

President Joseph R. Biden Jr.
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

March 10, 2022

Dear President Biden,

The signatories to this letter deplore Russia's invasion of Ukraine, condemn in the strongest possible terms the grave violations committed by Russian forces there, and applaud efforts by the Biden Administration and other governments to respond with strong and targeted measures. However, we write to express our concerns about growing calls to interfere with the Russian people's access to the internet, which we fear will hurt individuals attempting to organize in opposition to the war, report openly and honestly on events in Russia, and access information about what is happening in Ukraine and abroad. These measures could also unnecessarily facilitate further repression by the Russian government.

Some governments, including the U.S. government, may be considering disrupting internet access in Russia through new sanctions. There is also increasing pressure, internally and externally, on information and communications technology vendors like internet, telecommunications, and cloud service providers to voluntarily restrict or block access by users in Russia. Moreover, Ukraine has made repeated requests along these lines.¹

We urge all actors considering steps that would limit internet access in the Russian Federation to carefully consider the full impact of such measures and their possible unintended consequences, and to act in a targeted, open, and strategic manner, consistent with international human rights principles of legality, legitimacy, necessity and proportionality. We also call upon the Treasury Department's Office of Foreign Assets Control (OFAC) to act immediately to protect the free flow of information in Russia through **issuing a General License** authorizing the provision of services, software, and hardware necessary for personal communications over the internet, and robustly clarifying and disseminating notice of this license to relevant stakeholders.

¹ These include requests to the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunication Union, and other bodies.

On Friday March 4, Cogent, one of the largest providers of internet backbone services in Russia, [cut service](#) to customers in the country, citing Russia's unprovoked invasion of Ukraine and U.S. government sanctions. On March 8, Lumen, a second major internet carrier, also [pulled out](#) of Russia. Major U.S.-based software and internet platforms are banning [sales](#) and suspending services to Russia, citing compliance with U.S. sanctions as one reason. These actions and [others](#) by [technology companies](#) to cease sales and cut ties with Russia may be motivated in part by efforts to comply with sanctions that the United States, the European Union, and other governments imposed on Russian persons and entities, actions that we fear foreshadow more onerous restrictions on internet communications in Russia.

It is not clear whether the U.S. government explicitly authorizes the lawful provision of even the most simple internet applications, services, or software in Russia at the moment. However, past U.S. sanctions programs, including those applying to Iran, Cuba, and Syria, have included authorizations for personal communications, software services, software, and hardware offered at cost, based on the recognition that information technologies offer unprecedented opportunities for independent media, person-to-person exchange, and documentation of human rights violations. Through these actions, OFAC and the U.S. government set a precedent: it is within the public interest to ensure that access to digital platforms and modern communication technologies are, and remain, unaffected by sanctions.

These general licenses for personal communications have received wide support from civil society organizations and Congress, and do not contradict the overall objectives of the sanctions programs. Access to the internet is essential to the protection of freedom of expression, access to information, and free association, and is increasingly recognized as a human right. Journalism and independent media depend on access to secure and reliable information technologies to document events inside contested areas, and to enable people to bypass state controls on information. Overly broad restrictions on the access of the Russian people to the internet would further isolate the embattled pro-democracy and anti-war activists, and impede the ability of NGOs, human rights groups, journalists, and attorneys inside and outside Russia to provide critical information to citizens about the current state of affairs and their rights. These actions would inadvertently speed up what the Kremlin has set out to achieve through its "sovereign internet" tools - a complete and total control of information space inside Russia.

Moreover, restricting access to foreign technology and communications platforms could further isolate the region and force users to rely on alternative and available services provided

by Russian companies. These services are highly controlled by Russian authorities and have actively stifled independent channels of information through aggressive censorship and surveillance. In addition, these steps can drive individuals toward unauthorized or pirated versions of software and services that are likely to be vulnerable to hacking and surveillance.

For its part, Russia is likewise ramping up efforts to [block](#), [throttle](#), and [commandeer](#) platforms and providers operating there. It has banned Facebook, Twitter, and over a dozen independent media, and has sent censorship notices to a number of foreign outlets including the Wikimedia Foundation, threatening to block those services within Russia. We should work in every capacity to counteract those authoritarian actions and ensure that sanctions and other steps meant to repudiate the Russian government's illegal actions do not [backfire](#), by reinforcing Putin's efforts to assert information control.

For these reasons, the Biden Administration and like-minded governments seeking to sanction the actions of the Russian Federation and its allies should take the following steps:

- Immediately authorize the provision of services, software, and hardware incident to personal communications over the internet, while providers are still considering compliance strategies, rather than waiting until after individuals in Russia are cut off from these vital services;
- Consult with civil society actors and technology companies to understand the likely ramifications of potential sanctions;
- Ensure that sanctions are implemented in a smart and targeted manner, consistent with international human rights principles, including by providing clear guidance about how sanctions should be implemented in ways that protect human rights and humanitarian initiatives;
- Be transparent about the justifications for and impacts of sanctions, clarify how they are developed, and enable stakeholders to provide evidence on current and potential targets and measures;
- Pledge to regularly review and, if necessary, revise sanctions to ensure that they remain fit-for-purpose, in close consultation with civil society;
- Include clearly articulated guidance about the possibility of sanctions removal and delisting, and the specific factors that will lead to the revision of sanctions; and
- Apply a similar approach to any potential sanctions on Belarus, as its role in the conflict evolves.

Thank you for your consideration of these important points. We are available to discuss and assist with any further efforts along these lines, as appropriate.

Signatories:

Access Now

ARTICLE 19

Azerbaijan Internet Watch

Beam Reports

Center for Democracy & Technology

Committee to Protect Journalists

Dangerous Speech Project/Christchurch Call Advisory Network

Digital Impact and Governance Initiative (DIGI) @ New America

Digital Rights Kashmir

Electronic Frontier Foundation (EFF)

Free Belarus Coalition

Freedom House

Free Press Unlimited

Friends of Angola

Global Forum for Media Development (GFMD)

Global Network Initiative

Guernica 37 Group

Harvard Law School Cyberlaw Clinic at the Berkman Klein Center

Human Rights First

Human Rights Foundation

Human Rights Watch

Index on Censorship

International Senior Lawyers Project (ISLP)

Internet Society

Paradigm Initiative (PIN)

Project Expedite Justice

Manushya Foundation

Mass Media Defence Centre

Media Diversity Institute - Armenia

Media Foundation for West Africa (MFWA)

Miaan Group

Net Freedoms Project

Ranking Digital Rights
RFK Human Rights
RosKomSvoboda
Teplitsa. Technologies for Social Good
US Ukrainian Activists
Wikimedia Foundation
Women of Uganda Network (WOUGNET)
World Wide Web Foundation
Xnet - Spain