IN THE EUROPEAN COURT OF HUMAN RIGHTS **App No. 10795/14**

KHARITONOV
- v –
RUSSIA

THIRD PARTY INTERVENTION SUBMISSIONS
BY ACCESS NOW

Introduction

1. This third party intervention is submitted on behalf of Access Now, hereafter "the Intervener" or "Access Now".
2. The Intervener welcomes the opportunity to intervene as third party in this case, by the leave of the President of the Court, which was granted on 6 September 2017 pursuant to Rule 44 (3) of the Rules of Court. These submissions do not address the facts or merits of the applicant's case.
3. Access Now is a global civil society organisation dedicated to defending and extending the digital rights of users at risk.[1] Through representation in 10 countries around the world – including in the European Union – Access Now 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 from more than 185 countries. Access Now also operates a 24/7 digital security helpline that provides real-time direct technical assistance to affected communities and vulnerable persons around the world. Access Now is non-partisan, not-for-profit, and not affiliated with any country, corporation, or religion.
4. Access Now has previously submitted third party interventions with the Court in Delfi v. Estonia (Application No. 64569/09), Magyar Jeti v. Hungary (Application No. 11257/16, Big Brother Watch and Others v. the United Kingdom (Application No. 58171/13) and in Navalnyy v. Russia (Application No. 62670/12). In addition to third party interventions with the Court, Access Now routinely files amicus briefs in the United States and in other countries such as Cameroon. In 2016, Access Now was granted special consultative status to the UN Economic and Social Council (ECOSOC).
5. The present case implicates human rights to freedom of expression and access to information for internet users around the world. The case concerns whether and under what circumstances website blocking is compatible with Article 10 of the Convention.
6. The impact of website blocking and consequent collateral website blocking can only be considered and assessed in the larger context of freedom of expression online and its existing limits, whether disproportionate or not. These limits range from content regulations related to hate speech, copyright, countering terrorism and violent extremism, through banning VPNs and internet anonymisers to internet shutdowns.
7. The intervener's submissions will focus on (1) how the problem of potentially harmful content can be solved in a right respecting fashion in democratic states; (2) what the minimum safeguards are for online content restrictions in order to be considered proportionate and necessary in a democratic society; and (3) what technical measures are

available to avoid or to minimise collateral website blocking and mitigate its adverse interference with human rights.

I. Addressing potentially harmful content in a human rights respecting fashion

Freedom of Expression restrictions online related to website blocking

8. This case provides the Court with the opportunity to "define the limits of permitted state interference in the online environment." Access to the free and open internet is not only an enabler of the full enjoyment of freedom of information but also a precondition of exercising freedom of expression. Disproportionate and/or unnecessary restrictions on these rights also undermine other values guaranteed by the Convention, and consequently the functioning of democratic societies. The geographic impact of the case and the underlying issues go beyond the question whether the Russian laws and practices around website blocking are permissible under the Convention. There are similar legislative measures and approaches by governments and state authorities around the world, and member states of the Council of Europe in particular, to block websites without adequate legal and technical safeguards. Case studies and legal cases include Turkey, Ukraine, Hungary, and more.[2]
9. To assess the proportionality and necessity of a restriction on freedom of expression, including website blocking, both procedural and substantive elements must be taken into account thus the question of "what" the website blocking is applicable to and "how".
10. The "what" starts with vague and varying definitions. The different definitions and legal standards for harmful or illegal content is extremely problematic especially in countries where the government is systematically suppressing dissent. The fragmentation of the legal basis for considering content illegal and what kind of illegal content can be subject to measures such as website blocking or content takedown, and the use of disproportionate restrictions have only grown since the Court recognised this situation in Ahmet Yildrim v. Turkey (Application no. 3111/10).
11. *Hate speech and countering violent extremism online*
12. Countering illegal hate speech and violent extremism are also "popular" objectives for governments to introduce freedom of expression limitations. The most recent national level law to tackle illegal online content and hate speech in particular was the German "Enforcement on Social Networks", also known as the "NetzDG".[3] In the absence of Europe wide consensus on hate speech regulation (see the discussion of the 'Code of Conduct' below in para 37) the European Union is exploring different solutions often without proper harmonisation and dialogue.[4]
13. Governments, policymakers, and law enforcement across the world are showing increased interest in pushing for proactive monitoring, surveilling, censoring, or otherwise modifying certain types of online content, under the broad rubric of "preventing" or "countering" violent extremism (PVE or CVE).[5] CVE-related proposals that include plans for proactive removal of content, manual or algorithmic "de-prioritisation" of content, or other types of interference with content, may appeal to governments concerned about violent extremism. However, these approaches directly impact the right to free expression. And just like there is no "magic key" to ensure that only a trusted government can break encryption to access Protected Information, there is no "magic eraser" to allow companies automatically to identify and remove or de-prioritise only illegal content.
14. Governments may also pursue mass take-down requests for content that is alleged to encourage violent extremism. This includes the increasingly popular practice of creating so-called internet referral units, through which a large number of takedown requests are

