IN THE EUROPEAN COURT OF HUMAN RIGHTS
APPLICATIONS NO. 12468/15, 20159/15, 23489/15, 19074/16 & 61919/16

BETWEEN:-

OOO FLAVUS and others

Applicants

- v -

RUSSIA

Respondent Government

15 January 2018

THIRD-PARTY INTERVENTION SUBMISSIONS BY ARTICLE 19, THE ELECTRONIC FRONTIER FOUNDATION, ACCESS NOW AND REPORTERS WITHOUT BORDERS

---

1. This third-party intervention is submitted on behalf of *ARTICLE 19: Global Campaign for Free Expression* (ARTICLE 19), *Electronic Frontier Foundation* (EFF), *Access Now* and *Reporters without Borders* (RSF) (jointly the Interveners).[1] The Interveners welcome the opportunity to intervene in these cases, by leave of the President of the Court, granted on 6 December 2017 pursuant to Rule 44 (3) of the Rules of Court.

SUMMARY

2. These cases concern a series of blocking orders made against websites alleged to contain: (i) calls for mass disorder, extremist activities, and participation in unauthorised mass gatherings;[2] (ii) extremist materials;[3] and (iii) information about technologies which could be used to obtain access to blocked websites containing extremist materials.[4] Along with the case of *Kharitonov v Russia*,[5] these cases represent the first opportunity for the Court to examine Russian legislation granting far-reaching powers to the State to block websites. The cases additionally concern national legal proceedings leading to websites being blocked by court orders, with the operators of websites subject to blocking orders alleging that they were unaware of the relevant proceedings and did not, therefore, have an opportunity to be heard by the court.

3. The Interveners address the following matters in these submissions: (i) international law standards applicable to measures for tackling online extremism or violence, including a requirement for a direct and immediate connection between online content and the alleged threat of violence; (ii) international approaches to tackling online extremism or violence, including comparative regulatory approaches and standards on website blocking measures; (iii) the need for website blocking measures to be subject to a legal framework ensuring tight control over the scope of such measures and providing for effective judicial review, and for strict scrutiny to ensure that such measures are necessary and proportionate; and (iv) the importance, under Article 10 of the European Convention, of protecting the procedural rights of the authors of content that would be rendered inaccessible by a blocking order.

SUBMISSIONS

I. International law standards applicable to measures for tackling online extremism or violence

a. Definitions of extremism

4. At the outset, the Interveners highlight that there is no established, unified, generally accepted definition of "extremism"[6] in international law. Nonetheless, the term has been used in a number of resolutions of the UN General Assembly (GA)[7] and the UN Security Council (UNSC),[8] and in reports of UN working groups and task forces focusing on counter-terrorism.[9] A number of governments

and international organisations have also agreed memoranda on good practices to combat "violent extremism" at the Global Counter-Terrorism Forum.[10] At the same time, none of these documents provide a working definition of the term.

5. Notions of "extremism" or "extremist activities" are often conflated with "terrorism", which is itself a term without a universal definition under international law.[11] However, UN human rights bodies have recommended that definitions of "terrorism" and "extremism" must be consistent with Member States' obligations under international law, in particular international human rights law.[12] They have also highlighted the tension between freedom of expression and counter-terrorism measures. In particular, General Comment No.34 to the International Covenant on Civil and Political Rights (ICCPR) clearly provides:

> 46. States parties should ensure that counter-terrorism measures are compatible with paragraph 3 [of Article 19 of the ICCPR]. Such offences as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying", or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. Excessive restrictions on access to information must also be avoided. The media plays a crucial role in informing the public about acts of terrorism and its capacity to operate should not be unduly restricted. In this regard, journalists should not be penalized for carrying out their legitimate activities.

b. Applicable international standards

6. International human rights bodies and this Court have explicitly recognised that the right to freedom of expression extends and applies to the online sphere.[13] They have also repeatedly stressed that this freedom applies to ideas, information and opinions "that offend, shock or disturb the State or any part of the population. While the right to freedom of expression is a qualified right that can, and sometimes must, be limited, these restrictions must not jeopardize the essence of the right."[14]

