizens and foreigners.

At the same time, Moscow is cracking down on ISPs that don't adhere to their SORM obligations. We discovered Roskomnadzor (the Agency for the Supervision of Information Technology, Communications, and Mass Media) statistics covering the number of warnings issued to ISPs and telecoms providers. In 2010, there were 16 such warnings, and there were another 13 in 2011. The next year, that number jumped to 30 warnings. In most cases, when the local FSB or prosecutor's office identified shortcomings, they sent the information to Roskomnadzor, which warned the ISP. Penalties for failure to meet their obligations are swift and sure. First, the ISP is fined, then if violations persist, its license may be revoked.

## TARGETING WHOM?

In 2011-2012, while protesters flooded Moscow's streets, the phones of a number of Russian opposition leaders and members of the State Duma were hacked. Recordings of their private telephone conversations were even published online. On December 19, 2011, audio-files of nine tapped phone calls of Boris Nemtsov, a former deputy prime minister and now a prominent opposition leader, were posted on the pro-government site lifenews.ru. Nemtsov requested an official investigation. As yet,

AFTER SECURING THE LEGAL ABILITY TO SNOOP ON MOBILE PHONES AND EMAILS, THE RUSSIAN SECRET SERVICES TARGETED SOCIAL NETWORKS.

none of the leakers have been found or prosecuted, and the official investigation has not identified a single culprit.

Such victims have no doubt they were bugged and filmed by security services, but only in the fall of 2012 did the first clear indication emerge that SORM was used to wiretap opponents of President Vladimir Putin. On November 12, 2012, Russia's Supreme Court upheld the right of authorities to eavesdrop on the opposition. The court ruled that spying on Maxim Petlin, a regional opposition leader in Yekaterinburg, was lawful since he had taken part in rallies that included calls against extending the powers of Russia's security services. The court decided that these were demands for "extremist actions" and approved surveillance and telephone interception.

## FACEBOOK THREAT

After securing the legal ability to snoop on mobile phones and emails, the Russian secret services targeted social networks next. Immediately after the Arab Spring, they were tasked with finding a response to the threat of political stability ostensibly posed by social networks. In August 2011, at an informal summit of the Collective Security Treaty Organization (CSTO), a regional military alliance led by Moscow, in Astana, Kazakhstan, the main topics of discussion were the revolutions in the Middle East and the role played by social networks. The summit, which was attended by then Russian president Dmitry Medvedev, adopted a confidential document recognizing the potential danger of social media in the organization of protests in Russia.

But nobody in the Kremlin and security services seemed to have any strategies in place in December 2011, when mass protests broke out in Moscow prompted by Putin's campaign to return to the presidency. All the FSB could muster was a fax, signed by the chief of the St. Petersburg FSB department, to Pavel Durov, a founder of the Russian social network VKontakte, requiring him to neutralize the websites of protest groups. Durov refused.

On March 27, 2012, this failure to find the means to deal with protesters' activities on social networks was admitted by the first deputy director of the FSB, Sergei Smirnov. At a meeting of the regional anti-terrorist group operating within the Shanghai Cooperation Organization—a broad group of nations that includes most CSTO states as well as China—Smirnov referred directly to the challenge posed by the Arab Spring. "New technologies {are being} used by Western special services to create and maintain a level of continual tension in society with serious intentions extending even to regime change. … Our elections, especially the presidential election and the situation in the preceding period, revealed the potential of the blogosphere." Smirnov stated that it was essential to develop ways to react to such technologies and confessed that "this has not yet happened."

The Kremlin's goal was to use any available type of regional security alliance to build a system of regional cybersecurity—a plausible pretext to help Central Asian states protect themselves and Russia from the fallout of Arab Spring movements. The Russian secret services launched several programs to control what's published on the Internet. The FSB, the Interior Ministry, the Foreign Intelligence SVR, and the Investigative Committee (the Russian analog of the FBI) have new software systems to monitor social networks and identify partici-

pants in online debates. But apparently it's the FSB's Center for Information Security that has taken the lead in policing what Russians are allowed to read and write.

A gloomy, monumental building on the corner of Lubyanka Square and Myasnitskaya Street houses the FSB's counter-intelligence department. This looming fortress, built in the 1980s as the KGB's IT Center, forms a part of a row of buildings, known as the Lubyanka, where thousands of dissidents were imprisoned and interrogated back in the days of the feared Lavrentiy Beria, Stalin's hated spymaster. Initially the Center was responsible for protecting computer networks and tracking down hackers, but in the late 2000s, it was tasked with monitoring social networks and the Internet as a whole.