sent to companies outside the channel for legal removal requests.[6] Such mass takedowns can often be counterproductive, risking silencing voices seeking to respond to or counter violent extremist narratives. Content should not be removed until it is specifically adjudicated as being illegal, in line with international standards in this area (see Section II below).

15. If a company engages in a CVE programme, the company and those who review content (whether employees or contractors) cannot be tasked with the primary duty of evaluating the legality of content in the absence of rule-of-law mechanisms. When companies review complaints regarding content, it's necessary for staff to be well-trained to consider context and other factors. If a company uses content-flagging tools for a CVE programme, use of these tools should be limited to drawing reviewers' attention to content, not automatically flagging and taking down content, nor automatically suspending accounts. These reviewers must receive training on applying human rights standards — within the framework of local contexts — in addition to other kinds of support and resources.
16. Additionally, reviewers cannot be placed in situations where they are asked to act as editors, choosing to keep some categories of content online while removing others based on "countering violent extremism" strategies.[7] Such practices can result in reviewers or moderators knowingly or unknowingly chilling free expression, as well as suppressing satire or other kinds of speech seeking to respond to or counter calls to violent extremist action. Their role should remain focused on taking down content when they are notified that it explicitly violates their terms of service, or when they receive legal process requiring access to content be suspended or disabled. It's misleading to argue for countering violent extremism online using technical solutions such as filtering or proactive content takedown simply because they're used in other situations (for example, in the context of removing child sexual abuse material).
17. These methods are also a poor policy choice. They have a demonstrably high false positive rate (particularly for content outside of specifically blacklisted child sexual material), and do not suit situations that lack a clear definition for content, context, or legal mandate.[8] Even in "emergency" situations, we cannot suspend human rights protections. Governments and public officials are sometimes confronted with situations pertaining to online content and violent extremism that they regard as fast moving, and with potential negative consequences for the safety of citizens and public order. Policy planning for such situations should be underpinned in legal mechanisms that allow for rapid responses while ensuring that procedural safeguards are in place and the requirements of international human rights law are met.[9] It is not acceptable to implement state-operated mechanisms or other arrangements in the absence of law.
18. One specific risk of CVE based restrictions is the growing trend to label and discredit certain dissenting or marginalised groups as extremists or terrorists. One key target of such government action is civil society organisations in a number of Council of Europe member states including Hungary and Russia. In particular those that have a human rights mission and a watchdog function. Independent civil society is necessary for a functioning democracy and it has a key role to ensure that both private and public actors respect and promote digital rights and human rights in general. NGOs have always operated under difficult conditions but the level of attacks have intensified and reached the European Union as well. The threats and attacks include legislating against NGOs, government funded smear campaigns, undermining funding sources, secret surveillance measures, imposing administrative procedures and carrying out police raids. We are all responsible to stand up for the values and principles NGOs represent and to fight for their rights the same way they have been fighting for ours.[10]
19. *Copyright notice and takedown and EU reform upload filtering*

