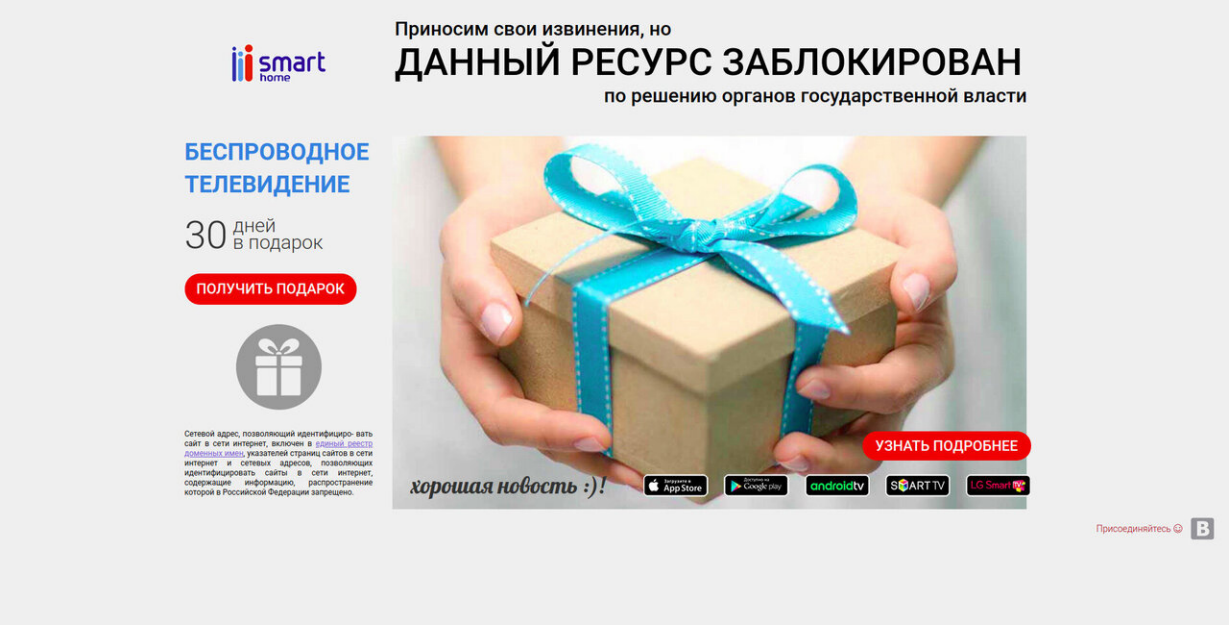
Study: Russia's web-censoring tool sets pace for imitators

November 6 2019, by Tami Abdollah



This screen grab from the website deny.smartpb.net and provided by Censored Planet, a lab at the University of Michigan, shows the website is blocked in Russia. A study by University of Michigan researchers shows Russia is succeeding in imposing a highly effective internet censorship regime across thousands of disparate, privately owned providers in an effort also aimed at making government snooping pervasive. The website address "deny.smartpb.net" translated to English states, "We apologize, but this resource is blocked by decision of state authorities." The provider includes an ad for wireless television and 30-days free as a gift. (Censored Planet via AP)

Russia is succeeding in imposing a highly effective internet censorship regime across thousands of disparate, privately owned providers in an effort also aimed at making government snooping pervasive, according to a study released Wednesday.

The study by University of Michigan researchers says the model can be easily exported to other nations, and it challenges the notion that decentralized internet service can prevent large-scale censorship of the types imposed by Iran and China.

"What this study shows is that Russia has created a blueprint for censoring the internet on top of a network of internet service providers that is very much like the networks found in Western democracies," said J. Alex Halderman, a leading computer scientist at the university who was not involved in the study. "As other governments decide to crack down on the free flow of information online, they may follow Russia's game plan."

