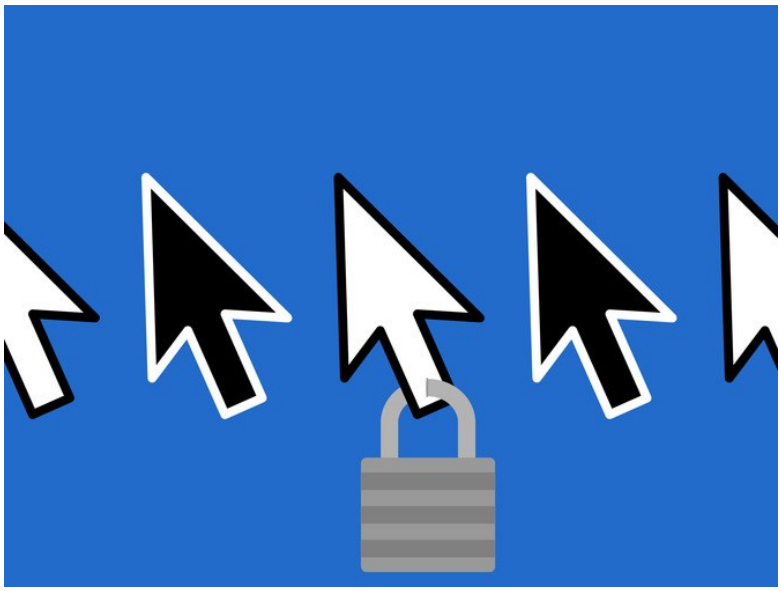
LILY HAY NEWMAN SECURITY 08.04.17 10:00 AM

THE ATTACK ON GLOBAL PRIVACY LEAVES FEW PLACES TO TURN



HOTLITTLEPOTATO

DIGITAL PRIVACY HAS had a very bad summer. As China and Russia move to block virtual private network services, well over a billion people face losing their best chance at circumventing censorship laws. First, China asked telecom companies to start blocking user access to VPNs that didn't pass government muster by next February. More recently, Russian president Vladimir Putin signed a law to ban VPNs and other anonymous browsing tools that undermine government censorship.

As citizens of these countries and people around the world scramble to understand the repercussions, US-based companies that operate in the countries have been swept up in the controversy. Apple complied with a Chinese government order to remove VPNs from its Chinese iOS AppStore, and the company that runs Amazon's cloud services in China this week said it would no longer support VPN use. Even hotels around China that offered VPN services to foreign visitors are largely curtailing the practice.

China and Russia's recent actions aren't new movements toward censorship, but they are escalations. And they leave citizens with few viable options for accessing the open internet.

Crackdown

While the suppressive efforts share the same end goal, they do take different forms. China has laid the foundation for its "Great Firewall" for more than two decades, attempting to control citizens' internet access on a very large scale. Creating and upgrading such a system over time takes massive resources. While Putin has praised the approach, Russia doesn't have a comparable apparatus. Instead, since about 2012, the

legal force more than technical control.

"These crackdowns and ratcheting up of internet censorship in China tend to ebb and flow, and so it is possible that eventually we may see VPNs sort of silently reappear," says Eva Galperin, the director of cybersecurity at the Electronic Frontier Foundation. "In Russia what they're doing is they're passing more and more draconian laws that are extremely difficult to implement. The reason for this is it makes sure that at any given time everyone is breaking the law—anyone that the government wants to target and wants to lean on for information is in violation of the law."

RELATED STORIES

EMILY PARKER
Apple Caved to China, Just Like Almost Every Other Tech Giant

JEREMY HSU
Why Apple Is Losing Its Shine in China

JULIA GREENBERG
Netflix May Never Break Into China

Both approaches have made Russia and China insular markets, challenging for international companies to operate in. Apple, which has been accused of hypocrisy for pushing back against government surveillance in the US while complying with VPN takedown requirements in China, worked for years to enter the Chinese market. "We would obviously rather not remove the apps, but like we do in other countries we follow the law wherever we do business," company CEO Tim Cook said in an earnings call on Tuesday. "We strongly believe participating in markets and bringing benefits to customers is in the best interest of the folks there and in other countries as well."

