IN THE EUROPEAN COURT OF HUMAN RIGHTS **APP NO. 13232/18**

B E T W E E N :

TELEGRAM MESSENGER LLP AND TELEGRAM MESSENGER INC.

Applicants

-v-

RUSSIA

Respondent Government

WRITTEN SUBMISSIONS ON BEHALF OF THE INTERVENERS

INTRODUCTION AND SUMMARY

1. These are the written submissions on behalf of Access Now, Article 19, Electronic Frontier Foundation, Human Rights Watch, Privacy International and Reporters Without Borders ("the **Interveners**"). The Interveners are a coalition of international human rights and media freedom organisations whose areas of expertise include the right to freedom of expression and the right to privacy. They advocate for the use of strong encryption technologies to protect the right to seek, receive, and impart information anonymously online.[1] Jointly, and together with other civil society groups, they have called on governments to reject laws, policies, and practices that limit access to or undermine encryption and other secure communications tools and technologies.

2. The Interveners welcome the leave of the Court, granted on 20 May 2022, to intervene jointly as a third party in this case in order to address (i) the role of internet intermediaries in protecting the rights to freedom of expression and privacy of their users; (ii) the importance of encryption for journalists, human rights defenders, protesters and other dissidents, and the need for safeguards in the context of decryption orders; (iii) the reasons why restrictions on access to websites or apps as a sanction for non-compliance is an inherently disproportionate measure.

3. As directed, these submissions do not comment on the facts or merits of the case.

(I) THE ROLE OF INTERNET INTERMEDIARIES IN PROTECTING FREEDOM OF EXPRESSION AND PRIVACY OF THEIR USERS

4. The role played by internet intermediaries in protecting the rights of their users to freedom of expression and privacy has been consistently recognised at the international and regional level. This section addresses, firstly, the Court's own case law in this area; secondly, the relevant international standards as identified by the UN Special Rapporteur on freedom of expression; and, thirdly, the comparative standards adopted by Canada and the US in this area.

The Court's case law concerning interferences with electronic communications

5. The Court has previously considered the extent to which restrictions on electronic communications interfere with Article 10 ECHR. 'Restrictions' in this context refers both to a state-demand to access electronic communications such that individuals are no longer able to communicate privately, as well as the blocking or otherwise limiting of access to electronic communication methods.

6. In *Ahmet Yildirim v Turkey,* no. 3111/10, ECHR 2012, the Court emphasised that Article 10 is a right which applies to "everyone" regardless of the nature of the aim being pursued or the role played by the natural or legal persons in the exercise of that freedom (§50). The Court also noted the importance of the internet which is "*one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest*" (§54). In that case, criminal proceedings had been brought before the court in relation to a website which insulted the memory of Ataturk (this being prohibited by Turkish law). The national court's order went beyond blocking access to the website in question, its effect was to block <u>all</u> access to Google Sites (§51). This measure constituted an interference with the Article 10 rights of the Applicant, who operated a 'collateral' website (§56).

7. *Cengiz and Others v Turkey,* nos 48226/10 and 14027/11 is a case which – similarly to *Ahmet Yildrim* - concerned the collateral effects of an order blocking access to the video-hosting website 'YouTube'. Although the applicants were not the target of the blocking order, the effect of the order was to deprive them of the ability to access YouTube which was "*a significant means of exercising their right to freedom to receive and impart information and ideas*" (§54). This was an interference with their Article 10 rights.

8. The Court in *Magyar Kétfarkú Párt v Hungary* [GC], no. 201/17, 20 January 2020, stated that it was "*established that Article 10 applies not only to the content of information but also to the means of dissemination, since any restriction imposed on the latter necessarily interferes with the right to receive and impart information"* (§87). Similarly the Court observed that *"the protection of Article 10 extends not only to the substance of the ideas and information expressed but also to the form in which they are conveyed (see Jersild v. Denmark, 23 September 1994, § 31, Series A no. 298, and Bédat v. Switzerland [GC], no. 56925/08, § 58, 29 March 2016)".*

9. On that basis, and having reviewed the case law considered above, the Court concluded that imposing a fine on a political party for designing a mobile 'application' (app) which permitted voters to anonymously share their ballot papers and encouraged voters to cast invalid ballots, amounted to an interference with the Article 10 ECHR rights of the mobile app operator.