Seven years of publicly available data reviewed by the researchers, who call their lab Censored Planet, attests to the Russian government's increasing success at getting privately owned internet providers to block online addresses used by critics of President Vladimir Putin and independent news outlets.

Previously, Censored Planet's discovery of efforts by Kazakhstan's government to surveil internet traffic led Mozilla, Apple and Google to add protections to their browsers. Its latest study comes as a new Russian law formalizes Kremlin censorship and seeks to further tighten information control.

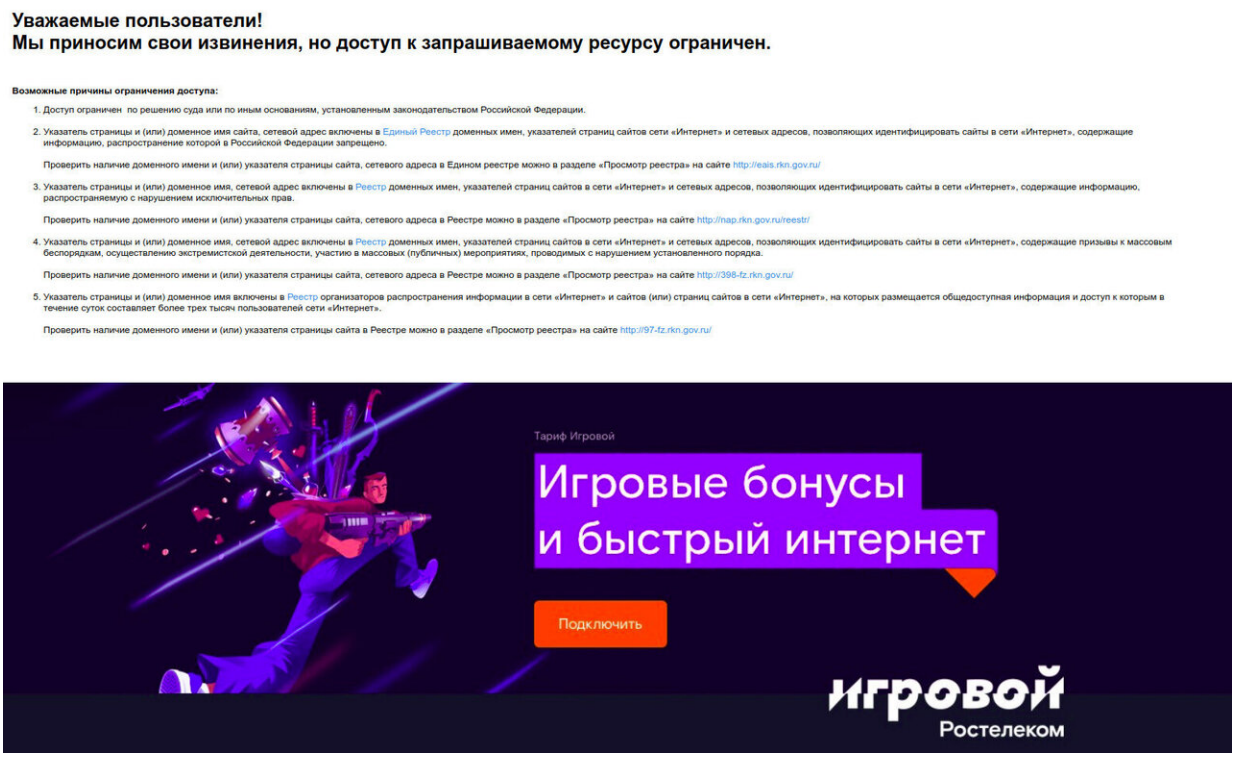
Under the law, devices known as "middleboxes" that surgically filter web content are required, and the state will buy the deep-packet inspection technology and provide it to the internet service providers, effectively

assuming direct control over internet traffic. The boxes must be configured so that the Kremlin can access and manage internet traffic.