20. The European Commission has set in its agenda reforming copyright as one of the foundations to build the Digital Single Market. In September 2016, the European Commission published its proposal for a new Copyright Directive that aims at modernising EU copyright rules. The proposal has received mixed responses so far in the European Parliament and heavy criticism from academics, civil society and many industry members.
21. From a freedom of expression perspective the most problematic article of the proposal is Article 13 which introduces new obligations on internet service providers that share and store user-generated content, such as video or photo-sharing platforms or even creative writing websites, including obligations to filter uploads to their services. Article 13 appears to provoke such legal uncertainty that online services will have no other option than to monitor, filter and block EU citizens' communications if they are to have any chance of staying in business.[11] The legislation is awaiting a vote in the Legal Affairs Committee of the EU Parliament and it is still a long process for it to become a law. In its current form, however, (1) it would violate the right to freedom of expression set out in the Charter of Fundamental Rights; (2) provoke such legal uncertainty that online services would have no other option than to monitor, filter and block EU citizens' communications; and (3) includes obligations on internet companies that would be impossible to respect without imposing excessive restrictions on citizens' fundamental rights.

22. Barriers to anonymity online

23. In June 2017 Russian lawmakers unanimously adopted the first reading of legislation to ban VPNs and Internet anonymisers. The objective of the law is to "ban technologies that make it possible to circumvent Internet censorship".[12] In the law's explanatory note, the Duma deputies argue that Russia's existing system to block illegal content on the Web is "not effective enough."

24. Internet shutdowns

25. Internet shutdowns represent an extreme form of censorship that, unfortunately, more governments around the world wield with alarming regularity. The UN describes internet shutdowns as measures that "aim to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law" (A/HRC/RES/32/13). According to the definition developed by Access Now and the global #KeepItOn Coalition of 137 organizations, an internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.[13] In other words an internet shutdown happens when someone — usually a government — intentionally disrupts the internet or mobile apps to control what people say or do. Shutdowns are also sometimes called "blackouts" or "kill switches".
26. Access Now identified 55 internet shutdowns in 2016, and 61 in the first three quarters of 2017. At least 30 countries experienced internet shutdowns in 2016 and thus far in 2017[14]
27. In practice, shutdowns disproportionately prevent access to infrastructure like cell towers or fiber optic cables, online communications platforms like messaging applications or social media websites, or traditional telecom services like SMS or voice telephony. The disruptions obstruct access to information, often during times of crisis or instability, and also prevent commerce, social, and cultural exchange across borders and within nations.[15] Blunt censorship like shutting down channels of communication does not satisfy the 3-part test for restrictions on expression, including the necessity prong, nor is it the least restrictive means available to achieve a legitimate aim. For these reasons, the UN Human Rights Council "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights

law and calls on all States to refrain from and cease such measures."[16]

28. Website blocking bears many worrisome similarities to internet shutdowns. For example, both measures tend to bar access to information on a massive scale, inevitably interfering with the legitimate exercise of freedom of expression. Likewise, both methods target communications channels and platforms, rather than specific content, with long term impacts on the restricted sites. As more sites adopt interactive features, blocking URLs -- like cutting mobile voice or data connections -- restricts multiple speakers from imparting and receiving information, not simply the site's owner or operator.

