December 8, 2021

Pavel Durov
CEO and Co-Founder
Telegram

Dear Mr. Durov,

Access Now, an international human rights organization with a mission to defend and extend the rights of users at risk in the digital age, and the undersigned organizations, are writing to you to bring your attention to the safety and security issues related to Telegram, and provide recommendations to ensure the human rights of people who use your platform are protected.

Today, over 500 million users around the world rely on Telegram for their personal and professional lives. Thanks to its unique features, human rights defenders, bloggers, journalists, and other users in Russia, Iran, Belarus, Hong Kong, and beyond have been extensively relying on Telegram chat groups and news channels to organize and share information, despite their governments' brutal crackdowns, censorship, and internet shutdowns.

While Telegram protects voices that governments seek to silence, and offers a space for dissenters and vulnerable communities to organize and support each other, challenges remain around the reliability and verification of information, digital security, and content moderation, given clear instances of abuse and manipulation. Civil society and affected individuals have long been struggling in their efforts to remain safe and pursue accountability on the platform.

Recommendations

In June 2021, RightsCon, a leading annual summit on human rights in the digital age, held a session dedicated to sharing insights and challenges experienced by the communities who rely on Telegram to exercise their rights to freedom of expression and peaceful assembly. Together with the audience, the panel, which consisted of an activist from Hong Kong, independent media editor from Belarus, and an Iranian-American scholar, took stock of successful strategies that could ensure that Telegram protects the rights of its users.

The issues and strategies identified resonated with the civil society, academia, and digital security experts' concerns beyond the RightsCon panel, and were formulated as the following recommendations:

1. ***Design and implement clear and transparent policies and procedures***

Robust access to social media platforms, such as Telegram, is a prerequisite for individuals to exercise their rights, including freedom of expression, access to information, and freedom of association, in the digital age. Retaining dossiers of customers' personal data, social media platforms impact the right to privacy in many ways, including through potential security breaches, or third-party transfer of user

data. To mitigate such human rights impacts, the United Nations Guiding Principles on Human Rights (UNGPs) and OECD Guidelines require companies to develop human rights and due diligence policies to protect the rights of their customers and other affected individuals.

However, based on the feedback of its most vulnerable users, Telegram has not been taking these risks and responsibilities seriously enough. Instead of developing a robust human rights compliance framework and clear policies, Telegram has been seemingly operating and making decisions affecting millions based on opaque and arbitrary decisions. Telegram's definitions of illegal content or clarification of circumstances under which the platform would share data with the government are scarce, and can be deciphered only by reading interviews with yourself, or your personal or social media posts. It is notable that Telegram has often stood up for human rights, and as co-founder, you have made many statements in this regard. However, these pledges do not substitute meaningful policy. The absence of robust and unambiguous rules results in confusion and rumors about the company's ties to authoritarian governments and fuels speculations about the potential or actual blockings of Telegram channels that occasionally appear in the news.

For example, the decision of Telegram to suspend the "Smart Voting" chatbot during the 2021 Russian State Duma elections failed to provide predictability and transparency. Even after the publication of Telegram's official statement and press conference on this incident, it is still unclear what the exact grounds for such censorship were: the threat of Apple and Google's removal of Telegram from the country's app store or Telegram's own policy related to political campaigning during elections. This arbitrary decision making only heightens concerns of users at risk in other countries, including Belarus, where more than 200 independent Telegram channels are declared as extremist and ordered to be blocked, based on the Russian precedent.

Telegram must build a robust human rights policy, due diligence policies, and a participatory, clear, transparent and multistakeholder content governance framework. All content moderation rules, sanctions, and exceptions should be (i) made in a clear, specific, and predictable way, (ii) properly communicated to users in advance; and (iii) appealable by users affected. The company should enable meaningful participation of users at different stages of the creation, implementation, and evaluation of its rules and policies.

Telegram must also issue a regular Transparency Report, disclosing comprehensive information on all restrictions to the free and open flow of information and all requests for content and account restrictions, whether issued by public or private parties, trusted flaggers, automated tools, or as a result of the enforcement of its own policies. This information should be accompanied with reasons for determining the legality of content or how it infringes the platform's terms of service. Furthermore, transparency reports should include requests for data access and preservation, and other best practices identified by the Ranking Digital Rights Corporate Accountability Index.

