IN THE EUROPEAN COURT OF HUMAN RIGHTS
APP NO. 10795/14
BETWEEN:-

KHARITONOV

Applicant

- v -

RUSSIA

Respondent Government

THIRD-PARTY INTERVENTION SUBMISSIONS BY ARTICLE 19 AND THE ELECTRONIC FRONTIER FOUNDATION

-

INTRODUCTION

1. This third-party intervention is submitted on behalf of ARTICLE 19: Global Campaign for Free Expression (ARTICLE 19) and the Electronic Frontier Foundation ('EFF'), hereafter 'the Interveners'.

2. ARTICLE 19 is an independent 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. ARTICLE 19 monitors threats to freedom of expression in different regions of the world, as well as national and global trends and develops long-term strategies to address them and advocates for the implementation of the highest standards of freedom of expression, nationally and globally.

3. The Electronic Frontier Foundation is a non-profit legal and policy organization that safeguards freedom of expression and privacy in the digital world. EFF regularly files amicus curiae or intervener briefs in court cases of consequence regarding freedom of expression. Drawing on the expertise of its attorneys and staff technologists, EFF's briefs seek to educate courts about Internet technologies and the broader consequences of laws and decisions affecting those technologies.

4. The Interveners welcome the opportunity to intervene as third parties in this case, by the leave of the President of the Court, which was granted on 6 July 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.

5. The present case concerns the compatibility of a sweeping website blocking order made by the Russian authorities with the requirements of Article 10 of the Convention. Russian law presently allows the wholesale blocking of websites by governmental bodies, irrespective of the number and nature of different websites that might share the

same IP address (so-called 'collateral' victims of overbroad blocking measures). This case also concerns the lack of effective remedies for such collateral victims, contrary to Article 13 taken in conjunction with Article 10 ECHR.

6. The Interveners believe that the present case is significant because it is the first case in which the Court will be called upon to examine the Russian legal framework which grants far-reaching powers to a government agency to block websites. As such, it represents a test case for the protection of freedom of expression online in Russia.

7. In these submissions, the Interveners address the following: (i) international standards on the importance of the right to impart and receive information online; (ii) international and comparative law standards on website blocking measures, with a focus on regulatory approaches and remedies for violations of the right to freedom of expression as a result of website blocking; and (iii) the proper approach to cases involving website blocking, including an approach to the problem of overbroad blocking and collateral harm.

I. THE IMPORTANCE OF FREEDOM OF EXPRESSION ONLINE

The right to receive and impart information online must be strongly protected

8. The importance of the Internet as a medium for sharing and disseminating ideas has been widely recognised at international and European levels. In his 2011 report on freedom of expression and the Internet, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, noted that the Internet has become "*one of the most powerful instrument for…increasing access to information, and for facilitating active citizen participation in building democratic societies*",[1] and is "*a key means by which individuals can exercise their right to freedom of expression"*.[2] The Special Rapporteur further noted "*the vast potential and benefits of the Internet … rooted in its unique characteristics, such as its speed, worldwide reach and relative anonymity"*.[3]

9. Similarly, the Joint Declaration on Freedom of Expression and the Internet – issued by the four special mandates on freedom of expression in June 2011 – stressed *'the transformative nature of the Internet in terms of giving voice to billions of people around the world, of significantly enhancing their ability to access information and of enhancing pluralism and reporting'.*[4] It also advocated that greater attention be dedicated to *"developing alternative, tailored approaches, which are adapted to the unique characteristics of the Internet, for responding to illegal content."*

10. In its General Comment No. 34 on Article 19 of the International Covenant on Civil and Political Rights 1966 ("ICCPR"), the UN Human Rights Committee also emphasised the importance of new information and communication technologies; it went on to urge States parties to take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto.[5]

11. Consistent with this approach, this Court 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*" (see *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 54, ECHR 2012, and *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom*, nos. 3002/03 and 23676/03, § 27, ECHR 2009). It has also found that States had a positive obligation to create an appropriate regulatory framework to protect journalists' freedom of expression on the Internet (see *Editorial Board of Pravoye Delo and Shtekel v. Ukraine,* no. 33014/05, 5 May 2011, paras. 63-65). More recently, it recognised that active users of Youtube could claim victim status in circumstances where they were unable to access the YouTube platform,

which had been blocked entirely by the Turkish authorities.[6] In light of the above, the Interveners submit that the importance of free expression justifies States being under a positive obligation to provide an effective remedy against wrongful and collateral website blocking (see part III further below).