Implications of website blocking measure on other human rights and democratic principles

29. *The right to privacy in relation to website blocking*
30. Website blocking measures often entail social media monitoring, algorithmic content reporting, or content referral programmes, in order to identify content that may trigger content or account removal as well. Surveillance of this sort can have a disparate impact on users at risk, including but not limited to vulnerable groups such as journalists and activists, communities of colour, persecuted religious groups, and members of LGBTQI communities. Human rights experts have specifically noted the concern raised by basing surveillance on ethnic or religious profiling, and the targeting of whole communities rather than specific individuals.[17]
31. If governments deputise companies and individual users to conduct monitoring — or undertake the monitoring themselves, there must be adherence to international human rights law and comparative global standards, including the International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate" principles), which has 13 principles: Legality, Legitimate Aim, Necessity, Adequacy, Proportionality, Competent Judicial Authority, Due Process, User Notification, Transparency, and Public Oversight, Integrity of Communications and Systems, Safeguards for International Cooperation, and Safeguards Against Illegitimate Access.
32. Government-run or state-supported programmes for online tracking and monitoring can have serious repercussions. To monitor social media en masse is to treat all users like suspects, which has a chilling effect on human rights such as the rights to privacy, free speech, and access to information. It also discourages trust in the internet economy. In practice, such large-scale monitoring of a vaguely defined category of content subject to website blocking can — and often is — applied with a discriminatory impact that adversely affects people in social movements, such as those advocating for racial and gender equality and criminal justice.
33. Tools such as algorithmic content flagging also carry high risks with respect to the likelihood of false positives. This may further exacerbate the negative impact of such programmes, including further radicalising communities, silencing others, and undermining global trust in the opportunities for communication and open dialogue that the internet provides.
34. Whenever a website blocking measure entails tracking or monitoring it must be subject to the same normative and legal restrictions applicable to communications surveillance in other contexts.
35. *The rule of law and privatised enforcement*
36. Recurring elements of the above described content regulation measures that the Court should consider include the problematic role of private actors in the enforcement process. Internet companies - both internet service providers and Over the Top service providers - are put in the center of the practical and legal application of content regulations which creates overbroad and unclear censorship powers and obligations for these companies.

This phenomenon is prevalent both on the broader European Union level and also on the national level in Council of Europe member states.

37. In the European Union existing frameworks such as the European Commission's Hate Speech Code of Conduct are built on voluntary self-regulation measures on the basis of the private companies' terms and services rather than rule of law. The lack of clarity of application of rules set out by these private policies, and of adequate due process safeguards and effective remedies for individuals result in violations of human rights standards. The Code of Conduct downgrades the law to a second-class status, behind the "leading role" of private companies that are being asked to arbitrarily implement their terms of service. This process, established outside an accountable democratic framework, exploits unclear liability rules for online companies. It also creates serious risks for freedom of expression, as legal — but controversial — content may well be deleted as a result of this voluntary and unaccountable take-down mechanism.[18]
38. To avoid different forms of intermediary liability - such as fines - internet companies are encouraged by governments to voluntarily censor more content than it was strictly necessary. The first report after the review process of the Code of Conduct shows that the metrics are flawed from a human rights perspective. The Commission is taking into account the progress in terms of time (how fast the company took down, blocked or filtered the potentially unlawful content) and number of such actions. The examination of lawful or unlawful nature of the content that was or was supposed to be taken down is marginal. The chilling effect of rewarding "overcompliance" might be even bigger than we think since there is no mandatory reporting mechanism and criteria on takedowns on the basis of terms and service violations.
39. Beyond the serious limitations on the availability of adequate information for the general public, terms and service based takedowns also prevent law enforcement to understand the landscape of illegal content online or to prosecute criminal actions. Voluntary and self-regulatory rules offer no remedies for individuals either as being victims of criminal activities or of the overbroad takedown practices companies. With encouraging privatised enforcement, and disproportionate privatised enforcement in particular, states violate their positive obligation to protect and promote human rights. Governments therefore must avoid coercion of private industry to undermine free expression protections. Governments must not compel companies to conduct programmes to counter violent extremism, either by advancing new legislation or by threatening to screen or censor speech outside of legal process.[19]
40. Further evidence shows that in relation to "violent extremism" mass take-down initiatives that take place outside of legal process frustrate corporate transparency and are not likely to deter the cultivation of "violent extremism", and in fact may encourage it, inflaming resistance and helping "violent extremist" recruiters discredit platforms that might otherwise support online expression and debate.[20]
41. Considering the above trends courts should apply strict scrutiny over freedom of expression restrictions to amplify the effect of human rights standards as enforced by the judiciary as opposed to private actors.