10. In *Standard Verlagsgesellschaft MBH v Austria (No 3)*, no 39378/15, 7 December 2021, an online newspaper was the subject of criminal and civil proceedings for failing to remove allegedly defamatory comments made by third party users about private individuals who had been named in media reports. Among other things, the Austrian courts had directed the newspaper to disclose the user data of the commentors in order that they may be identified. In the course of its judgment, the Court reiterated the observations made by the Grand Chamber in *Delfi AS v Estonia,* no 64569/09, 16 June 2015, that anonymity "*has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of opinions, ideas and information in an important manner, including, notably, on the Internet …. Thus, it can indirectly also serve the interests of a media company*" (§76). It went on to note that the applicant newspaper, "*as a media company, awards its users a certain degree of anonymity not only in order to protect its freedom of the press but also to protect users' private sphere and freedom of expression – rights all protected by Articles 8 and 10 of the Convention …. The Court observes that this anonymity would not be effective if the applicant company could not defend it by its own means. It would be difficult for users to defend their anonymity themselves should their identities have been disclosed to the civil courts*" (§78). The Court ultimately concluded that the requirement imposed by the Austrian courts to disclose the requested user data "*constituted an interference with the applicant company's right to enjoy freedom of the press*" (§80) which was not "*necessary in a democratic society*" as required by art 10(2) since the domestic appellate courts had made no attempt to explain "*why the plaintiffs' interests in the disclosure of the data were 'overriding' the applicant company's interests in*

protecting their authors' anonymity" (§93). The Interveners submit that the same principles identified by the Court in relation to the protection afforded to the anonymity of internet users and their user data apply *a fortiori* to the encryption of the content of private communications.

International law on encryption

11. In recognition of the significance of the internet and electronic communication methods to freedom of expression and privacy of individuals, and the importance of those rights to democratic society, there has been careful consideration of encryption of electronic communications at the international level.

May 2015 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

12. In his May 2015 report to the General Assembly concerning the use of encryption and anonymity in digital communications, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye described privacy as a "*gateway for freedom of opinion an expression*". [2] He stated: [3]

> *16. Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks. The previous mandate holder noted that the rights to "privacy and freedom of expression are interlinked" and found that encryption and anonymity are protected because of the critical role they can play in securing those rights (A/HRC/23/40 and Corr.1). Echoing article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights specifically protects the individual against "arbitrary or unlawful interference with his or her privacy, family, home or correspondence" and "unlawful attacks on his or her honour and reputation", and provides that "everyone has the right to the protection of the law against such interference or attacks". The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression (see General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8).*
>
> *17. Encryption and anonymity are especially useful for the development and sharing of opinions, which often occur through online correspondence such as e-mail, text messaging, and other online interactions. Encryption provides security so that individuals are able "to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion" (see A/HRC/23/40 and Corr.1, para. 23). ….*

> *18. Individuals and civil society are subjected to interference and attack by State and non-State actors, against which encryption and anonymity may provide protection. In article 17 (2) of the International Covenant on Civil and Political Rights, States are obliged to protect privacy against unlawful and arbitrary interference and attacks. Under such an affirmative obligation, States should ensure the existence of domestic legislation that prohibits unlawful and arbitrary interference and attacks on privacy, whether committed by government or non-governmental actors...*

13. The Special Rapporteur emphasised that the permissible limitations on the right to privacy should be read strictly regardless of the legal rubric under which it is considered.[4] He went on to recommend that states "*should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression*" and counselled them to "*avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows*".[5] As he noted:[6]

> *intentional flaws invariably undermine the security of all users online, since a backdoor, even if intended solely for government access, can be accessed by unauthorized entities, including other States and non-State actors. Given its widespread and indiscriminate impact, back-door access would affect, disproportionately, all online users.*

14. The consideration of whether any restriction on encryption or anonymity is "*necessary*" to achieve a legitimate objective also involves an assessment of the proportionality of the measure in question to the aim:[7]

> *A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result". The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be "proportionate to the interest to be protected". A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high.*

2016 Report on the promotion and protection of the right to freedom of opinion and expression[8]

15. The Special Rapporteur's 2016 report noted that private corporations were coming under increasing pressure from states to compromise the security of their customers' digital devices (para 62). The Special Rapporteur recommended that "*states must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with*

the freedom of expression… any demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19 (3) of the International Covenant on Civil and Political Rights" (para 85).[9]

July 2018 Encryption and Anonymity follow-up report

16. In July 2018, the UN Special Rapporteur issued an '*Encryption and Anonymity follow-up report*' to the 2015 Report discussed above. It also emphasises that freedom of expression is only protected by the proportionality of any restrictions on encryption: "*blanket prohibitions of encryption plainly fail these conditions. Measures that systematically weaken encryption and digital security more generally, such as backdoors, key escrows and data localization requirements, also interfere with rights to opinion, expression and privacy. Court-ordered decryption should only be permitted on a case-by-case basis applied to individuals…"*.[10] The Report highlighted as a concern the intentional weakening of encryption across <u>all devices</u> by states which purport to be concerned about individual devices, citing examples such as (i) the FBI in the USA seeking to compel Apple to create software that would disable security features on iPhones; (ii) the Russian government's banning of Telegram after the company refused to provide the state with access to encryption keys; and (iii) Iran issuing its own ban on Telegram shortly after the actions of Russia.[11]