Russia's track record in undermining freedom of expression online

12. The Interveners further submit that strong protection for the right to receive and impart information online takes on particular importance when set against the state of Internet freedom in Russia. Since 2012, Russia has adopted several laws, which have increasingly stifled freedom of expression online, including: [7]

    a) Federal Law № 139-FZ "On Introducing Amendments to the Law on the Protection of Children from Information Harmful to their Health and Development", which established for the first time a registry of websites deemed unlawful by Roskomnadzor, the federal government agency tasked with overseeing online content and mass media;
    b) Federal Law № 135 also known as the "gay propaganda ban", which mandates the blacklisting of "propaganda of non-traditional sexual relations";
    c) Federal Law № FZ-398 or "Lugovoi Law", which grants broad powers to the authorities to block access to online sources of information calling for "mass riots, extremist activities and unauthorized mass public events";
    d) The 2014 "Bloggers Law", which – among other things – required bloggers with more than 3,000 single visits per day to register with Roskomnadzor and imposed on them duties and responsibilities similar to that of the mass media. These provisions were recently repealed by Federal Law № 276-FZ (see below);
    e) Federal Law № 241-FZ, which bans anonymity for users of online messaging applications; and
    f) Federal Law № 276-FZ, which bans Virtual Private Networks and Internet anonymisers from providing access to websites banned in Russia.

13. Several other laws have been adopted between 2012 and 2017 that further criminalise expression[8] or unduly restrict the right to privacy by mandating the retention of vast amounts of data for long periods of time.[9] The upshot of this is that the Russian Internet, which until 2011 was considered to be relatively free, is now considered to be among the most restrictive.[10] Several human rights organisations, including Human Rights Watch, ARTICLE 19, EFF and Reporters Without Borders, among others, regularly voice their concern at the state of Internet freedom in Russia.[11] In particular, legitimate content is routinely blocked, either deliberately or as the collateral effect of overbroad measures. In this regard, the Council of Europe noted in a recent study on blocking, filtering and takedown on the Internet that Russia had extended the common grounds under which blocking may be legitimately authorized.[12] This is confirmed in Freedom House's 2016 Freedom on the Net report, which reported:[13]

> According to the nonprofit organization RosComSvoboda, which conducts ongoing monitoring of blocked content, the following were blocked by the end of May 2016:
>
> - 1,587 sites for extremism and calls for protests (by orders of Prosecutor General's Office)
> - 9,982 sites containing drug-related content (by orders of the Federal Drug Control Service)
> - 228 sites containing suicide propaganda (by orders of the Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing, or Rospotrebnadzor)
> - 5,253 sites for the distribution of child pornography (by orders of Roskomnadzor)
> - 9,593 sites for the publication of various prohibited information (based on court decisions)
> - 1,465 sites for copyright infringement (based on decisions of Moscow City Court)

- 6,313 sites for information about gambling (by orders of the Federal Tax Service).

14. In light of the above, the Interveners respectfully invite the Court to give the most anxious scrutiny to the Russian legal framework governing website blocking measures.

II. INTERNATIONAL & COMPARATIVE LAW STANDARDS ON WEBSITE BLOCKING MEASURES

International standards on website blocking

15. International human rights bodies have long expressed their deep concern about blocking and filtering measures. In particular, the four special mandates on freedom of expression held in their 2011 Joint Declaration on Freedom of Expression on the Internet:[14]

> 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. [emphasis added]

16. Similarly, the UN Special Rapporteur on freedom of expression, Frank LaRue, found in his report of May 2011:[15]

> 31. States' use of blocking or filtering technologies is frequently in violation of their obligation to guarantee the right to freedom of expression, as the criteria mentioned under chapter III are not met. 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, paragraph 3, of the International Covenant on Civil and Political Rights, 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 of achieving 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 or possibility of review by a judicial or independent body.