II. Safeguards for online content restrictions in order to be considered proportionate and necessary in a democratic society

42. International human rights standards for the necessity and proportionality test regarding limitations on freedom of expression and website blocking are flashed out by other interveners in the case.[21] Therefore, we will only touch on those standards briefly to emphasise their importance.

43. Internet shutdowns categorically fail to uphold international human rights norms. International human rights law holds a standard three-part test for restrictions on freedom of expression. To justify their interference with human rights, the restrictions must be (1) provided by law; (2) strictly pursuant to a legitimate aim, as delineated in Article 19 (3) of the ICCPR; and (3) necessary and proportionate to achieve that aim, using the least intrusive means possible.
44. Applying this test, in 2011, the UN Special Rapporteur on freedom of opinion and expression, the African Commission Special Rapporteur on Freedom of Expression and Access to Information, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, and the Organization of American States (OAS) Special Rapporteur on Freedom of Expression jointly declared that the;

> *"[c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds. The same applies to slow-downs imposed on the Internet or parts of the Internet."*[22]

45. The special experts also declared that the;

> *"[m]andatory 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."*[23]

46. A website blocking measure must comply with the three-part test for restrictions on freedom of expression under Article 19(3) ICCPR. The then-UN Special Rapporteur on freedom of expression, Frank La Rue, clarified in his report of May 2011 specific requirements to do so: (1) Blocking and filtering provisions should be clearly laid out by law; (2) Any determination of what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences; (3) Blocking orders must be strictly limited in scope in line with the requirements of necessity and proportionality under Article 19 (3); (4) Lists of blocked websites together with full details regarding the necessity and justification for blocking each individual website should be published; (5) An explanation should also be provided to the affected websites as to why they have been blocked.
47. Special Rapporteur Frank La Rue's 2011 report also spoke directly to the over-blocking that can result even from blocking orders with legitimate purposes:

> "*Even where a legitimate aim 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*."[24]

48. In addition, as General Comment 34 points out:

> "*Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3. **Permissible restrictions generally should be content-specific**; generic bans on the operation of certain sites and systems are not compatible with paragraph 3 [of Article 19]".*
>
> Collateral website blocking is not content-specific, and likely does not fall within the strictly-construed categories of excepted restrictions on expression permissible under Article 19(3) of the ICCPR.

49. Special Rapporteur David Kaye reported to the UN on safeguards to ensure states do not infringe freedom of expression through their demands on ICT companies:

a. "*States must not require or otherwise pressure the private sector to take steps that unnecessarily or disproportionately interfere with freedom of expression, whether through laws, policies, or extralegal means. 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. Particularly in the context of regulating the private sector, State laws and policies must be transparently adopted and implemented.*"

50. Consistent with this approach, this Court in Yildirim v. Turkey (no. 3111/10) has previously held that "the Internet has now become 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".
51. The Council of Europe commissioned a recent comparative study on blocking, filtering and take-down of illegal content. The report shows different approaches between countries that have specific legal frameworks on the issue of blocking, filtering and take-downs and the ones, self regulations and no legislations. The study also explores considerations for freedom of expression such as voluntary blocking, the assessment of legal basis and removal of content.[25] As Nils Muižnieks, Council of Europe's Commissioner for Human Rights, has put it "It is high time that member states stop relying on or encouraging private companies to regulate the online communication space without ensuring themselves that human rights are protected and that due process guarantees are upheld in line with the European Convention on Human Rights".[26]
52. The European Union adopted the Regulation 2015/2120 on net neutrality and the open internet which contains rules on website blocking[27]. The default binding rule in the EU is the prohibition of website blocking. Recital 3 of the regulation offers a background on why the legislator believes that the open internet is necessary and beneficial and why therefore we need to prevent blocking.