The VPN crackdowns in China and Russia came as no surprise to those who follow digital rights closely. "We expected it at some point, it wasn't like we didn't know where it came from," says Robert Knapp, the CEO of the Romanian VPN provider CyberGhost, which had its app removed from the iOS AppStore in China. "We had seen the Chinese government putting more and more pressure on VPN providers in a technical sense—blocking our IPs, blocking the server infrastructure we were using, detecting traffic from certain sources."

After years of investing in technical control, China now seems focused on experimenting with regulatory enforcement as well. In the Xinjiang region of western China, reports indicate that the government is requiring citizens to install spyware on their smartphones—ostensibly for anti-terrorism initiatives—and is doing random stops to check whether local residents have complied. They have also arrested citizens over conversations in private chatrooms, indicating that the local government may be actively taking advantage of the spyware. "We are extremely alarmed. This is about as far as a nation-state has gone to submit its people to monitoring," Jeremy Malcolm, a senior global policy analyst at EFF, said of the situation in Xinjiang.

content such that is has extensive control of the internet at this point. After the Russian government took broad control of television and media in the early 2000s, the internet was the only place left for free communication. "Now the government is trying to close in on that," says Rachel Denber, the deputy director of the Europe and Central Asia division at Human Rights Watch. "It's the logical progression of things. Once you go down the road of trying to expand state control over online communication, [banning VPNs] would be the next post to hit."

The Russian government may also be reacting to the current geopolitical situation, in which the country has been called out for hacking numerous Western countries, particularly leading up to democratic elections. "The authorities may also be looking ahead to the 2018 [Russian] presidential election, and they might want to take preemptive steps to ensure that no opposition mobilization takes place online," Denber notes.

Circumvention

For now there are still some ways around the Chinese and Russian governments' internet barriers, if you're willing to accept the risk. iPhones can only download apps from the App Store (unless a unit is jailbroken, which is not impossible but technically difficult, and introduces a host of security vulnerabilities). Android phones, though, can still sideload VPN apps from third-party app stores, since users aren't required to get apps from the Play Store. Google doesn't even operate its Play Store in China. For now, it's also easier to download desktop VPNs than mobile ones.

Other anonymizing tools besides VPNs remain a viable option as well, like the Tor Browser. That may carry more risk in Russia, though, given the recent arrest of someone who ran a Tor exit node—a gateway between the service and the internet—for participating in protests. Using Tor Browser in China, meanwhile, requires extensive technical skill, to get around the Great Firewall.