17. The UN Special Rapporteur made it absolutely clear that blocking measures must always comply with the three-part test under Article 19(3) ICCPR.[16] In this respect, he laid down some minimum criteria that must be met in order for website blocking and filtering to be justified under international law, namely:[17]

    (i) Blocking and filtering provisions should be clearly laid out by law;

    (ii) 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;

    (iii) Blocking orders must be strictly limited in scope in line with the requirements of necessity and proportionality under Article 19 (3);

    (iv) Lists of blocked websites together with full details regarding the necessity and justification for blocking each individual website should be published;

    (v) An explanation should also be provided to the affected websites as to why they have been blocked.

18. Similarly, the UN Human Rights Committee held in its General Comment no. 34: [18]

> 43. 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...

19. The above standards have been echoed by regional mechanisms for the protection of human rights, including the OAS Special Rapporteur on Freedom of Expression,[19] the Council of Europe[20] and the Court itself.[21]

20. Most recently, the Court of Justice of the European Union ('CJEU') held in the landmark *UPC Telekabel* case that the addressee of a copyright injunction had to ensure compliance with the fundamental right of internet users to freedom of information when choosing the appropriate measures to be adopted in order to comply with the injunction.[22] The CJEU went on to note:

> 56. In this respect, the measures adopted by the internet service provider must be strictly targeted, in the sense that they must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued. [emphasis added]

21. The CJEU concluded that in order to ensure that copyright injunctions complied with fundamental rights, national procedural rules had to provide a possibility for Internet users to assert their rights before the court once the implementing measures taken by the Internet service provider were known.[23] This requirement is reflected in the 2015 EU Regulation on Open Internet Access, which provides that "*national measures regarding end-users' access to or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, including in relation to privacy and due process, as defined in Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms*."[24]

Comparative law standards on website blocking

22. In *Ahmet Yıldırım v. Turkey*, the Court examined a number of comparative law materials on website blocking.[25] The Court concluded that the regulatory frameworks governing website blocking was highly 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.

23. Since then, the Council of Europe has conducted a comprehensive study of filtering, blocking and takedown of illegal content on the Internet, which was published in June 2016.[26] Among other things, the Council of Europe concluded:[27]

    (i) 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 usually rely on existing legislation to deal with the issues raised by illegal content on the Internet (the UK, Austria, the Netherlands, Ireland, Poland, the Czech Republic and Switzerland). In practice, this also means that the courts determine whether or not content is illegal and should be blocked.

    (ii) 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, national security, including terrorism, health and morals and "hate crimes". However, the COE noted that some countries,

such as Russia, had extended the common grounds under which blocking may be legitimately authorized to include e.g. homosexual propaganda.[28]

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

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

24. Of those countries, which have adopted a specific legal framework allowing website blocking, it appears that very few explicitly provide for "wholesale" blocking of websites or wholesale blocking of websites "sharing the same IP address". Turkey amended its legislation in order to provide explicitly for wholesale blocking of websites following the *Yildirim* judgment. In France, a special branch of the police can require ISPs to block access to "electronic addresses" whose content is in breach of the relevant laws on terrorism and child pornography. [29] The regulations specify that electronic addresses must contain either a domain name (DNS) or the name of a host in the form of a domain name and the name of a server.[30] In Spain, the courts can require ISPs to implement the voluntary measures imposed by the Intellectual Property Commission in order to enforce intellectual property rights. [31] This includes the "suspension" of access to information society providers. [32] However, such measures must be objective, proportionate and non-discriminatory.[33]

25. More generally, it appears that primary legislation seldom provides for the various criteria that should be taken into account before a blocking order can be made. For instance, the Spanish criminal code provides that an entire website may be blocked when it "predominantly" contains hate speech content.[34] However, it appears to be an isolated case. More details can sometimes be found in secondary legislation. In Italy, the Communications Authority "AGCOM" can order the blocking of an entire site in cases involving "massive" infringement of intellectual property rights.[35] Similarly, with some limited exceptions (Greece,[36] Italy[37], France[38]), the law is generally silent on the type of technology that may be used to comply with a blocking order.