    "*The internet has developed over the past decades as an open platform for innovation with low access barriers for end-users, providers of content, applications and services and providers of internet access services. The existing regulatory framework aims to promote the ability of end-users to access and distribute information or run applications and services of their choice. However, a significant number of end-users are affected by traffic management practices which block or slow down specific applications or services. Those tendencies require common rules at the Union level to ensure the openness of the internet and to avoid fragmentation of the internal market resulting from measures adopted by individual Member States.*"

53. Recitals 11-17 complement Article 9 which sets out the prohibition of website blocking and the exceptions to that rule. Website blocking is not permitted unless it is transparent (specific requirements around transparency in Article 4), non-non-discriminatory, limited in time, proportionate, does not lead to the monitoring of the content, the blocking is not for commercial purposes, and the blocking falls under the exceptions in Article 3 para 3 (a)-(c). Article 3 of the regulation sets out the safeguards of open internet access.

    "Providers of internet access services shall treat all traffic equally, when providing internet access services, without discrimination, restriction or interference, and irrespective of the sender and receiver, the content accessed or distributed, the applications or services used or provided, or the terminal equipment used. The first subparagraph shall not prevent providers of internet access services from implementing reasonable traffic management measures. In

order to be deemed to be reasonable, such measures shall be transparent, non-discriminatory and proportionate, and shall not be based on commercial considerations but on objectively different technical quality of service requirements of specific categories of traffic. Such measures shall not monitor the specific content and shall not be maintained for longer than necessary. Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to: a. comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers; b. preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users.

54. As a global example for similar trends and threats to freedom of expression internationally, Cameroon courts reviewing their government's recent order to shutdown the internet, Access Now submitted evidence that the blocking violated freedom of expression:

> *Measures amounting to internet service disruption, website blocking, and online "kill switches" or "shutdowns" have been widely condemned by international, regional and domestic courts and human rights bodies. ... [T]he uniquely valuable role that the internet plays in facilitating free expression has been internationally recognized and is relevant to considering the necessity of restrictions on access to the internet. Furthermore, international and regional courts and human rights institutions have determined that disrupting or blocking internet access are incompatible with the right to free expression. These findings are based primarily on the basis that such actions are not "provided by law", or are an unnecessary and disproportionate means of achieving their aim.*

55. In November 2016, the African Commission adopted a Resolution in which it expressed its concern over, "*the emerging practice of State Parties of interrupting or limiting access to telecommunication services such as the Internet, social media and messaging services, increasingly during elections*".[28]

56. In its March 2015 judgment in *Shreya Singhal* v. *Union of India*, Justice Rohinton Nariman stated on behalf of the Supreme Court of India that India's constitutional protection to free speech applied to internet communication as well, and that Section 66A of India's Information Technology Act - which criminalised the sending of "offensive messages" - had to be struck down since the overbroad criminalisation of speech and resulting chilling effect would "fall foul of the repeated injunctions of this Court that restrictions on the freedom of speech must be couched in the narrowest possible terms".[29]

III. Technical measures to avoid or to minimise collateral website blocking and mitigate its adverse interference with human rights

57. Website blocking interferes with human rights, most directly the freedoms of opinion, expression, and access to information, and also the right to association and a host of economic, social, and cultural rights. Collateral website blocking likewise interferes with human rights.
58. The Internet Society (ISOC) recently identified common methods of blocking online content: IP and Protocol-Based Blocking; Deep Packet Inspection-Based Blocking;

Platform-Based Blocking; DNS-Based Content Blocking; and Infrastructure Disruption.[30]

59. According to the Internet Society, "Our conclusion, based on technical analyses, is that using Internet blocking to address illegal content or activities is generally inefficient, often ineffective and generally causes unintended damages to Internet users."[31]
60. We concur in that finding. While it is possible that the interference may be mitigated through technical measures taken by various intermediaries that reduce the scope, scale, and impact of the blocking, this comes down to a case-by-case determination. Thus, we recommend that courts who order blocking and other interference with access to content online always invite technical experts, from the private and civil society sectors, to inform the court on the potential impacts of the blocking, and methods to mitigate and sufficiently target the order to ensure its implementation does not interfere with access to information and other human rights.

