AMERICAN FOREIGN POLICY COUNCIL

# Russia's 'Data Localization' Efforts May Guide Other Governments

January 13, 2020 **Samuel Bendett**, **Justin Sherman** *DefenseOne*

**Related Categories:** Cybersecurity and Cyberwarfare; Democracy and Governance; Science and Technology; China; Europe; Russia

Cyberspace, as many liberal democratic governments see it, is inherently free and open, a boon to democracy that states should not control. Russia, which does not share this view, worries that information flowing into the country may bring malign foreign influence, while data flowing out may provide leverage to its enemies. So the government is expanding "data localization": rules and infrastructure to help the state keep data on home soil. These efforts will have repercussions far beyond Russia's own borders: they will be closely studied by other authoritarian states keen to adopt new mechanisms of control — and by liberal democracies that may be rethinking their own rejections of the notion of cyber sovereignty.

Fending off foreign influence is a centuries-old obsession of Russia's leaders, who began to formally organize their concerns about the internet in 2000's Information Security Doctrine of the Russian Federation. At the time, the government was already reassembling a Soviet-like control of print and TV media outlets, yet Russian citizens freely used the internet to share their thoughts and concerns with each other and the world.

The Kremlin accelerated its cyber sovereignty push after the 2010-12 Arab Spring, whose popular revolts were abetted by the internet's enabling of online-offline citizen mobilization. In 2014, Russian Foreign Minister Sergei Lavrov decried these and other "color revolutions"; Defense Minister Sergei Shoigu added that such uprisings "are always accompanied by information warfare." In 2018, Russia enacted a (rather easily circumvented) ban on the secure-messaging app Telegram. In 2019, a new domestic internet law allowed tighter regulation. In particular, it laid the legal foundation for the Kremlin's drive to reshape the country's networking infrastructure so it could cut access to the global internet, if and when desired.

The push also includes data localization efforts: requirements that private companies keep data inside Russia. Generally, these are perceived as efforts to increase law enforcement or intelligence services' access to sensitive information held by corporations. Such concerns were raised when Russia demanded that Apple store its users' encryption keys on servers on Russian territory.

But a better way to think of data localization is on a spectrum of severity. For example, companies might be required to locally store only certain types of data, such as payment information. They may be required to locally store only a copy of data sent abroad, a requirement dubbed "mirroring." Or they may be required to provide their services in a way in which no data may leave the country.

These various approaches reflect the differing reasons governments pursue data localization. Perhaps they want to increase law enforcement's access to data. They might want to make it harder for foreign businesses to compete with local ones. (It's often unclear whether this works in specific cases.) Or they might reflect political motivations, governing goals, and principles.

Russia's push for data localization is part of its effort to exert sovereignty over the internet. Its focus to date has been on mirroring.

But its objection to data outflow was on display when the federal media and censorship agency Roskomnadzor discovered late last year that the personal data of a million Russian citizens — including surnames, first names, patronymics, home addresses and phone numbers — was stored on the France-registered website *nomerekaterinburga.com*. On Dec. 17, state media reported that the site had been "included in the register of violators of the rights of subjects of personal data" and that "in the future, access to it will be limited."

This concern may also reflect growing popular concern about personal data. Today's Russian youth—the slice of the population that makes the most use of internet and mobile technologies—are starting to take their personal data seriously. A recent study found that 83 percent of students ages 9 to 17 have a clear understanding of the concept — up from 43 percent a year earlier. The Roskomnadzor study also found that just one-third of students post personal information on social networks, and that half had adjusted privacy settings when using social media.

Overall, the Kremlin's control of the internet is not quite as tight as its sway over television and print media. Aided by the spread of faster, cheaper LTE mobile-networking technology, Russian citizens are downloading and generating content faster than ever before. The Ministry of Communications reports that Russian mobile subscribers downloaded more data in the first nine months of 2019 than in all of 2018. Some is surely information that the government feels should be stored and protected in the country. Yet protests against the domestic internet law underscore some citizen opposition to tight regulation of the web.

Questions that remain to be answered include: how effectively can Russia use economic pressure to force foreign-incorporated companies to comply with data localization rules? Will Russia will tighten its data localization rules, and how? Will Russia work with China to develop cross-border data transfer rules, and how? Will Russian businesses and civil society organizations push back against cyber sovereignty proposals, and how?

One thing is sure: as Russia proceeds with its data-localization efforts, authoritarian and democratic countries alike will be watching.

*Justin Sherman is a Cybersecurity Policy Fellow at New America, a Fellow at the Duke Center on Law & Technology, and a student at Duke University. Full bio*

*Samuel Bendett an Adviser at the CNA Corporation and a member of CNA's Center for Autonomy and AI. He is also a Fellow in Russia Studies at the American Foreign Policy Council. The views expressed here are his own. Full bio*

---