26. By contrast, a great deal of guidance can be found in countries that have left the issuing of blocking orders to the courts, particularly in the area of intellectual property law.[39] For instance, in *Cartier International AG v BSkyB* before the High Court of Justice of England and Wales, Arnold J considered:[40]

> 189. For the reasons discussed above, I conclude that, in considering the proportionality of the orders sought by Richemont, 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;
> In addition, it is relevant to consider the substitutability of other websites for the Target Websites.

27. The application of these criteria, however, does not prevent the courts from ordering the blocking of entire websites if they conclude that it is appropriate to do so in the circumstances of the case. For instance, in the *Goldesel* case, the German Federal Court of Justice effectively concluded that the blocking of an entire website may be

permissible when the content of the site was mainly unlawful.[41] The courts of England and Wales[42] and Denmark[43] have reached similar conclusions. At the same time, the German decision made clear that website blocking should be used as a measure of last resort.

28. In addition, some courts have examined the kind of technology available to comply with their orders and determined which should apply in specific cases. In particular, some courts have expressly rejected the use of IP-address blocking and ordered the use of DNS blocking instead:

    (i) In a 2011 Pirate Bay judgment, the Antwerp Court of Appeal considered that IP-blocking had undesirable effects on third parties since it carried greater risks of blocking legitimate information. As such, DNS blocking, which carried less risk, was preferable.[44]

    (ii) In its judgment of May 2012 in *Dramatico v Sky (No. 2)*, the High Court of Justice of England and Wales noted: '*IP address blocking is generally only appropriate where the relevant website's IP address is not shared with anyone else. If it is shared, the result is likely to be overblocking*'. [45] Similarly, in *Cartier International v BSkyB*,[46] Arnold J accepted that IP-address blocking would not be appropriate when a target website for the purposes of a blocking order shares an IP-address with a legitimate website.

    (iii) In the decisions of the *Goldesel*[47] and *3dl.am*[48] cases, delivered on the same day, the Federal Court of Justice of Germany noted that IP-address blocking could lead to "overblocking", particularly when several websites shared a unique IP-address. [49]

    (iv) In a recent 2017 decision, the Swedish Patent and Trademark Courts of Appeal rejected the use of IP-blocking particularly in circumstances where the rights-holder had not provided sufficient evidence that the IP-addresses at issue were not shared with hosts of lawful content.[50]

29. By contrast, some courts have allowed IP-address blocking when they were satisfied that it would not affect lawful third party websites and that the rights of users would be protected. For instance, in the 11 November 2014 judgment in the *Cartier International v BskyB case,* Arnold J agreed that IP-blocking could be applied in circumstances where: (i) it was perfectly obvious that the website sharing an IP-address with a target website was engaged in 'unlawful activity'; (ii) the operators of the 'unlawful' websites would be given a seven-day grace period to move their site to another server or object before the IP address was blocked, in which case a determination would have to be made by the court. [51]

30. Notwithstanding the above, most judgments only tend to make reference to the particular outcome that ISPs are required to achieve without specifying the type of technology they should use to comply. This aspect is usually left to the discretion of the ISP. Thus, in the 2014 decision that put an end to the *Telekabel* case[52], the Austrian Highest Court did not specify the technical means that the ISP should use in order to prevent access to an infringing website, with the caveat that the ISP might be liable if such measures resulted in restricting access to lawful content. In this respect, it is worth noting that the choice of blocking technology that may be used by an ISP in order to comply with an order may be dictated by its cost implications.[53]

31. Finally, whereas in most countries *ISPs* typically have a remedy available to them to challenge blocking orders addressed to them, few countries explicitly provide *third-party websites* with a remedy when they are victim of collateral blocking. In Spain, a website owner was allowed to challenge the wrongful blocking of his site on the basis of tort liability.[54] In the UK, the English High Court agreed to an IP-blocking order drafted by the parties as third-party websites were allowed to object to IP-blocking when they shared an IP-address with a targeted website. [55]

32. In other countries, statute or case-law makes express reference more broadly to the right of *Internet users* to challenge wrongful website blocking: the United Kingdom[56], Austria[57] and France.[58] In Austria, the Supreme Court has established that although affected users cannot challenge a blocking order, they can sue both the ISPs under contract law and/or the rightsholder under tort law if the blocking is overly broad. Although most countries do not appear to require that minimum information be provided about remedies for wrongful blocking, France[59] and the United Kingdom[60] explicitly require as a matter of law that users of the blocked website are redirected to a page where they will be informed of their right to challenge the decision. Although both Austrian and French law only make reference to Internet "users", it seems reasonable to assume that this right extends to third-party websites affected by a blocking order. In this sense, the laws of some countries (Belgium[61] and Spain[62]) make reference to the rights of "affected" or "interested" parties to challenge a blocking order.