The Commonwealth of Independent States (CIS), a regional organization made up of nine former Soviet states, uses special analytical search systems developed by Russian programmers. Called "Semantic Archive," the system is produced by the Russian firm Analytic Business Solutions. On the first floor of the Stalin-era yellow brick building, more than 20 programmers headed by 37-year old Denis Shatrov are busy updating Semantic Archive. Not long after the release of the first version in 2004, it was installed in the Russian Security Council and Ministry of Defense headquarters, as well as the FSB and the Interior Ministry. "From the beginning we aimed our systems at the security services," says Denis Shatrov, a trained programmer who founded the company in 2004. "We thought that if we worked with them, then we would also attract business from our intelligence services and those of our competitors too." Shatrov told us that he began developing analytic systems in the mid-90s with his father, the director of a factory that produced automated steering systems for spacecraft. Then they began to produce simulation systems—for electoral and economic applications. Their success came in 1999 when they sold their product to the Ukrainian President Kuchma's situation room for use in his successful campaign for a second term. In the mid-2000s father and son separated, the elder Shatrov specializing in economic modeling, Denis in media analysis.

The idea of its most popular product, Semantic Archive, is to monitor any sorts of open data—media archives, online sources, blogs, and social networks—for key words and then to produce analyses, most famously, by building charts of connections. As it boasts on the company's own website, "the system uses this raw information to extract objects of interest (certain persons, organizations, corporate brands, regions, etc.), their actions and relationships."

SINCE LAST NOVEMBER, HUNDREDS OF WEBSITES HAVE BEEN BANNED FROM THE RUSSIAN INTERNET.

Semantic Archive is not the only product used by the Russian security services to monitor social networks, but all of them seem to share the same fundamental flaw. These systems were developed for searching structured computer files, or databases, and only afterwards adapted, some more successfully than others, for semantic analysis of the Internet. Most of these systems were designed to work with open sources and are incapable of monitoring closed accounts such as Facebook.

The FSB discovered early on that the only way to deal with the problem was to turn to SORM. The licenses require busi-

nesses that rent out site space on servers to give the security services access to these servers via SORM, without informing site owners. With this provision, the FSB has had few problems monitoring closed groups and accounts on Russian social networks Vkontakte and Odnoklassniki. But Facebook and Twitter are not hosted in Russia and that has posed a real challenge for surveillance.

## FILTERING

In November 2012, Russia acquired a nationwide system of Internet-filtering. The principle of Internet censorship wasn't new to Russian authorities. Since 2007, regional prosecutors have implemented court decisions requiring Internet providers to block access to banned sites accused of extremism. But this had not been done systematically. Sites blocked in one region remained accessible in others. The Single Register, officially introduced on November 1, 2012, aimed to solve this problem. Three government agencies—the Roskomnadzor, the Federal Anti-Drug Agency, and the Federal Service for the Supervision of Consumer Rights and Public Welfare—submit data for the government's black list of sites. Service providers are then required to block access to each such site within 24 hours.

Since last November, hundreds of websites have been banned from the Russian Internet. The list ranges from the lighthearted Australian viral YouTube hit "Dumb Ways to Die" to Absurdopedia (the Russian version of Uncyclopedia). Even the parody web site Gospoisk (gossearch.ru) was blocked. The site was a fake search engine, ostensibly created with government support, structured so that when a visitor types a query in the search box, he is asked to enter his first and last name, patronymic, passport details, address, and the reason for the request. Since it was a parody, this data evaporated into the ether.

The new Internet monitoring law has had some substantial offline consequences as well. Institutions providing public access to the Internet—schools, libraries, Internet cafés, and even post offices—have been targeted for law enforcement inspections to check for computers containing software that might allow access to banned websites. This problem took on a new urgency, especially in the Muslim-dominated region of the North Caucasus after the appearance of a YouTube video in September 2012 called The Real Life of Muhammad that was viewed as a direct insult to the Prophet Muhammad. Russian authorities promptly blocked the entire website in some regions. That made global Internet service providers much more cooperative with Russian requests. Google removed the video from YouTube on December 26. Then Twitter blocked an account that promoted drugs on March 15 and on March 29. Facebook took down a page called Club Suicide rather than see the entire network blacklisted by the Russians.

The apparent readiness of global services to cooperate with the Russian government seems to provoke the authorities to push increasingly in the Chinese direction, especially in dealing with social networks. Moscow is attempting to force international social networking companies into Russia's national jurisdiction.

Then, right on time, Edward Snowden appeared on the world stage. The NSA scandal made a perfect excuse for the Russian authorities to launch a campaign to bring global web platforms such as Gmail and Facebook under Russian law—either requiring them to be accessible in Russia by the domain extension .ru, or obliging

them to be hosted on Russian territory. Under Russian control, these companies and their Russian users could protect their data from U.S. government surveillance and, most importantly, be completely transparent for Russian secret services.

