c/o Office of the High Commissioner for Human Rights
United Nations Office at Geneva
1211 Geneva 10 Switzerland

Attn: Prof. David KAYE
the Special Rapporteur on the promotion and protection
of the right to freedom of opinion and expression

December 14, 2017

Dear Professor Kaye,

I am writing to you on behalf of Telegram Messenger LLP, a company incorporated in England and Wales on February 21st, 2014 under company number OC391410 which has its registered office at 71-75 Shelton Street, Covent Garden, London, UK WC2H 9JQ ('The Company') owning the Internet instant messaging service Telegram. My appeal is caused by serious threats to freedom of expression, which are the recent actions of the Russian authorities regarding the Internet in general, and Telegram in particular.

The Company was fined for refusing to provide the Federal Security Service of the Russian Federation ('FSB') with access to confidential correspondence of its users and in the coming weeks Telegram may be blocked on the territory of Russia.

About Telegram

Telegram – is a free cloud-based cross-platform instant messaging service. Users can send messages and exchange photos, videos, stickers, audio and files of any type. It also supports voice calls in real time. Currently, the service audience is more than 100 million people worldwide. In Russia Telegram has from 6 to 8 million users.

Telegram allows users to use two types of messaging channels – 'cloud chats" and 'secret chats". In secret chats an end-to-end encryption algorithm is used, in which regularly modifiable encryption keys are generated on users' devices, and the transmitted messages are not stored on Telegram servers. At the same time, no one, including the software developer and the service administrator, has the technical ability to obtain or make duplicates of these keys. Such an architecture is a condition for the safety of communication, reducing the risk of third-party access to unauthorized access to user correspondence.

Telegram was among the first mass Internet services which provided secure messaging services, and now most of the most popular instant messengers, including WhatsApp, Viber, WeChat, iMessage, Signal and others, to some extent use end-to-end encryption, which has become in fact 'the golden standard' of the industry.

Telegram also provides the opportunity to conduct public broadcasting messages (so-called Telegram-channels) that in authoritarian countries with strong censorship have become one of the few independent and free sources of information and platforms to share opinions on actual social and political issues.

At the same time, the Company actively opposes the use of the service for propaganda of violence independently monthly removing hundreds of channels in which terrorist content is distributed.

Background. Limiting anonymity online

Leading human rights organizations which focus on defense and promotion of freedom of expression note that, since 2013, the Russian authorities have been deliberately taking steps to expand surveillance capabilities and limit privacy and anonymity on the Internet[1].

On July 6th, 2016 in Russia a package of legislative amendments was adopted under the pretext of countering terrorism, which affected various aspects of Internet regulation, including privacy and anonymity. Thus, online services are required to store all the users' correspondence for six months, providing this data at the request of the FSB. **Services that use encryption, in addition, must provide the FSB with keys that allow to decrypt any messages that are transmitted, received and processed in their networks. At the same time, the current law does not oblige the intelligence services to obtain a preliminary judicial permission to access such information.**

Currently, the list of companies covered by the law[2] consists of 98 services, including such popular platforms as Vkontakte, Odnoklassniki, Mail.ru, Yandex, Threema, Badoo, as well as media, local community and professional forums, etc. According to the Russian telecommunication authorities, the issue of including Apple, Twitter, Facebook and WhatsApp, Google, Microsoft, Viber and other international companies representing billions of users around the world into the list is being considered.

The Russian courts on prosecution claims prohibit the sharing instructions on the use of VPN and means of circumvention of blockings. Law enforcement agencies and intelligence services officials regularly call for the blocking of the Tor network and banning access to online anonymizers. In addition, from January 1st, 2018 in Russia the law obliging Internet messengers to identify users and to provide relevant information to the authorities will come into force.

It should be noted that the principles of access to Internet communication, developed by the Russian authorities, are in general similar to the system of wiretapping (SORM), which has already been the subject of evaluation by the European Court of Human Rights. In the Grand Chamber's judgment on the case of 'Roman Zakharov v. Russia', the Court explicitly indicated that '*legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications'*[3].

According to the report of the International Human Rights Group Agora 'Russia under surveillance 2017: How the Russian state is setting up a system of total control over its citizens', over the past 10 years Russian courts have granted more than 98% of requests for permission to wire the telephone calls or to intercept information from communication channels[4].

Background. Blocking and filtering – are the main tools of Internet regulation

After 2012, when the first law that allows extra-judicial procedures to restrict access to information on the Internet has come into power, the criteria of banning information and the range of authorities authorized to take decisions on the blocking has been constantly expanded. Currently, more than 94,000 links have been added to the Registry of Prohibited Websites, and the total number of blocked resources for the whole period is approaching 9 million. In August 2017, the European Court of Human Rights communicated several applications covering various aspects of blocking information on the Internet (Kharitonov v. Russia, no., 10795/14; OOO Flavus and the Others v. Russia, nos. 12468/15, 23489 / 15, 20159/15, 19074/16 and 61919/16).