III. THE PROPER APPROACH TO WEBSITE BLOCKING

Any requirement to block unlawful content must be provided by law

33. At the outset, 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 unlawful). For this reason, we consider that blocking an entire website is almost certain to amount to a disproportionate interference with the right to freedom of expression given the risks involved and the extent of the adverse impact. As such, it should never be required by law. As the present case shows, moreover, the risks of overblocking are very real and the adverse effects on freedom of expression dramatic.

34. However, to the extent that governments seek to impose blocking measures, any such measure must comply with the requirements of Article 10 (2) ECHR and be provided by law. In particular, this means that the law should be drafted sufficiently precisely for individuals to be able to regulate their conduct.[63]

35. The Interveners further submit that blocking measures should only be permitted in respect of content, which is unlawful or can otherwise be legitimately restricted under international standards on freedom of expression.[64] 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.

36. Moreover, consistent with the international and comparative law standards set out in Part II, the Interveners submit that the law should provide for the following procedural safeguards:

    (i) Blocking should only be ordered by a court or other independent and impartial adjudicatory body. The Interveners note that regulatory models whereby government agencies issue blocking orders are problematic, as government agencies are – due to their executive nature – more likely to call for measures that protect the interests they are tasked to protect, such as national security or child safety, rather than freedom of expression;
    (ii) When a public authority or third party applies for a blocking order, ISPs or other relevant internet intermediaries should be given the opportunity to be heard in order to contest the application;
    (iii) Similarly, there should be procedures 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;

(iv) Users should be given a right to challenge, after the fact, the decision of a court or public body to block access to content.[65] *A fortiori*, this must include a right for victims of collateral blocking to challenge the wrongful blocking of their website or webpage;
(v) Whenever an order has been made to block content, anyone attempting to access it must be able to see that it has been blocked and a summary of the reasons why it was blocked, in order that they may have the opportunity to challenge the decision.[66] In particular, blocked pages should contain the following minimum information:
    a) the party requesting the block;
    b) the legal basis for the decision to block; the reasons for the decision in plain language;
    c) the case number, if any, together with a link to the relevant court order;
    d) the period during which the order is valid;
    e) contact details in case of an error;
    f) and information about avenues of appeal or other redress mechanisms.

37. Finally, in countries where blocking decisions are made by public authorities, the law should guarantee that these authorities are independent of government and that their decisions can be challenged before a court or tribunal.[67] Moreover, the law should lay down the criteria to be applied by these authorities before issuing any blocking order.

Blocking orders should be strictly proportionate to the aim pursued

38. As noted above, the Interveners consider that the wholesale blocking of a website should not be required by law. Even if it is so required, it should always be considered a disproportionate restriction on freedom of expression At the same time, the Interveners submit that any order to block access to content should be limited in scope and strictly proportionate to the legitimate aim pursued. It follows from the comparative material outlined in Part II above that in determining the scope of any blocking order, the courts should address themselves to the following:[68]

    (i) Any blocking order should be as narrowly targeted as possible;

    (ii) Whether 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;

    (iii) Whether access to other lawful material will be impeded and if so to what extent, bearing in mind that in principle, lawful content should never be blocked;

    (iv) 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;

    (v) 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;

39. The same criteria should be applied by administrative bodies tasked with issuing blocking orders. Moreover, as Judge Lemmens pointed out in the *Cengiz* case, even where the law does not provide explicitly for wholesale blocking or any of the safeguards outlined above, the Court should examine whether such orders pursue a legitimate aim and are necessary and proportionate.[69]

CONCLUSION

40. With the advent of the Internet, millions of users are now able to publish content online on a daily basis. Some of this content inevitably falls short of various countries' laws aimed at protecting the rights of others, national security, public order or public health and morals. In the last few years, States have increasingly resorted to website blocking as a silver bullet preventing access to unlawful and sometimes merely 'harmful' or 'undesirable' content.