Russia wants to shift supervision and control of the Internet from global companies to local or national authorities, allowing the FSB more authority and latitude to thwart penetration from outside. At December's International Telecommunications Union (ITU) conference in Dubai, Moscow tried to win over other countries to its plan for a new system of control. The key to the project is to hand off the functions of managing distribution of domain names/IP-addresses from the U.S.-based organization ICANN to an international organization such as the ITU, where Russia can play a central role. Russia also proposed limiting the right of access to the Internet in such cases where "telecommunication services are used for the purpose of interfering in the internal affairs or undermining the sovereignty, national security, territorial integrity, and public safety of other states, or to divulge information of a sensitive nature." Some 89 countries voted for the Russian proposals, but not the United States, United Kingdom, Western Europe, Australia, or Canada. The result is a stalemate.

Web services would be required to build backdoors for the Russian secret services to access what's stored there. Prominent Russian MP Sergei Zheleznyak, a member of the ruling United Russia party, has called on Russia to reclaim its "digital sovereignty" and wean its citizens off foreign websites. He said he would introduce legislation this fall to create a "national server," which analysts say would require foreign websites to register on Russian territory, thus giving the Kremlin's own security services the access they have long been seeking. Of course, building such a national system would defeat the global value of the Internet.

## BEYOND RUSSIAN BORDERS

Fearing Arab Spring-style uprisings, former Soviet republics have looked to Moscow for guidance on dealing with free speech in cyberspace. On June 15, 2011 Nursultan Nazarbayev, president of Kazakhstan, proposed the idea of an alliance-wide cyber police force at the opening of the Shanghai Cooperation Organization summit in Astana. He added that it was time to include the concept of "electronic borders" and "e-sovereignty" in international law.

> SOON WE WILL END UP WITH A BALKANIZATION OF WHAT WAS ONCE A GLOBAL INTERNET, REPLACED BY A COLLECTION OF NATIONAL OR REGIONAL INTERNETS.

Ten months later, at a second SCO summit, member states agreed on joint measures to be taken by their secret services to "prevent and disrupt the usage of the Internet for terrorist, separatist, and extremist purposes." In turn, the Collective Security Treaty Organization of the CIS countries established a working group on information security and launched a series of joint operations by secret services of member-states. The operation was called PROKSI, and Nikolai Bordyuzha, secretary general of the CSTO, reported that it has led to the shutdown of 216 websites in Russia alone. But the leaders of these countries clearly understand that censorship and Internet-filtering should

be combined with surveillance. After all, they share the same Soviet legacy. When the Soviet Union collapsed, the KGB's regional branches became the security services of the newly independent states. But they retained the KGB's operational DNA, which is apparent in the CIS states' continued use of Soviet and Russian terminology for surveillance operations. The term ORM, or Operative-Investigative Measures, was kept by all CIS countries. At the same time, the Russian approach to "lawful interception" has been adopted in Belarus, Ukraine, Uzbekistan, Kyrgyzstan, and Kazakhstan. And over the last three years Belarus, Ukraine, and Kyrgyzstan have all updated their national interception systems, modeled after the Russian SORM.

In March 2010, Belarusian president Alexander Lukashenko introduced SORM into his country. Two years later, the national telecom operator Beltelecom installed SORM on its data network. In late 2010, Ukraine updated its national requirements for SORM equipment. And in August 2012, Kyrgyzstan updated its network to make it virtually identical to the Russian interception system—in all, bringing tens of millions of new individuals under potential surveillance by security services.

Meanwhile, the export of Russian surveillance procedures and equipment in many cases also means exporting Russian technology, giving homegrown manufacturers natural advantages over their Western counterparts. This, in turn, has led to the growing presence of Russian advisers. SORM is also not the only surveillance technology imported from Russia to the other CIS countries. The Semantic Archive, the favorite technology of monitoring social networks, was installed in Ukraine, Belarus, and Kazakhstan—much to the delight, and profit, of Denis Shatrov.

The further localization of the Internet is likely. Soon, we will end up with a Balkanization of what was once a global internet, replaced by a collection of national or regional internets. Local security services will sell their various surveillance technologies and strategies. Governments will be delighted to extract more controls, with the global Internet services themselves being driven in the same direction of increased fragmentation by the very logic of the advertising business which requires ever finer targeting and accountability of their audience. Russian customers are led to google.ru, not because it's established by the Kremlin or the FSB, but because Google can target ads with more precision. In the future, however, it could be the FSB directing your Internet travels.

Today, global Internet platforms are rightly considered public services, and for the benefit of the public or its institutions. To keep web services and products, not to mention the information they carry, both transparent and global, companies and countries need to resist pressure to fragment the Internet.

The World Wide Web must keep its first W. It is in the interest of all those trying to spread the ideas of democracy around the world. ●