---

[1] Russia: Joint UPR Submission shows restrictive new laws on free expression. ARTICLE 19 // https://www.article19.org/resources/russia-joint-upr-submission-shows-restrictive-new-laws-on-free-expression/

[2] According to the terminology of the Russian legislation - the Register of Information Dissemination Organizers

[3] Roman Zakharov v. Russia [GC], no. 47143/06, §302, ECHR 2015

[4] https://opendemocracy.net/files/Agora-Russiaundersurveillance2017.pdf

Meanwhile, **the refusal to provide the FSB with full access to the correspondence of users in addition to a significant fine (about 15 000 EURO in each case) also entails the blocking of the service on the territory of Russia. The ISP, which refused to voluntarily provide the Russian authorities with the information needed for inclusion in the Register of Information Dissemination Organizers, is also subject to blocking**. Thus in 2017 the BlackBerry Messenger, Imo, Line, Vchat, as well as Internet radio Zello were blocked on these grounds.

The case of Telegram

On June 28th, 2017 Telegram was forcibly included in the Register of Information Dissemination Organizers by decision of Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass-Media). That, according to the position of the Russian authorities, means the duty of the service administrator to store a variety of metadata and all users' correspondence on the territory of Russia and provide them to intelligence services upon request.

On July 14, 2017, the FSB requested Telegram Messenger LLP to provide the keys needed to decrypt the correspondence on 6 phone numbers. **There were no court orders provided to the Company. The decryption keys must be sent via regular e-mail to the public address of the Internet reception of the FSB (fsb@fsb.ru).** The Company refused to comply with this request.

On October 16, 2017, the magistrate in Moscow issued a decree recognizing the Telegram Messenger LLP guilty of committing an administrative offense provided for in part 2.1 of Article 13.31 of the Code of Administrative Offenses of the Russian Federation (failure to provide information needed for decoding messages) and fined 800,000 rubles (approximately 11 000 EURO).

In November 2017, prominent Russian journalists Alexander Plyushchev and Oleg Kashin sued the court to recognize the requests to provide FSB with decryption keys illegal, as these actions threaten the right of journalists to communicate with sources securely, many of whom agree to communicate only on conditions of full confidentiality and require the use of secure communication channels. The national courts refused even to consider the journalists' claims for.

On December 12, 2017 the decision of the magistrate for Telegram was confirmed by the Meshchansky District Court of Moscow and entered into force. Since that moment, the Russian authorities have a formal ground to block Telegram on the territory of Russia in accordance with Article 15.4 of the Federal Law "On Information, Information Technologies and Information Protection".

Thus, as a result of Telegram Messenger LLP adhering the position aimed at ensuring the maximum level of safety for users' communications around the world, Russian users may lose access to one of the most important sources of information on social and political issues that are not controlled by the Russian Government and lose a secure means of communication.

Currently, the Company is preparing an appeal to the European Court of Human Rights on violation of Articles 6, 8, 10, 13 and 18 of the Convention.

General Conclusions

The case of Telegram undoubtedly contributes to the consolidation of negative judicial and law enforcement practices concerning ISPs. All of that has been written above seriously undermines the exercise of the right to freedom of expression in Russia and violates Article 19 of the International Covenant on Civil and Political Rights.

Whereas the Company due the service architecture does not have the technical ability to obtain decryption keys and pass them to anyone, it is actually being forced to create a backdoor, and give the authorities an opportunity to uncontrollably access the users' correspondence at any time. This contradicts the principled position of the Company, according to which it does not intend to give out information about its users to anyone, including the government of Russia.

This also contravenes the position of the Special Rapporteur that *in the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online* (A/HRC/29/32, para.8).

The Company confirms its commitment to the obligation to respect human rights regardless of the location of its users and regardless of whether Russia fulfills its human rights obligations or not (A/HRC 27/37, para.43) and believes that by protecting safety of it users, it facilitates the exercise of their freedom of expression.

I believe that the actions of the Russian authorities, in fact aimed at complete liquidation of anonymity online, contradict the General Assembly resolution 'The right to privacy in the digital age, which calls on all member states *to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law* as well *as to refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way* (A/RES/71/199, paras. 'c' and 'i').

It is my submission that actions taken by Russian authorities against Telegram and potential blocking access to unique and popular online service used by millions of Russians fall within your mandate as defined by the UN Human Rights Council.

On the basis of the information written above I respectfully urge, as a matter of priority, to:

1. Immediately *request* information from the Russian Government concerning the situation with blocking access to Telegram in the Russian Federation;

2. Promptly *recommend* the Government of the Russian Federation to refrain from expanding the practice of arbitrary interference with the right of citizens to freedom of expression, as well as privacy and anonymity, including online, and to follow the call comprised it the GA Resolution to review its procedures, practices and legislation relating to mass surveillance.

I confirm my willingness to provide you with any additional information I have about the case of Telegram or the situation with Internet freedom in Russia.

Yours sincerely,

Damir Gainutdinov

Lawyer of International Human Rights Group Agora