Comparative law on encryption

USA

17. In the USA there are at present no legal powers which can be used to require online messaging apps such as 'Telegram' to decrypt messages exchanged between users. Under the Communications Assistance for Law Enforcement Act of 1994 ("**CALEA**"), 47 U.S.C. §1001(4), Telegram is likely to be regarded as an 'electronic messaging service' which is defined as "*software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages"*. Electronic messaging services are, pursuant to 47 U.S.C. § 1001(6)(B)(iii), a type of 'information service'. Information services are expressly exempted from the requirements of CALEA which require 'telecommunication carriers' to facilitate the decryption of encrypted communications. *See* 47 U.S.C. §§ 1002(b)(1), (2). And, importantly, telecommunication

carriers are not required to decrypt, or to ensure the government's ability to decrypt, any communications which are encrypted by the user and which the carrier does not have the key to decrypt: 47 U.S.C. § 1002(b)(3).[12] See also the analysis *In re Apple, Inc.,* 149 F.Supp 3d 341, 356 (E.D.N.Y. 2016) at 354-356 where the court considers that CALEA exempts corporations like "Apple" (which provides messaging apps such as 'iMessage'), from the statutory obligation under CALEA to assist law enforcement.

Canada

18. There are no legal powers in Canada which can be used to require telecommunication or online service providers to facilitate the decryption of encrypted communications. There are general powers under the Criminal Code including the provision of assistance orders (s.487.014) and production orders (s.487.02) which could potentially be used in individual cases, depending upon the technology in question. Section 8 of the Canadian Charter of Rights and Freedoms requires not only that the search is reasonable, but that the search is conducted in a reasonable manner. Evidence obtained in breach of a Charter right can be excluded subject to section 24(2) of the Charter. In terms of case law, in *R v. Boudreau-Fontaine* (2010 QCCA 1108) the Quebec Court of Appeal found that an order compelling an individual to provide a password violated his constitutional rights, including his rights to silence and against self-incrimination. Various lower courts have followed this decision, although the Supreme Court of Canada has not ruled on this issue.

(II) THE IMPORTANCE OF ENCRYPTION FOR JOURNALISTS, HUMAN RIGHTS DEFENDERS AND OTHERS, AND THE NEED FOR SAFEGUARDS IN THE CONTEXT OF DECRYPTION ORDERS

19. The Interveners agree with the dicta of the Court, summarised at paras 5-11 above, that the internet and electronic communication methods (such as electronic messaging applications) are now an essential tool for the exercise of the human right of freedom of opinion and expression.[13] This being the case, the UN Special Rapporteur is accurate in his assessment that corporations play a significant role in safeguarding fundamental freedoms of expression. This is reflected in the Court's long-standing recognition that Article 10 extends to protecting the means by which information is communication and also protects the rights of platforms (which derive, in turn, from the rights of their users) who operate the technology by which information

is communicated and received. Moreover, the Special Rapporteur is also right to emphasise the reasons why privacy is fundamental to the freedom of expression.

20. Whilst Article 10 ECHR protects "*everyone*", the Interveners emphasise the importance of encryption for journalists, human rights defenders, lawyers, activists, and dissidents. These groups depend on encryption to provide the privacy which is key to communicating with others freely, candidly and – critically – safely. The Court need only consider the position of internet users in Ukraine, or activists in Russia, who would be at risk of violations of their fundamental rights if their private communications and/or their identities were revealed to the Russian authorities in the course of the current conflict.

21. The Interveners draw the following propositions from the case law of the Court:

    (i) Article 10 ECHR protects the public generally ("*everyone*"), and guarantees not only the right of the public to communicate information but also to receive it;

    (ii) Electronic communication methods are now the principal tool individuals use to participate in activities and discussions, including on politics and issues of general interest;

    (iii) As such, electronic communication methods have become one of the principal means by which individuals exercise their rights to freedom of expression and information;

    (iv) Therefore, Article 10 is engaged not only in relation to the content of individual private messages or user accounts, but also the electronic methods by which those messages are disseminated – in other words, the technology which apps such as Telegram provide to facilitate the exchange of messages. This necessarily *includes* encryption services;

    (v) It follows that Article 10 protects not only the individuals who produce or view the content communication on electronic messaging applications, but also the Article 10 rights of the operator of the electronic messaging application.