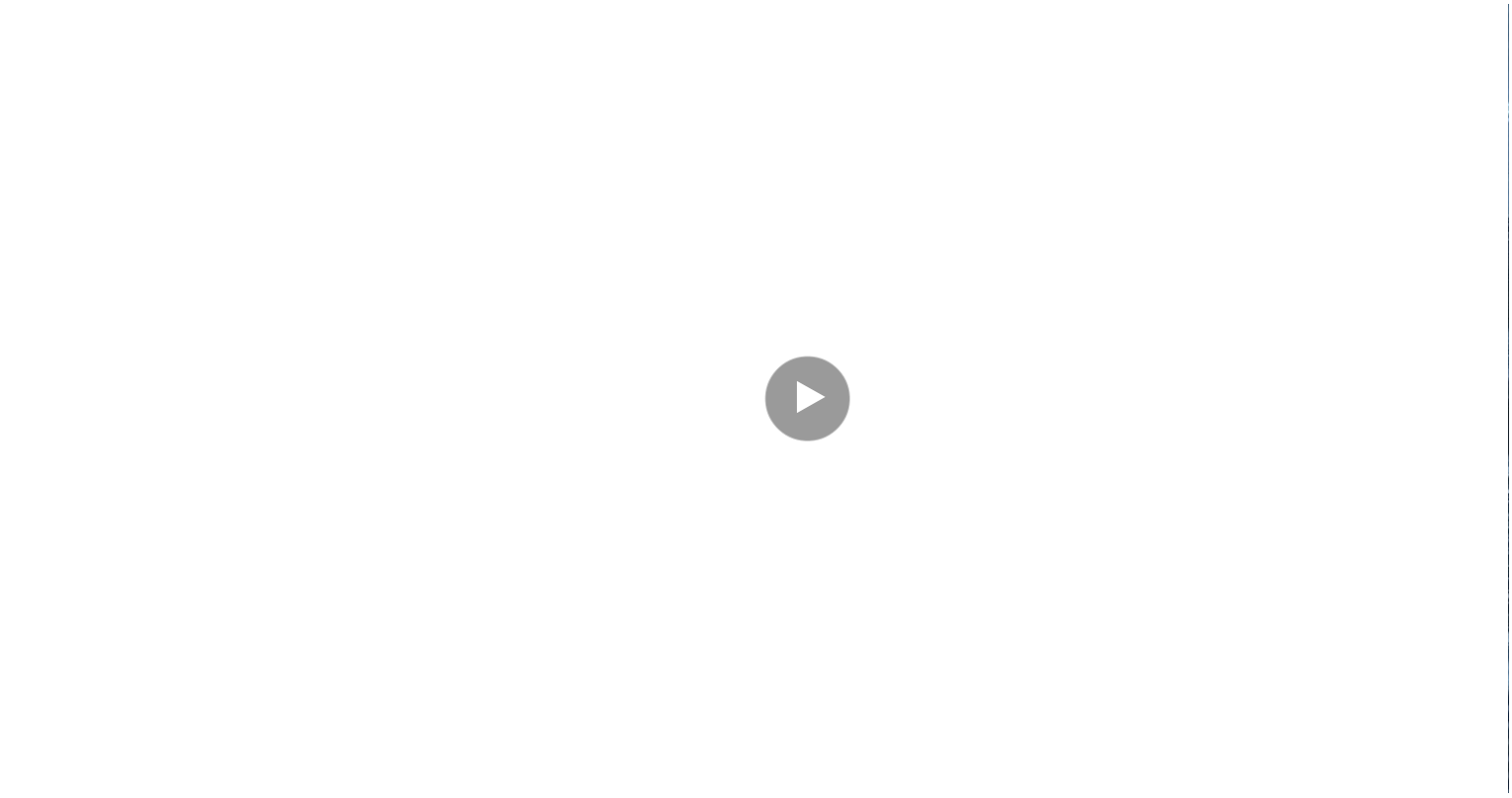
It's also possible to install VPNs on devices while in other countries, and then use them in Russia or China. And end-to-end encrypted messaging services like Signal are a totally separate way of communicating and potentially receiving uncensored information without dealing with VPNs at all.

Experts report that both China and Russia may enact anti-VPN enforcement through checkpoints and arrests to intimidate citizens. "We are still used in Russia, we still count downloads, our Russian community is actually still growing," CyberGhost's Knapp says. "But instead of simply blocking VPN traffic, the Russian government is pulling another string now. They forbid it and they are going to enforce it—maybe brutally enforce it."

There could be unforeseen side effects as well. At the same time that eliminating these tools helps governments expand surveillance and control access to information, banning them also has the potential to degrade countries' overall security posture. Institutions that don't have access to VPNs could be at increased risk of being infiltrated or breached by foreign attackers. And if repressive governments set their sights on encryption next, they could undermine the integrity of basic economic drivers like secure digital transactions.

pursue it regardless may find they lose more than they intended.

RELATED VIDEO



SECURITY

How to Make Your Browsing Data More Private than a Thousand Incognito Windows

Thanks to an assist from Congress, your cable company has the legal right to sell your web-browsing data without your consent. This is how to protect your data from preying eyes.

#CHINA #RUSSIA #VPN

VIEW COMMENTS

SPONSORED STORIES

MORE SECURITY

CYBERSECURITY
All the Ways US Government Cybersecurity Falls Flat
LILY HAY NEWMAN

DON'T PANIC
Your Handy Guide to the Many Tech Anxieties of Our Time

BUSINESS
Sorry, Banning ‘Killer Robots’ Just Isn’t Practical
TOM SIMONITE

SECURITY

Stormfront Nazis Think the 'Alt-Right' Is Full of Idiots

ASHLEY FEINBERG

HACKS

Watch Hackers Hijack Three Robots for Spying and Sabotage

ANDY GREENBERG

FICTION

What if All Your Secrets Went Public?