

September 16, 2025

The undersigned entities, organizations, and individuals write to express our urgent concerns regarding escalating efforts by Russian authorities to [block access to end-to-end encrypted communication platforms](#), such as WhatsApp, following [last year's blocking of Signal](#). These actions by the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) violate internationally recognized human rights, including the rights to freedom of opinion and expression, access to information, and privacy.

Encrypted services are lifelines, [recognized](#) by the UN and international human rights experts as critical enablers of secure communication and democratic participation. They enable journalists, human rights defenders, activists, and ordinary people to communicate without fear of surveillance, censorship, or retaliation. Eliminating access to these services undermines fundamental rights to privacy and freedom of expression, and threatens the safety of millions of users who rely on encryption for secure communication.

These latest restrictions are part of a broader effort by the Kremlin to enforce “[digital sovereignty](#)” by asserting increasingly inappropriate and excessive authority over the provision of digital services, while simultaneously supporting the development of and reliance on state-controlled platforms. In addition to throttling and blocking global services, the Russian government has [ordered](#) that a government-backed, non-encrypted messenger called [Max](#) be pre-installed on all mobile phones and tablets sold in the country. Integrated with government services and launched by the state-controlled company [VK](#), Max cannot provide the same protections as end-to-end encrypted services.

Similarly, Russia [blocks](#) the use of many virtual private networks (VPNs), tools that provide essential, lawful means for individuals to realize their rights by bypassing censorship and protecting their privacy. Restricting both encrypted communication platforms and VPNs leaves people in Russia with exceedingly few options for secure communication.

In this context, we:

1. Condemn Russia's blocking of end-to-end encrypted messaging applications and the forced pre-installation of unencrypted alternatives that do not confer the same level of protection for privacy and free expression;
2. Reaffirm the critical importance of encryption and VPNs in enabling access to information, facilitating secure communications, and resisting unlawful surveillance.
3. Support efforts by companies, civil society, and multistakeholder initiatives to maintain and expand access to encrypted communication services for people in Russia and around the world.
4. Commit to helping people resist pressures to adopt similarly restrictive measures in other jurisdictions, recognizing the global risks of normalizing such practices.

The blocking of encrypted services in Russia, combined with the mandatory deployment of non-encrypted state-controlled apps, should be understood as part of a wider campaign against human rights, rather than isolated acts of regulation. If unchallenged, these tactics risk setting a dangerous precedent for digital authoritarianism elsewhere. The international community must respond with clarity and resolve: free, private, and secure communication is not a privilege, but a fundamental right that must be protected everywhere.

We stand in solidarity with those in Russia whose voices are being silenced, and will continue to defend encryption, VPNs, and the open internet as essential pillars of freedom in the digital age.

Sincerely,

### **Civil Society Organizations**

Access Now

Advocacy For Principled Action In Government

Africa Rural Internet and STEM Initiative - AFRISTEMI

ARTICLE 19

Chayn

Center for Democracy & Technology

Center for Online Safety and Liberty

Electronic Frontier Foundation (EFF)

Emerald Onion

Encryption Advocates Council

Fight for the Future

Global Network Initiative

Global Partners Digital

Human Rights Journalists Network Nigeria

Index on Censorship

Internet Society Catalan Chapter (ISOC-CAT)

JCA-NET(Japan)

LGBT Tech

Surveillance Technology Oversight Project (S.T.O.P.)

Success Bridge Community Development Foundation

The Tor Project

World Ethical Data Foundation

Zaina Foundation

### **Corporations and Trade Associations**

Nord Security

Proton

Tuta Mail

### **Cybersecurity Experts and Academics\***

Dr. Sanjana Hattotuwa

Dr Jean Linis-Dinco

Dr. Preeti Kamra

Prof. Jordi Domingo-Pascual, *Universitat Politècnica de Catalunya (UPC BarcelonaTECH)*

Riana Pfefferkorn, *Stanford University*

Sofia Celi, *Brave / University of Bristol*

Vyara Savova, *EUCI/UniBit*

*\*Affiliation is indicated for purposes of identification only.*