IV. Conclusion

61. Content regulation measures lack a global standard for speech limitation on the substance of "what" can be subject to blocking, filtering or takedown but there are existing global human rights rules and criteria for the "how" and "why".
62. Based on the different level of ambiguity around the alleged illegality of the specific content (including defamation, hate speech, copyright, child pornography etc.) the level of safeguards and protections must be adjusted. The more arguable the unlawful nature of the online content, the higher the criteria and safeguards against any restrictions should be.
63. On that scale website blocking is a very serious interference with the right to freedom of expression. For this reason, as it draws from international human rights law standards including established case law, website blocking interferes with the core essence of the right to freedom of expression and the Court should apply a strict assessment for its necessity and proportionality. Beyond a basis in law, being ordered by a court (or other independent body), concerned individuals must be notified and granted with adequate remedies to challenge website blocking measures.
64. The issues the Court is being asked to rule upon in Kharitonov v. Russia implicate human rights to freedom of expression and and access to and freedom of information for internet users around the world. The internet empowers individuals and enables citizens to take part in struggles for justice, participate in society, and realise human rights around the globe. But government enabled censorship risks turning the internet into a tool of repression, and quells political dissent and the spread of nonconforming ideas. Human rights must be promoted and protected equally on the internet as they have traditionally been implemented in the physical world.

Fanny Hidvegi, European Policy Manager and Legal Counsel
Peter Micek, General Counsel and Global Policy Lead - Business and Human Rights

Access Now

17 October 2017

[1] https://www.accessnow.org/about-us/

[2] https://tasz.hu/informacioszabadsag/nem-teljes-titok-tobbe-mediahatosag-internetes-feketelistaja

[3] TechCrunch, Germany's social media hate speech law is now in effect, 2 Oct 2017, https://techcrunch.com/2017/10/02/germanys-social-media-hate-speech-law-is-now-in-effect/.

[4] EDRi, Commission's position on tackling illegal content online is contradictory and dangerous for free speech, 28 Sept 2017, https://edri.org/commissions-position-tackling-illegal-content-online-contradictory-dangerous-free-speech/.

[5] Access Now Position Paper, A digital rights approach to proposals for preventing or countering violent extremism online, 2016, https://www.accessnow.org/cms/assets/uploads/2016/10/CVE-online-10.27.pdf.

[6] For examples of this and the concerns triggered for digital rights, see Access Now, Europol's Internet Referral Unit risks harming rights and feeding extremism, 17 June 2016, https://www.accessnow.org/europols-internet-referral-unit-risks-harming-rights-isolating-extremists/.

[7] Such steps must also be avoided due the impact they would have on the legal position on internet intermediaries, given that many jurisdictions across the world possess legal provisions that provide a limited "safe harbour" protection to intermediaries for third party or user generated content — but often subject to the requirement that they do not interfere or editorially engage with the content in question.

[8] Many of these proposals also fail to note that the usage of such technical tools to detect and report child sexual abuse material was developed in the specific context of legal regimes across most countries criminalising the very possession of such material, under provisions meant to combat child pornography or sexual abuse.

[9] The framing of any such legal models must be approached cautiously. Many proposals may grant certain public officials the power to issue emergency web content blocking orders, which are then post-facto reviewed by review committees or other authorities. One example of this is Section 69A of the Indian Information Technology Act and its implementing rules, which allow the issuance of emergency blocking orders which have to be later examined by a review committee. The operation of this review committee and the emergency blocking process has been criticised for being opaque and limiting itself to procedural review without any examination of the validity of blocking requests. See Human Rights Watch, Stifling Dissent The Criminalization of Peaceful Expression in India, 24 May 2016, https://www.hrw.org/report/2016/05/24/stifling-dissent/criminalization-peaceful-expression-india .