"When the government controls this filtering equipment they can do anything, and civil society can't scrutinize it. In China and Iran people don't know what's being blocked," said Alexander Isavnin, who lives in Moscow and works with Russia's Internet Protection Society, a nongovernmental organization. He previously worked at a Russian internet service provider for more than 15 years.

Artyom Kozlyuk, founder of the Roskosvoboda online free speech group, said authorities could use the new law, which took effect Nov. 1, to stifle dissent.

"It gives the government new instruments that would allow it to limit internet traffic the authorities view as negative," he said in remarks published in the independent newspaper Novaya Gazeta.



This screen grab from website warning.rt.ru and provided by Censored Planet, a lab at the University of Michigan shows the website is blocked in Russia. A study by University of Michigan researchers shows Russia is succeeding in imposing a highly effective internet censorship regime across thousands of disparate, privately owned providers in an effort also aimed at making government snooping pervasive. The website address warning.rt.ru, when translated to English, tells users "We apologize, but access to the requested resource is limited." The page notes that "access is restricted by court order or on other grounds established by the legislation of the Russian Federation." (Censored Planet via AP)

Kozlyuk said the law gives Russia's state communications regulator, Roskomnadzor, broad powers to control the internet.

"If mass protests erupt in some regions, we may see shutdowns of mobile

internet, or even entire internet access," Kozlyuk said.

Russian media have reported that it may take another year to install the deep-packet inspection equipment needed to implement the new "sovereign internet" law. Experts predict diminished internet quality in Russia.

The use of "middleboxes" has grown globally. Much of the equipment is sold by U.S. companies like Cisco Systems, Inc. and Procera Networks, Inc. Other providers include Russia's EcoFilter and VAS Experts, China's Huawei Technologies Co., Ltd., and Israel's Allot Communications, Ltd.

Censored Planet founder Roya Ensafi, a University of Michigan computer scientist, said the boxes can be found for as little as $8,000. The technology is often used, especially in the United States, by telecoms and businesses for analyzing online customer behavior and protecting users from phishing attacks.

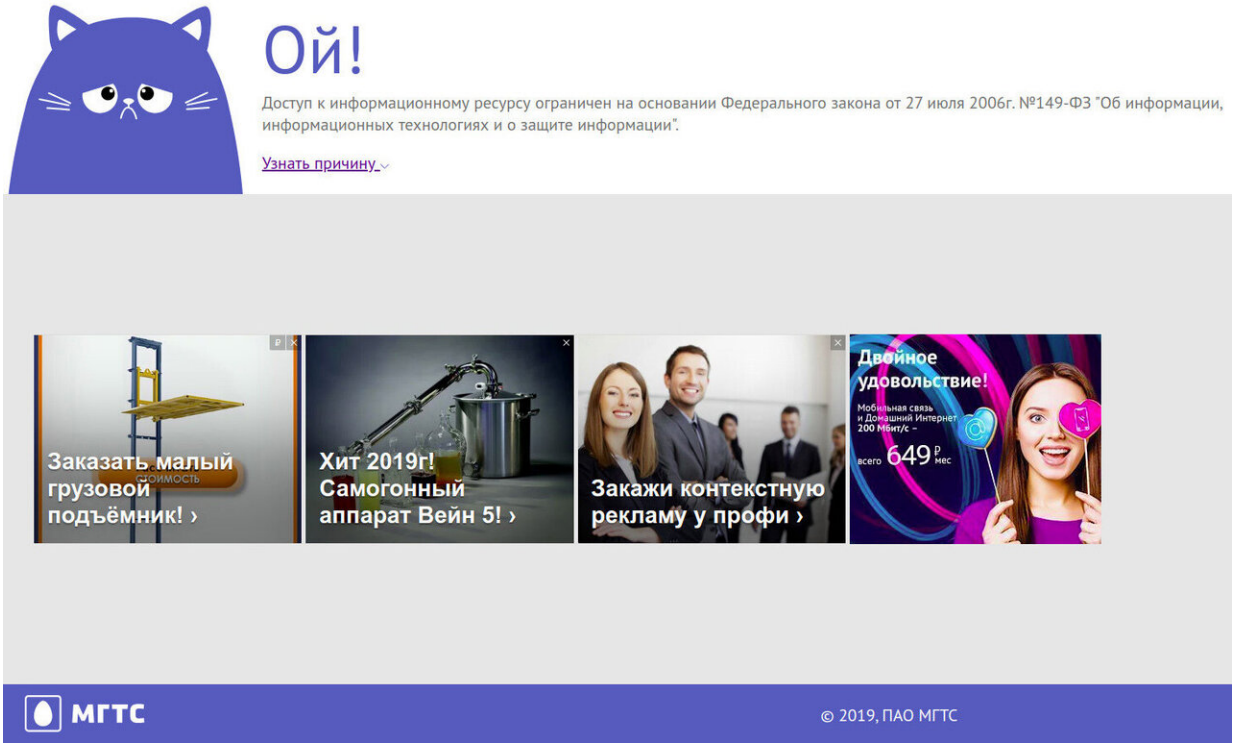
Deep-packet inspection is a dual-use technology that can be used beneficially for security purposes but also abused for population-scale information-access control, Halderman said.