7. Under both international and European Convention standards, limitations of the right to freedom of expression must be strictly and narrowly tailored, ensuring that the essence of the right remains intact. The restrictions must be (i) provided by law with a sufficient degree of clarity and precision; (ii) pursue a legitimate aim expressly enumerated in the relevant treaty; and, (iii) be necessary and proportionate to the legitimate aim pursued, requiring that if a less intrusive measure is capable of achieving the same purpose as a more restrictive one, the least restrictive measure be applied.[15]

8. The UN Human Rights Committee, in its General Comment No.34, stated that the permissible restrictions on freedom of expression enumerated in Article 19 of the ICCPR: "*may never be invoked as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights*".[16] The Interveners submit that legislation invoking "extremism" as a justification to restrict freedom of expression, without a clear and appropriately narrow definition of "extremism", is likely to give rise to a violation of this principle.

9. The Interveners also submit that international law standards applicable to measures for tackling online "extremism" or violence include the requirement for a direct and immediate connection between online content and the alleged threat of violence to be established.

10. In their Joint Declaration on Freedom of Expression and countering violent extremism,**[17]** four freedom of expression mandates have elaborated on the scope of the right to freedom of expression as it relates to content that may fall within the scope of extremism, through six general principles, including:

> 1. General Principles:
> a) *Everyone has the right to seek, receive and impart information and ideas of all kinds,* especially on matters of public concern, including issues relating to violence and terrorism, as well as to

comment on and criticise the manner in which States and politicians respond to these phenomena(…)
c) *Any restrictions on freedom of expression should comply with the standards for such restrictions recognised under international human rights law.* In compliance with those standards, States must set out *clearly in validly enacted law* any restrictions on expression and demonstrate that such restrictions are *necessary and proportionate* to protect a legitimate interest.(…) *[emphasis added]*

11. The same Joint Declaration contains further specific recommendations, including:

2. Specific Recommendations: (...)
c*) The concepts of "violent extremism" and "extremism" should not be used as the basis for restricting freedom of expression unless they are defined clearly and appropriately narrowly* (…)

e) States should not subject Internet intermediaries to mandatory orders to remove or otherwise restrict content except where the content is lawfully restricted in accordance with the standards outlined above. States should refrain from pressuring, punishing or rewarding intermediaries with the aim of restricting lawful content (…)

j) States should not adopt, or should revise, laws and policies which involve the following:
i) *Blanket prohibitions on encryption and anonymity, which are inherently unnecessary and disproportionate*, and hence not legitimate as restrictions on freedom of expression, including as part of States' responses to terrorism and other forms of violence.

ii) Measures that *weaken available digital security tools*, such as backdoors and key escrows, since these disproportionately restrict freedom of expression and privacy and render communications networks more vulnerable to attack." *[emphasis added]*

12. Similarly, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has further elaborated on what constitutes views considered "extreme" under countering violent extremism provisions:

38. [*S]imply holding or peacefully expressing views that are considered 'extreme' under any definition should never be criminalised, unless they are associated with violence or criminal activity. The peaceful pursuance of a political, or any other, agenda – even where that agenda is different from the objectives of the government and considered to be 'extreme'–* must be protected. Governments should counter ideas they disagree with, but should not seek to prevent non-violent ideas and opinions from being discussed.[18]

13. He has further said that:

40. *[A]ny measure taken to prevent or remove messages communicated through the Internet or other forms of technology constitute an interference with the right to freedom of expression and must be justified.* The Human Rights Committee notes that bans on the operation of certain sites *should not be generic but content-specific, and that no site or information-dissemination system should be prohibited from publishing material solely on the basis that it may be critical of the Government or the social system espoused by the Government.*"[19] *[emphasis added]*

14. In addition, the 1996 Johannesburg Principles on National Security Freedom of Expression and Access to Information (Johannesburg Principles)[20] consider extensively the types of restrictions that can be imposed on freedom of expression for the purposes of protecting national security. This includes the requirements that such limitations should not be imposed:

To protect a government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.[21]

15. The Johannesburg Principles specify that States should guarantee that:

> No one may be punished for criticising or insulting the nation, the state or its symbols, the government, its agencies, or public officials, or a foreign nation, state or its symbols, government, agency or public official unless the criticism or insult was intended and likely to incite imminent violence. [22]

16. Finally, it should be noted that Article 20(2) of the ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law. At the same time, inciting violence is more than just expressing views that people disapprove of or find offensive.[23] Rather, it is speech that encourages or solicits other people to engage in violence through vehemently discriminatory rhetoric. At international level, the UN has developed the Rabat Plan of Action – an inter-regional multi-stakeholder process involving UN human rights bodies, NGOs and academia –, which provides the closest definition of what constitutes incitement under Article 20(2) of the ICCPR.[24] In particular, the Rabat Plan of Action clarifies that regard should be had to six factors in assessing whether speech should be criminalised by States as incitement. These factors include the general context, the speaker, intent, content of the message or its form, the extent of the speech at issue and the likelihood of harm occurring, including its imminence.[25]

II. International approaches to tackling online "extremism" or violence

a. Invoking extremism as a justification for restricting freedom of expression

17. The stated purpose of limitations such as bans, censorship, blocking or suspension of websites due to "extremist" content is usually the protection of national security and/or public order.

18. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) has stated that:[26]

> 18. Among the permissible grounds for restrictions, States often rely on national security and public order. "National security", undefined in the Covenant, *should be limited in application to situations in which the interest of the whole nation is at stake, which would thereby exclude restrictions in the sole interest of a Government, regime or power group*, a point emphasized in the Siracusa Principles on the Limitation and Derogation Provisions in the [ICCPR]. It also may include protection of a State's political independence and territorial integrity. Similarly, "public order" (*ordre public*) must be limited to specific situations in which a limitation would be demonstrably warranted.
>
> 19. *Yet States often treat national security or public order as a label to legitimate any restriction* (...)
>
> 23. Public order is often used by States to justify measures to counter violent extremism. *The measures adopted are rarely drawn narrowly enough to satisfy the necessity or proportionality criteria*. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has urged Governments to address the problems of extremism with *precise definition and proportionate measures*(…)" *[emphasis added]*

19. The Special Rapporteur on FOE further emphasised that:[27]

> [E]fforts to counter 'violent extremism' can be *the 'perfect excuse' for democratic and authoritarian governments around the world to restrict free expression and seek to control access to information.* By 'balancing' freedom of expression and the prevention of violence, the programmes and initiatives aimed at countering 'violent extremism' have – often purposely, sometimes inadvertently – put at risk or curtailed the independence of media." *[emphasis added]*

20. As regards countering violent extremism measures, the Special Rapporteur on FOE has stressed that programs aimed at violent extremism:

> [M]ust be based on a legal framework and on evidence of their effectiveness and their necessity and proportionality to achieve legitimate objectives (…) [and that measures such as] content removal, surveillance, the blaming of security tools like encryption – risk undermining the potential of digital technologies to foster freedom of expression and access to information and to provide avenues for counter-speech.[28]

21. He has also warned that:

> Some governments target journalists, bloggers, political dissidents, activists and human rights defenders as 'extremists' or 'terrorists', criminalizing and detaining them, using legal systems to counter broad and unclear offences (…)
>
> The harm is felt not only by journalists but also by their audiences, the public that deserves the right to know and to access information of public interest.[29]

b. State approaches to "extremism"

