Russia: Telegram block leads to widespread assault on freedom of expression online

Monday 30 April 2018

We, the undersigned 26 international human rights, media and Internet freedom organisations, strongly condemn the attempts by the Russian Federation to block the Internet messaging service Telegram, which have resulted in extensive violations of freedom of expression and access to information, including mass collateral website blocking.

We call on Russia to stop blocking Telegram and cease its relentless attacks on Internet freedom more broadly. We also call the United Nations (UN), the Council of Europe (CoE), the Organisation for Security and Cooperation in Europe (OSCE), the European Union (EU), the United States and other concerned governments to challenge Russia's actions and uphold the fundamental rights to freedom of expression and privacy online as well as offline. Lastly, we call on Internet companies to resist unfounded and extra-legal orders that violate their users' rights.

Massive Internet disruptions

On 13 April 2018, Moscow's Tagansky District Court granted Roskomnadzor, Russia's communications regulator, its request to block access to Telegram on the grounds that the company had not complied with a 2017 order to provide decryption keys to the Russian Federal Security Service (FSB). Since then, the actions taken by the Russian authorities to restrict access to Telegram have caused mass Internet disruption, including:

- Between 16-18 April 2018, almost 20 million Internet Protocol (IP) addresses were ordered to be blocked by Roskomnadzor as it attempted to restrict access to Telegram. The majority of the blocked addresses are owned by international Internet companies, including Google, Amazon and Microsoft. Currently 14.6 remain blocked.
- This mass blocking of IP addresses has had a detrimental effect on a wide range of web-based services that have nothing to do with Telegram, including, but not limited to, online banking and booking sites, shopping, and flight reservations.
- Agora, the human rights and legal group, representing Telegram in Russia, has reported it has received requests for assistance with issues arising from the mass blocking from about 60 companies, including online stores, delivery services, and software developers.
- At least six online media outlets (Petersburg Diary, Coda Story, FlashNord, FlashSiberia, Tayga.info, and 7x7) found access to their websites was temporarily blocked.
- On 17 April 2018, Roskomnadzor requested that Google and Apple remove access to the Telegram app from their App stores, despite having no basis in Russian law to make this request. The app remains available, but Telegram has not been able to provide upgrades that would allow better proxy access for users.
- Virtual Private Network (VPN) providers – such as TgVPN, Le VPN and VeeSecurity proxy - have also been targeted for providing alternative means to access Telegram. Federal Law 276-FZ bans VPNs and Internet anonymisers from providing access to websites banned in Russia and authorises Roskomnadzor to order the blocking of any site explaining how to use these services.

Background on restrictive Internet laws

Over the past six years, Russia has adopted a huge raft of laws restricting freedom of expression and the right to privacy online. These include the creation in 2012 of a blacklist of Internet websites, managed by Roskomnadzor, and the incremental extension of the grounds upon which websites can be blocked, including without a court order.

The 2016 so-called 'Yarovaya Law', justified on the grounds of "countering extremism", requires all communications providers and Internet operators to store metadata about their users' communications activities, to disclose decryption keys at the security services' request, and to use only encryption methods approved by the Russian government - in practical terms, to create a backdoor for Russia's security agents to access internet users' data, traffic, and communications.

In October 2017, a magistrate found Telegram guilty of an administrative offense for failing to provide decryption keys to the Russian authorities – which the company states it cannot do due to Telegram's use of end-to-end encryption. The company was fined 800,000 rubles (approx. 11,000 EUR). Telegram lost an appeal against the

administrative charge in March 2018, giving the Russian authorities formal grounds to block Telegram in Russia, under Article 15.4 of the Federal Law "On Information, Information Technologies and Information Protection".

The Russian authorities' latest move against Telegram demonstrates the serious implications for people's freedom of expression and right to privacy online in Russia and worldwide:

- For Russian users apps such as Telegram and similar services that seek to provide secure communications are crucial users' safety. They provide an important source of information on critical issues of politics, economics and social life, free of undue government interference. For media outlets and journalists based in and outside Russia, Telegram serves not only as a messaging platform for secure communication with sources, but also as a publishing venue. Through its channels, Telegram acts as a carrier and distributor of content for entire media outlets as well as for individual journalists and bloggers. In light of the direct and indirect control the state has over many traditional Russian media and the self-censorship many other media outlets feel compelled to exercise, instant messaging channels like Telegram have become a crucial means of disseminating ideas and opinions.

- Companies that comply with the requirements of the 'Yarovaya Law' by allowing the government a back-door key to their services jeopardize the security of the online communications of their Russian users and the people they communicate with abroad. Journalists, in particular, fear that providing the FSB with access to their communications would jeopardize their sources, a cornerstone of press freedom. Company compliance would also signal that communication services providers are willing to compromise their encryption standards and put the privacy and security of *all* their users at risk, as a cost of doing business.