[10] Access Now, Silencing civil society in Hungary: how to fight back?, 28 Apr 2017, https://www.accessnow.org/silencing-civil-society-hungary-fight-back/.

[11] EDRi, Civil society calls for the deletion of the #censorshipmachine, 16 October 2917, https://edri.org/civil-society-calls-for-the-deletion-of-the-censorshipmachine/.

[12]https://meduza.io/en/news/2017/06/23/russian-lawmakers-adopt-first-reading-of-legislation-to-ban-vpns-and-internet-anonymizers

[13] https://www.accessnow.org/keepiton/

[14] *See* Access Now, "Shutdown Tracker Optimization Project (STOP)," available at https://www.accessnow.org/keepiton-shutdown-tracker.

[15] For more information on one shutdown in Togo, and its impacts on people's lives, see "Dispatches from an internet shutdown — Togo," https://www.accessnow.org/dispatches-internet-shutdown-togo.

[16] A/HRC/RES/32/13, at para. 10.

[17] Joint Declaration on Free Expression and CVE, supra note 7.

[18] EDRi and Access Now withdraw from EU Commission discussion, 31 May 2016, https://www.accessnow.org/edri-access-now-withdraw-eu-commission-forum-discussions/.

[19] See Editorial Board of Pravoye Delo and Shtekel v. Ukraine, no. 33014/05, 5 May 2011, paras. 63-65

[20] See e.g., Kate Ferguson, Partnership for Conflict, Crime and Security Research University of East Anglia, Countering violent extremism through media and communication strategies: A review of the evidence, 1 March 2016, http://www.paccsresearch.org.uk/wp-content/uploads/2016/03/Countering-Violent-Extremism-Through-Media-and-Communication-Strategies-.pdf ("VE propaganda online has expanded in the face of CVE takedowns and counternarrative strategies"), and Colin Baulke, Mackenzie Institute, The Nature of the Platform: Dealing with Extremist Voices in the Digital Age, 8 May 2016, http://mackenzieinstitute.com/nature-platform-dealing-extremist-voices-digital-age/ ("... and to further complicate the problem, the impact of successful takedown campaigns is murky. In some extremist online circles, including ISIS, users view having a suspended account as a badge of honour. Essentially, increased suspensions equate to greater legitimacy.")

[21] https://www.article19.org/data/files/medialibrary/38859/170825-Submission-Kharitonov-v-Russia-A19EFF.pdf

[22] UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, OAS Special Rapporteur on Freedom of Expression and African Commission Special Rapporteur on Freedom of Expression and Access to Information, *Joint declaration on freedom of expression and the Internet*, 1 June 2011, par. 6(b).

[23] *Id*., par. 3(a).

[24] United Nations Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/17/27 (2011), par. 31.

[25] Comparative study on blocking, filtering and take-down of illegal content, 20 Dec 2015, https://rm.coe.int/168068511c

[26] Arbitrary internet blocking jeopardises freedom of expression, 26 Sept 2017, https://www.coe.int/en/web/commissioner/-/arbitrary-internet-blocking-jeopardises-freedom-of-expression.

[27] REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union

[28] African Commission on Human and Peoples' Rights, Resolution on the Right to Freedom of Information and Expression on the Internet in Africa, 59th Ordinary Session, held Banjul, Islamic Republic of The Gambia, from 21 October to 04 November 2016, ACHPR/Res. 362(LIX) 2016.

[29] Shreya Singhal v. Union of India, (2015) 5 SCC 1, at para 86.

[30] Internet Society, *Internet Society Perspectives on Internet Content Blocking: An Overview*, published 24 March 2017, available at <https://www.internetsociety.org/resources/doc/2017/internet-content-blocking>.

[31] *Id*.