22. The Interveners observe that States have mainly disregarded the requirements set out above, in particular that in order to meet international human rights standards on freedom of expression, the restrictions must not be vague and overbroad. Vague and overbroad definitions of "extremism" in turn have allowed individual States to target certain groups or minorities within their territories, and to suppress legitimate political dissent and criminalise speech, thought and expression in opposition of the government. For example, the report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, has identified the following problematic definitions: [30]
    - Norway defines violent extremism as the "activities of persons and groups that are willing to use violence in order to achieve political, ideological or religious goals";
    - Sweden defines a violent extremist as someone who is "deemed repeatedly to have displayed behaviour that does not just accept the use of violence but also supports or exercises ideologically motivated violence to promote something";
    - The UK defines extremism as "the vocal or active opposition to fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs, as well as calls for the death of United Kingdom armed forces at home or abroad";
    - In Denmark, extremism refers to groups that "can be characterized by their simplistic views of the world and of "the enemy", that reject fundamental democratic values and norms and that use illegal and possibly violent methods to achieve political/religious or ideological goals";
    - Australia defines violent extremism as "the use or support of violence to achieve ideological, religious or political goals".

c. Approaches to blocking "extremist" online content

23. States frequently claim that the Internet has played an important role in the recruitment or radicalisation of certain population groups; therefore often, measures aimed at countering extremism target online activities.[31] Many States have adopted "a combination of repressive legislative measures to block, filter and ban specific content or entire websites."[32]

24. In *Ahmet Yıldırım v. Turkey*, the Court examined a range of comparative law material on website blocking.[33] The Court concluded that the regulatory frameworks governing website blocking were fragmented, particularly in light of rapidly changing new technologies. As such, it was difficult to identify common standards based on a comparison of the legal situation in Council of Europe Member States.

25. Since then, the Council of Europe has conducted a comprehensive study of filtering, blocking and illegal content takedown practices on the Internet, which was published in June 2016.[34] Among other things, the Council of Europe concluded:[35]

- Several countries do not have specific legislation on blocking, filtering and takedown of illegal content, partly because of the difficulty in keeping pace with technological developments and partly due to their respective legal traditions. These countries (the UK, Austria, the Netherlands, Ireland, Poland, the Czech Republic and Switzerland) usually rely on existing legislation to deal with the issues raised by illegal content on the Internet. In practice, this also means that the courts determine whether or not content is illegal and should be blocked.

- A small number of countries, including Russia, France, Turkey, Portugal, Hungary, Spain and Finland have put in place a specific legal framework allowing blocking and takedown of certain categories of illegal content, in particular child abuse materials, content that endangers national security, including terrorist content, content that threatens public health and morals, as well as content that constitutes a "hate crime". However, the Council of Europe noted that some countries, such as Russia, had extended the common grounds under which blocking may be legitimately authorised to include, for example, so called "homosexual propaganda".[36]

- A minority of countries allow public authorities, such as the police, public prosecutors or other administrative bodies, to order the blocking of illegal material without prior judicial intervention (Greece, Portugal, Russia, France, Serbia and Turkey).

- In most countries, interested parties are given an opportunity to challenge blocking measures through criminal or civil procedure rules (see especially Portugal).

d. Standards on website blocking measures

26. International human rights bodies have long expressed concern about blocking and filtering measures. In particular, the four freedom of expression mandates observed, in their 2011 Joint Declaration on Freedom of Expression on the Internet, that:

> *Mandatory blocking of entire websites*, IP addresses, ports, network protocols or types of uses (such as social networking) is an *extreme measure* – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.[37] *[emphasis added]*

27. The Special Rapporteur on FOE has described blocking as follows:

> Blocking refers to measures taken to prevent certain content from reaching an end user. This includes preventing users from accessing specific websites, Internet Protocol (IP) addresses, domain name extensions, the taking down of websites from the web server where they are hosted, or using filtering technologies to exclude pages containing keywords or other specific content from appearing.[38]

28. He has further emphasised that website blocking measures rarely fulfil the conditions of legitimate restrictions:

> States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression(…). Firstly**,** *the specific conditions that justify blocking are not established in law*, or are provided by law but in an overly broad and vague manner, which risks content being blocked arbitrarily and excessively. Secondly, blocking *is not justified to pursue aims* which are listed under [Article 19, para 3 of the ICCPR], and blocking lists are *generally kept secret*, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose. Thirdly, *even where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim*, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that

which has been deemed illegal. Lastly, content is frequently blocked without the intervention of or possibility for review by a judicial or independent body.[39] *[emphasis added]*