2. Ensure workable channels of communication and remedy provision

Beyond creating appropriate human rights frameworks and policies, Telegram must ensure workable and accessible mechanisms for their users to provide input and feedback about the companies' actions that affect them, and to request and receive remedy for potential violations of their rights. However, civil society, academics, and even international organizations have long been expressing concerns and frustration regarding Telegram's lack of responsiveness to your users, including those most at risk, such as journalists and human rights defenders, as well as women, LGBTQI+ individuals, and other vulnerable groups. Access Now's Digital Security Helpline, and other members of the CiviCERT and the larger digital rights community have repeatedly faced silence when attempting to reach out to Telegram by using your standard communication channels in instances of online threats of violence and other serious security issues affecting civil society. For example, in Iraq, there are reports of people using your platform to plan the assassinations of activists by state-backed militias, with bounties of 1,000 USD in exchange for information on location of activists or their families. In some instances, individuals who have direct contact with you, Pavel Durov, are able to receive responses. However, these reactions are inconsistent and unpredictable.

To address this issue, Telegram must design, implement, and properly staff mechanisms for users to submit inputs and complaints about actions of Telegram or other actors occurring on the platform and receive timely responses and remedies for potential violation of their rights, including easily accessible appeal procedures. These mechanisms could include creation of helpdesks, Trust and Safety Councils, and user forums.

3. Implement better user safety and data security measures

Telegram has long prided itself on its security features, both in terms of technical measures, such as encryption and two factor authentication, as well as protection of users data and the platform's infrastructure from government censorship and surveillance measures. Your company has famously refused to cooperate with Russian government's Yarovaya Law requiring it to provide encryption keys to the government, a case that is currently being reviewed by the European Court of Human Rights, where Access Now, along with a number of signees, are seeking permission to intervene. Telegram also took special measures to reinforce its infrastructure to avoid President Lukashenko's attempts to block your platform during and after the August 2020 elections. Other recent security measures, such as disappearing messages on all chats have also been welcomed by users at risk.

However, based on the feedback from the civil society, including the RightsCon session participants, academic studies, and the digital security community, Telegram still lacks many basic security functions.

For instance, unlike WhatsApp or Signal, Telegram does not use end-to-end encryption on all its chats by default, and instead only offers it for Secret Chats, voice, and video calls. End-to-end encryption ensures that only the message sender and receiver can read the message, which protects the privacy

of the communications not only from the company itself but also from adversaries. The company should strongly consider making its chats end-to-end encrypted by default.

Telegram also uses its own proprietary, closed source MTProto cryptography protocol (or encryption algorithm) instead of using mature and tested protocols that already exist, the only major messaging app supporting end-to-end encryption messenger to do so. This makes Telegram less secure because cryptographic algorithms should not be trusted until the mathematics has been widely peer reviewed by the cryptology community. Improving the security of Telegram's protocol is especially important given the previously reported vulnerabilities and breaches exploited by the Iranian and Chinese authorities.

One such breach also highlighted another security flaw of Telegram's app, which is a verification mechanism that requires receiving verification code via an SMS message. This allows a hacker with access to the user's text messages to obtain these codes and add their own devices to the person's account.

Other measures suggested by civil society include better mechanisms to restrict the use of fake accounts and bots, restriction of download function of channels, deletion of orphaned channels, and effective user notification and education on security. While some measures may be more difficult to implement than others, Telegram has been open to consulting neither the civil society nor the digital security expert communities to help detect and prevent hacking and other security risks to the platform and its users.

We are open to consultation and eager to contribute to your efforts to respect the human rights of Telegram users. Please feel free to contact Natalia Krapiva, Tech Legal Counsel at Access Now at natalia@accessnow.org for any questions.

Sincerely,

ORGANIZATIONS

7amleh - The Arab Center for the Advancement of Social Media
Access Now
ARTICLE19
Association for Progressive Communications (APC)
Belarusian Helsinki Committee (Belarus)
Committee to Protect Journalists (CPJ)
Digital Paradigm PF (Kazakhstan)
Digital Security Lab Ukraine
Front Line Defenders
Heartland Initiative
Human Constanta (Belarus)
INSM Network for Digital Rights in Iraq
Internet Protection Society (Russia)
Internews Ukraine
IRIS - Instituto de Referência em Internet e Sociedade, Brazil

December 8, 2021

JOSA (Jordan Open Source Association)
Kandoo
Legal Media Center (Kazakhstan)
Masaar-Technology and Law Community
Media Diversity Institute (Armenia)
Mnemonic
OpenArchive
Ranking Digital Rights
Roskomsvoboda (Russia)
SMEX
Southeast Asia Freedom of Expression Network (SAFEnet)
Taraaz
Team CommUNITY
The Tahrir Institute for Middle East Policy (TIMEP)
Ubunteam

INDIVIDUALS

Alexey Sidorenko, Director at Teplitsa. Technologies for Social Good