22. The Interveners also emphasise that any interference with encryption – as with any interference with privacy and freedom of expression more generally - must be in accordance with the law and not go beyond that which is necessary to achieve the legitimate aim in question. The Court has already identified that 'collateral' effects of interferences engage Article 10 (*Ahmet Yildirim* and *Cengiz*); now the Court is invited to reject any suggestion that 'back door' access to

encrypted messaging applications could be compatible with Article 10. The protection of encryption of private communications is consistent with:

(i) the foundational principle that privacy underpins freedom of expression;

(ii) the development of international law in the field of privacy and freedom of expression, c.f the 2015 and 2018 reports of the UN Special Rapporteur on Freedom of Expression;

(iii) the position taken by the Parliamentary Assembly of the Council of Europe which has warned that "*the creation of "back doors" or any other techniques to weaken or circumvent security measures or exploit their existing weaknesses should be strictly prohibited…"*;

(iv) the comparative approach of such jurisdictions as the United States and Canada;

(v) the requirements of necessity and proportionality under the Convention. To date, no state has been able to show why a proportionate response to the need to access the communications of a particular individual is to have the key to access the communications of all individuals, see also the 2015, 2016 and 2018 reports of the UN Special Rapporteur and also the comparative approach of other jurisdictions above.

23. Encryption is an essential part of privacy, and therefore of freedom of expression, in the digital age. In any balancing of interests, the Court must afford preponderant weight to the need to maintain encryption as a public good and view with skepticism any measure that would seek to limit or undermine its effectiveness.

(III) WHY RESTRICTIONS ON ACCESS TO APPS AND WEBSITES AS A SANCTION FOR NON-COMPLIANCE IS AN INHERENTLY DISPROPORTIONATE MEASURE

24. Lastly, the Interveners cast doubt on the proportionality of any measure which seeks to restrict or block users' access to an app or a service due to a company's failure to comply with an administrative or even a judicial order. To the extent that sanctions are necessary to enforce compliance with lawful orders, such measures must always be targeted and proportionate to the legitimate aim pursued. As the UN Special Rapporteur observed in his 2015 report, "*blanket prohibitions fail to be necessary and proportionate*".[14]

25. Indeed, given the weight which the Convention and other international standards attach to internet intermediaries in the protection of fundamental rights, the Interveners submit that the restriction or blocking of a service or app used by thousands of people – or even millions of people – for the sake of enforcing an order relating to a relatively small group or category could never be a proportionate measure in the circumstances. Such a measure would be tantamount to a form of collective punishment visited upon an entire category of people for the sake of matters entirely outside their responsibility and beyond their control.

26. More generally, the Interveners note that collective punishments are contrary to customary principles of international law: see e.g. Article 33 to the Fourth Geneva Convention which provides that "*[n]o protected person may be punished for an offence he or she has not personally committed. Collective penalties and likewise all measures of intimidation or of terrorism are prohibited".* Similarly, Article 25(2) of the Rome Statute of the International Criminal Court restricts the Court's jurisdiction to those offences for which a person is "*individually responsible*".

ERIC METCALFE
KHATIJA HAFESJI
Monckton Chambers
10 June 2022

On behalf of the Interveners:

Access Now	**Human Rights Watch**
ARTICLE 19	**Privacy International**
Electronic Frontier Foundation	**Reporters Without Borders**

1 *Promote Strong Encryption and Anonymity in the Digital Age*, Joint Civil Society Statement Submitted to the 29th Session of the UN Human Rights Council, June 17 2015.
[2] A/HRC/29/32, 22 May 2015, p.7.
[3] A/HRC/29/32, 22 May 2015, paras 16-18.
[4] A/HRC/29/32, 22 May 2015, para 29.
[5] A/HRC/29/32, 22 May 2015, para 60.
[6] A/HRC/29/32, 22 May 2015, para 42.
[7] A/HRC/29/32, 22 May 2015, para 35.
[8] A/HRC/32/38, 11 May 2016.
[9] See also the UNESCO Human Rights and Encryption Report, 2016, pages 56-59.
[10] A/HRC/38/35/Add.5 13 July 2018, para 8. See also: UN Doc. A/HRC/31/64, 24 November 2016, para. 60.
[11] A/HRC/38/35/Add.5 13 July 2018, para 15.
[12] See *Congressional Research Service, In Focus: Law Enforcement and Technology: the "Lawful Access" Debate* (February 22 2021).
[13] See Executive Summary of Access Now, *26 recommendations on content governance: a guide for lawmakers, regulators and company policy makers*, March 2020.
[14] A/HRC/29/32, 22 May 2015, para 60.