29. States often refer to extremism as a basis for the sentencing of individuals in relation to statements they have made on the internet. The Special Rapporteur on FOE has explained that:[40]

> 36. Imprisoning individuals for seeking, receiving and imparting information and ideas can rarely be justified as a proportionate measure to achieve one of the legitimate aims under [Article 19 para 3 of the ICCPR]. The Special Rapporteur would like to reiterate that defamation should be decriminalized, and that protection of national security or countering terrorism cannot be used to justify restricting the right to expression unless the Government can demonstrate that: (a) the expression is intended to incite imminent violence; (b) it is likely to incite such violence; and (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.
>
> 37. Additionally, the Special Rapporteur reiterates that the right to freedom of expression includes expression of views and opinions that offend, shock or disturb. Moreover, as the Human Rights Council has also stated in its resolution 12/16, restrictions should never be applied, inter alia, to discussion of Government policies and political debate; reporting on human rights, Government activities and corruption in Government; engaging in election campaigns, peaceful demonstrations or political activities, including *for peace or democracy; and expression of opinion and dissent, religion or belief, including by persons belonging to minorities or vulnerable groups. [emphasis added]*

30. The Interveners note the guidance given by the High Court of Justice of England and Wales as to the principles to be considered in making blocking orders. In a case concerning copyright infringement, *Cartier International AG v British Sky Broadcasting Ltd*, the Judge (Mr Justice Arnold) observed:

> 189. (…) I conclude that, in considering the proportionality of the orders sought (…), the following considerations are particularly important:
> i) The comparative importance of the rights that are engaged and the justifications for interfering with those rights;
> ii) The availability of alternative measures which are less onerous;
> iii) The efficacy of the measures which the orders require to be adopted by the ISPs, and in particular whether they will seriously discourage the ISPs' subscribers from accessing the Target Websites;
> iv) The costs associated with those measures, and in particular the costs of implementing the measures;
> v) The dissuasiveness of those measures;
> vi) The impact of those measures on lawful users of the internet.
>
> 190. In addition, it is relevant to consider the substitutability of other websites for the Target Websites.[41]

III. The need for an adequate legal framework and protection of procedural rights

31. In the light of the international standards described above, the Interveners submit that blocking measures can only ever be compatible with international standards on freedom of expression where they are provided by law and a court has determined that a particular measure is necessary to protect legitimate aims specified in the European Convention.

a. Any requirement to block unlawful content must be provided by law

32. The Interveners reiterate that blocking access to websites is an extreme measure, which is analogous to banning a newspaper or television station. By its very nature, it is a blanket measure that is incapable of distinguishing between the different kinds of content that a website may contain (i.e. lawful and allegedly unlawful). For this reason, blocking an entire website is very likely to amount to a disproportionate interference with the right to freedom of expression, given the extent of the adverse impact.[42] As such, it should never be required by law. As the present

cases show, the risks of excessive blocking are real and the adverse effects on freedom of expression dramatic.

33. In order to meet the requirement that a restrictive measure is provided by law, the relevant law should be drafted sufficiently precisely for individuals to be able to regulate their conduct accordingly.[43] As such, national measures should not provide for online material to be blocked on the basis of concepts which are not clearly and narrowly defined (for example, on the basis of "extremism" *simpliciter* or "extremist activity").

34. Moreover, consistent with the international and comparative law standards set out above, even where blocking is permissible, the Interveners submit that the law should provide for the following procedural safeguards:
    - Blocking should only be ordered by a court or other independent and impartial adjudicatory body. Regulatory models whereby government agencies directly issue blocking orders are inherently problematic as executive agencies are, by nature, more likely to call for measures that protect the particular state interests they are tasked to protect, such as national security or child safety, rather than freedom of expression;

    - When a public authority or third party applies for a blocking order, the operators of the website, authors of the offending content, ISPs and/or other relevant internet intermediaries should be given the opportunity to be heard in order to contest the application;