Under Putin, the Russian state has been steadily tightening censorship against what the government calls "external threats." It has tried to block the messaging service Telegram, which has refused to hand over users' encrypted messages in defiance of a court order.

That effort caused unintended blockages, temporarily knocking offline unrelated apps—including Volvo car repair services—leading the Kremlin to pause that effort.

The study released Wednesday, aided by on-the-ground activists in

Russia, reviewed seven years of content blocking by internet providers, who daily are given an updated copy of a centralized blocklist maintained by Roskomnadzor. By April 2019, the list had grown to 132,798 internet domains, roughly 63% in Russian and 28% in English.



This screen grab from website blocked.mgts.ru and provided by Censored Planet, a lab at the University of Michigan shows the page blocked in Russia. A study by University of Michigan researchers shows Russia is succeeding in imposing a highly effective internet censorship regime across thousands of disparate, privately owned providers in an effort also aimed at making government snooping pervasive. The website address "blocked.mgts.ru" when translated to English, states "Oh! Access to the information resource is limited on the basis of the Federal Law." Below are ads, including for a dating site and moonshine. (Censored Planet via AP)

Virtual private network technology that can hide users' web activity from their internet provider is used globally to circumvent such blocking, though Russian law requires domestic VPNs to connect to the regulated network.

Plenty of VPN apps continue to allow Russians to circumvent the censorship, according to Valentin Weber, an Oxford University researcher who recently authored a study on efforts by the Russian and Chinese states to control information online.

The website blocking is transparent. Internet providers even notify customers when a site is blocked by government order. In many cases, those pages now also carry ads, Ensafi said.

Weber said the deep-packet inspection technology used by the middleboxes "increases not only your ability to filter and do censorship but to do increased surveillance capabilities."

Ensafi said she is worried about other countries—she named India, Indonesia, Portugal and Britain—with decentralized internet service adopting the same technology. Russian-sold filtering equipment is already deployed in former Soviet republics like Belarus and Ukraine and farther afield in Algeria, Cuba and Mexico, according to the Oxford study.

Britain uses a similar "censorship architecture," with the government asking internet providers to block child sexual abuse, which is primarily done using deep-packet inspection technology.

"It would only be a matter of programming to repurpose it to block other kinds of content," Halderman said.

In the U.S., meanwhile, the repeal of net neutrality allows internet

service providers to favor certain content over others—the same technical starting point for the use of deep-packet inspection in Russia and what has since allowed the jump to greater censorship there, the report says.

Isavnin said the trend in Russia should be a wake-up call for engineers, hardware and software developers at internet service providers who often prefer to stay in their geeky world and not get into politics.

"You cannot be just an engineer," he said. "You have to understand the consequences of what you're doing in the real world."