- Beginning in July 2018, other articles of the 'Yarovaya Law' will come into force requiring companies to store the content of *all* communications for six months and to make them accessible to the security services without a court order. This would affect the communications of both people in Russia and abroad.

Such attempts by the Russian authorities to control online communications and invade privacy go far beyond what can be considered necessary and proportionate to countering terrorism and violate international law.

International Standards

- Blocking websites or apps is an extreme measure, analogous to banning a newspaper or revoking the license of a TV station. As such, it is highly likely to constitute a disproportionate interference with freedom of expression and media freedom in the vast majority of cases, and must be subject to strict scrutiny. At a minimum, any blocking measures should be clearly laid down by law and require the courts to examine whether the wholesale blocking of access to an online service is necessary and in line with the criteria established and applied by the European Court of Human Rights. Blocking Telegram and the accompanying actions clearly do not meet this standard.

- Various requirements of the 'Yarovaya Law' are plainly incompatible with international standards on encryption and anonymity as set out in the 2015 report of the UN Special Rapporteur on Freedom of Expression report (A/HRC/29/32). The UN Special Rapporteur himself has written to the Russian government raising serious concerns that the 'Yarovaya Law' unduly restricts the rights to freedom of expression and privacy online. In the European Union, the Court of Justice has ruled that similar data retention obligations were incompatible with the EU Charter of Fundamental Rights. Although the European Court of Human Rights has not yet ruled on the compatibility of the Russian provisions for the disclosure of decryption keys with the European Convention on Human Rights, it has found that Russia's legal framework governing interception of communications does not provide adequate and effective guarantees against the arbitrariness and the risk of abuse inherent in any system of secret surveillance.

We, the undersigned organisations, call on:

- **The Russian authorities to** guarantee internet users' right to publish and browse anonymously and ensure that any restrictions to online anonymity are subject to requirements of a court order, and comply fully with Articles 17 and 19(3) of the ICCPR, and articles 8 and 10 of the European Convention on Human Rights, by:
    - Desisting from blocking Telegram and refraining from requiring messaging services, such as Telegram, to provide decryption keys in order to access users private communications;

- Repealing provisions in the 'Yarovaya Law' requiring Internet Service Providers (ISPs) to store all telecommunications data for six months and imposing mandatory cryptographic backdoors, and the 2014 Data Localisation law, which grant security service easy access to users' data without sufficient safeguards.
- Repealing Federal Law 241-FZ, which bans anonymity for users of online messaging applications; and Law 276-FZ which prohibits VPNs and Internet anonymisers from providing access to websites banned in Russia;
- Amending Federal Law 149-FZ "On Information, IT Technologies and Protection of Information" so that the process of blocking websites meets international standards. Any decision to block access to a website or app should be undertaken by an independent court and be limited by requirements of necessity and proportionality for a legitimate aim. In considering whether to grant a blocking order, the court or other independent body authorised to issue such an order should consider its impact on lawful content and what technology may be used to prevent over-blocking.

- **Representatives of the United Nations (UN), the Council of Europe (CoE), the Organisation for the Cooperation and Security in Europe (OSCE), the European Union (EU) the United States and other concerned governments** to scrutinise and publicly challenge Russia's actions in order to uphold the fundamental rights to freedom of expression and privacy both online and-offline, as stipulated in binding international agreements to which Russia is a party.

- **Internet companies to resist** orders that violate international human rights law**.** Companies should follow the United Nations' Guiding Principles on Business & Human Rights, which emphasise that the responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located and exists independently of whether the State meets its own human rights obligations.

Signed by

1. **ARTICLE 19**
2. **Agora International**
3. **Access Now**
4. **Amnesty International**
5. **Asociatia pentru Tehnologie si Internet – ApTI**
6. **Associação D3 - Defesa dos Direitos Digitais**
7. **Committee to Protect Journalists**
8. **Civil Rights Defenders**
9. **Electronic Frontier Foundation**
10. **Electronic Frontier Norway**
11. **Electronic Privacy Information Centre (EPIC)**
12. **Freedom House**
13. **Human Rights House Foundation**
14. **Human Rights Watch**
15. **Index on Censorship**
16. **International Media Support**
17. **International Partnership for Human Rights**
18. **ISOC Bulgaria**
19. **Open Media**
20. **Open Rights Group**
21. **PEN America**
22. **PEN International**
23. **Privacy International**
24. **Reporters without Borders**
25. **WWW Foundation**
26. **Xnet**