    - Similarly, procedures should be in place allowing other interested parties, such as free expression advocates or digital rights organisations, to intervene in proceedings in which a blocking order is sought;

    - Users should be given a right to challenge, after the fact, the decision of a court or other independent and impartial adjudicatory body to block access to content.[44] *A fortiori*, this must include a right for victims of collateral blocking to challenge the wrongful blocking of their website or webpage; and

    - Whenever an order has been made to block online content, anyone attempting to access it must be able to see that the respective content has been blocked as well as a summary of the reasons why it was blocked, in order that they may have the opportunity to challenge the decision.[45] In particular, blocked pages should contain the following minimum information:
        i) the party requesting the block;
        ii) the legal basis for the decision to block and the reasons for the decision in plain language;
        iii) the case number, if any, together with a link to the relevant court order;
        iv) the period during which the order is valid;
        v) contact details in case of an error; and
        vi) information about avenues of appeal or other redress mechanisms.

35. Finally, in countries where blocking decisions are made by public authorities, the law should guarantee that those authorities are independent of government and that their decisions can be readily challenged before a court or tribunal.[46] Moreover, the law should lay down the criteria to be applied by these authorities to determine whether any blocking order can be issued.

b. Any requirement to block content must pursue a legitimate aim

36. The Interveners further submit that blocking measures should only be permitted in respect of content that is unlawful or can otherwise be legitimately restricted by reference to international standards on freedom of expression.[47] Accordingly, any law providing for blocking powers should specify the categories of content that can be lawfully blocked, consistent with international standards on freedom of expression.

37. Legitimate aims are those that protect, *inter alia*, the human rights of others, protect national security or public order. As such, it would be impermissible to prohibit expression merely because it is critical of government or advocates for political change. Similarly, it is not permissible to pursue illegitimate objectives through a reliance on Article 10 of the European Convention that is merely a pretext for other, illegitimate objectives.. The Interveners recall that the General Comment No.34 notes that extreme care must be taken in crafting and applying laws that purport to restrict expression in order to protect national security.[48] Further, the Human Rights Committee have also observed that:

> [I]t is not compatible with [Article 19 para 3 of the ICCPR], for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information.[49]

38. As a result, the Interveners submit that the blocking of websites which contain information about VPNs or other similar technologies can never be justified. Such technologies are content-neutral and blocking such websites thus amounts to a restriction on access to all content which might be obtained using those technologies. Accordingly, the blocking of such technologies (or information about them) is inherently incapable of being adequately specified with reference to categories of legitimately proscribed content.

c. Blocking orders should be strictly proportionate to the aim pursued

39. The Interveners submit that: (i) the blanket blocking of a website, without reference to specific unlawful content, should not be required by law and should always be considered a disproportionate restriction on freedom of expression; (ii) national laws should not permit online content to be blocked on the basis of an alleged threat of violence or public disorder unless there is a direct and immediate connection between the online content and the likelihood or occurrence of such violence; and (iii) any order to block access to content should be limited in scope and strictly proportionate to the legitimate aim pursued.

40. It follows from the comparative material above that in determining the scope of any blocking order, the courts should address themselves to the following:[50]
    - Any blocking order should be as narrowly targeted as possible;
    - Determining that the blocking order is the least restrictive means available to deal with the alleged unlawful activity, including an assessment of any adverse impact on the right to freedom of expression which would result from issuing the order;
    - Determining whether access to other lawful material will be impeded by issuing an order and, if so, to what extent, bearing in mind that in principle, lawful content should never be blocked;
    - The overall effectiveness of the measure and the risks of over-blocking, including by reference to an examination of the technologies available in order to comply with the order; and
    - Whether the blocking order should be of limited duration. In this regard, the Interveners consider that blocking orders to prevent future unlawful activity are a form of prior censorship and, as such, are a disproportionate restriction on freedom of expression.

41. The same criteria should be applied by administrative bodies tasked with issuing blocking orders.

CONCLUSION

42. The Interveners submit that website blocking is a very serious interference with the right to freedom of expression. For this reason, it should only be permitted in the most exceptional circumstances and should be subject to the strictest safeguards. Moreover, any blocking measures based on vague and overbroad or ill-defined terms such as “extremism” risk blocking being used

to quash the democratic expression of alternative views and are almost certain to have a chilling effect on freedom of expression.

43. As a matter of basic procedural fairness, if mandatory blocking measures are permissible at all, they should: (i) have a basis in law, (ii) be ordered by a court or other independent body and (iii) be strictly necessary and proportionate to the legitimate aim pursued. The requirements of strict necessity and proportionality also mean that, in considering whether to grant a website blocking order, the court or other independent body tasked with making the order must take into account the impact of the order on lawful content and what technology may be used to prevent over-blocking. Basic procedural fairness also demands that all victims of blocking orders, including authors and publishers of content, and those who seek to access the content, should be given an opportunity to challenge such orders and must therefore be notified of their existence.

Barbora Bukovska, ARTICLE 19

Raman Jit Singh Chima, ACCESS NOW

Corynne McSherry, EEF

Paul Coppin, RSF

Represented by Gerry Facenna QC
Monckton Chambers, Gray's Inn, London

---

[1] **ARTICLE 19** is an international human rights organisation that works around the world to protect and promote the right to freedom of expression and the right to freedom of information. It monitors threats to freedom of expression nationally and globally, develops long-term strategies to address them and advocates for the implementation of the highest standards of freedom of expression. **EFF** is a non-profit legal and policy organisation that safeguards freedom of expression and privacy in the digital world. It regularly files amicus curiae or intervener briefs in court cases of consequence regarding freedom of expression. EFF's briefs seek to inform courts about Internet technologies and the broader consequences of laws and decisions affecting those technologies. **Access Now** is a global civil society organisation dedicated to defending and extending the digital rights of users at risk. Through representation in ten countries, it provides thought leadership and policy recommendations to the public and private sectors to ensure the Internet's continued openness and universality and wields an action-focused global community of nearly half a million users. **RSF** is a French not-for-profit type organisation which defends and promotes freedom of the press, freedom of information, and fights for the safety of journalists and others who contribute to collecting and disseminating information of public interest, worldwide.

[2] Application Numbers 12468/15, 23489/15 and 19074/16.

[3] Application Number 20159/15.

[4] Application Number 61919/16.

[5] ARTICLE 19 and EFF have submitted an intervention in those proceedings.

[6] Some reports consider violent terrorism to be an 'elusive concept;' see, e.g., the Office for Democratic Institutions and Human Rights of the OSCE, Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community Policing Approach (2014), p. 35.

[7] See, for example, A/Res/68/127; available at http://bit.ly/1MX8mlg.

[8] UNSC Resolution 2178 (2014); available at http://bit.ly/1EJ51QW. The Resolution "underscores that countering violent extremism, which can be conducive to terrorism, including preventing radicalization, recruitment, and mobilization of individuals into terrorist groups and becoming foreign terrorist fighters is an essential element of addressing the threat to international peace and security posed by foreign terrorist fighters, and calls upon Member States to enhance efforts to counter this kind of violent extremism."

[9] See e.g. Counter-Terrorism Implementation Task Force, *First Report of the Working Group on Radicalisation and Extremism that Lead to Terrorism: Inventory of State Programmes;* available at http://bit.ly/1NFVnRm.

[10] For more information about the Global Counter-Terrorism Forum, see http://bit.ly/1NFVoVj. See also Global Counterterrorism Forum, the Ankara Memorandum; available at http://bit.ly/1PQeT23.

[11] See e.g. UNODC, *Frequently Asked Questions on International Law Aspects of Countering Terrorism*, 2009, p.4; available at http://bit.ly/1PQeTiC. See also UNODC, *The Use of the Internet for Terrorist Purposes*, 2012, para 49; available at http://bit.ly/1X1yiTo.

[12] UN GA, Plan *of Action to Prevent Violent Extremism*, 24 December 2015, UN doc A/70/674, para 5; available at http://bit.ly/1n0F1wu.

[13] Human Rights Council resolutions 26/13 and 32/13; General Assembly resolution 68/167; Report of the Special Rapporteur on FOE, 11 May 2016, A/HRC/32/38, para 6.

[14] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 22 February 2016, UN doc. A/ HRC/31/65, sec.1, §38 p.14; available at http://bit.ly/2FpXxbV.

[15] HR Committee, *Velichkin v. Belarus*, Communication No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

[16] Human Rights Committee General comment No. 34, §23; see also UN doc.A/71/373, para 26.

[17] Joint Declaration on Freedom of Expression and countering violent extremism, adopted on 4 May 2016 by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information; available at . http://bit.ly/2c09lVC.
[18] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 22 February 2016, UN doc. A/HRC/31/65, para 38; available at http://bit.ly/2EugVDo.
[19] *Ibid.*, para 40.
[20] ARTICLE 19, The Johannesburg Principles on Freedom of Expression and National Security, available at http://bit.ly/1Oi176F.
[21] *Ibid.*, Principle 2b.
[22] *Ibid.*, Principle 7b.
[23] European Court of Human Rights, *Handyside v the UK*, judgment of 6 July 1976, para.56
[24] See UN Rabat Plan of Action (2012), available at http://bit.ly/1T2efOV.
[25] *Ibid.*, para 29.
[26] Report of the Special Rapporteur on FOE, 6 September 2016, UN doc. A/71/373, paras 18-19, 23; available http://bit.ly/2DgUkLi.
[27] Statement by the UN Special Rapporteur on FOE, Countering violent extremism, a 'perfect excuse' to restrict free speech and control the media – UN expert, 3 May 2016; available at http://bit.ly/2CYENmj.
[28] *Ibid.*
[29] *Ibid.*
[30] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/31/65, 22 February 2016; available at http://bit.ly/2muCJIw.
[31] Examples include the Europol Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda and United Kingdom Counter-Terrorism Internet Referral Unit.
[32] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 22 February 2016, UN doc no .A/HRC/31/65, sec.1, para 40; available at http://bit.ly/2EugVD.
[33] App. No. 3111/10, paras 31-37, ECHR 2012
[34] See Council of Europe, *Study on filtering, blocking and takedown of illegal content on the Internet*, June 2016; available at: http://bit.ly/28fwhWS.
[35] *Ibid.*, Executive Summary, available from here: https://rm.coe.int/168068511c
[36] *Ibid.*, Comparative analysis, available from here: https://rm.coe.int/16806575b4
[37] *Op.cit.*, para 3 a).
[38] Report of the Special Rapporteur FOE, 16 May 2011, UN doc. A/HRC/17/27. Sec.A, para 29;, available at http://bit.ly/QD35W5.
[39] *Ibid*, para 31.
[40] *Ibid*, paras 36-37.
[41] *Cartier International AG v British Sky Broadcasting Ltd [2014] EWHC 3354* (Ch), para 189; available at http://bit.ly/1t27hig.
[42] See *Cumhuriyet Vakfi and Others v. Turkey*, App. No 28255/07 ECHR 2013. The European Court held that Turkish courts injunction against a daily newspaper preventing some further publication had not been proportionate because the scope of the injunction had been unclear but potentially extremely wide.
[43] See, among many other authorities, *RTBF v. Belgium*, App. no. 50084/06, para 103, ECHR 2011
[44] See e.g. ECtHR, *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, ECHR 2015
[45] See Recommendation CM/Rec(2008)6, Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, adopted on 26 March 2008, Section I. and Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines, section III, §16.
[46] Ibid., *Recommendation* CM/Rec(2008)6, Section III (ii) and *Yildirim v Turkey*, *op.cit*, para 64
[47] See A/66/290, *Report of the Special Rapporteur on FOE*, 10 August 2011, para 81.
[48] General Comment 34, *op.cit.*, para 30.
[49] Concluding observations on the Russian Federation (CCPR/CO/79/RUS).
[50] *Yildirim v Turkey*, *op.cit*, para 66.