41. The Interveners submit that website blocking is a very serious interference with the right to freedom of expression, akin to the banning of a newspaper or a television station. For this reason, it should only be permitted by this Court in the most exceptional circumstances and be subject to the strictest safeguards. As a matter of basic procedural fairness, this means that even if mandatory blocking measures are permissible in the first instance, they should have a basis in law, should be ordered by a court or other independent body and should be strictly necessary and proportionate to the aim pursued. The latter requirement necessarily entails that in considering whether to grant a website blocking order, the court or other independent body tasked with making the order should consider the impact of the order on lawful content and what technology may be used to prevent overblocking. Equally, basic procedural fairness demands that the victims of overbroad blocking orders should be given an opportunity to challenge such orders and therefore be notified of their existence.

42. This case presents the Court with an opportunity to expand on the basic procedural safeguards necessary to justify website blocking orders. Anything less than the above would seriously undermine freedom of expression online.

Gabrielle Guillemin
ARTICLE 19

Mitchell Stoltz
EFF

[1] A/HRC/17/27, 16 May 2011, para. 2: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[2] *Ibid.* para. 20
[3] *Ibid*. para. 23
[4] The 2011 Joint Declaration is available here: http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf
[5] CCPR/C/GC/34, para. 15 available at: http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf
[6] See Cengiz and Others v Turkey, no. os. 48226/10 and 14027/11, §§ 54-55, 1 December 2015.
[7] For more details, see Human Rights Watch, *Russia's Assault on Freedom of Expression,* July 2017 available at: https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression and ARTICLE 19, *Changes in the Sphere of Internet and Media Regulation 2015-2016,* https://www.article19.org/data/files/medialibrary/38337/Russia---LA-Internet-Regulation-English-Version.pdf *;* see also https://russiadigitalrights.org/en/category/timeline/
[8] See e.g. the 2016"Yarovaya Law". For an analysis of this law, see e.g. the comments sent by the UN Special Rapporteur on freedom of expression to the Russian Federation: http://www.ohchr.org/Documents/Issues/Opinion/Legislation/RUS_7_2016.pdf
[9] *Ibid*.

[10] See Freedom House, *Freedom on the Net*, Russia country report, 2016: https://freedomhouse.org/report/freedom-net/2016/russia
[11] See fn 6 above, see also, e.g. https://rsf.org/en/news/russian-parliament-certifies-free-internets-death and https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws
[12] See Council of Europe, *Study on filtering, blocking and takedown of illegal content on the Internet,* June 2016, Russia country report, available from here: https://rm.coe.int/16806554a4
[13] See fn 9 above.
[14] See 2011 Joint Declaration, *op.cit.*
[15] See A/HRC/17/27, *op. cit.* at para. 31
[16] See A/66/290. para. 82
[17] *Ibid*. para. 82, see also A/HRC/17/2, *op.cit.* at paras. 70 and 71.
[18] General Comment No. 34, *op.cit.*, para 43; also *Yildirim v Turkey*, *op.cit.*, para. 68
[19] Inter-American Commission on Human Rights, Freedom of Expression and the Internet, December 2013, paras. 84-90.
[20] See most recently, Council of Europe, Recommendation CM/Rec (2016)5 of the Committee of Ministers to Members States on Internet Freedom: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa
[21] European Court of Human Rights (ECtHR), *Yildirim v Turkey*, no. 3111/10, 18 December 2012
[22] CJEU, C-314/12, judgment of 27 March 2014, para. 55
[23] *Ibid*. para. 57.
[24] See Article 8 amending Directive 2002/22/EC in Regulation EU 2015/2120 laying down measures on open internet access: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R2120&from=EN
[25] no. 3111/10, §§ 31-37, ECHR 2012
[26] See Council of Europe, *Study on filtering, blocking and takedown of illegal content on the Internet,* June 2016: http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet
[27] *Ibid*. Executive Summary, available from here: https://rm.coe.int/168068511c
[28] *Ibid*, Comparative analysis, available from here: https://rm.coe.int/16806575b4
[29] See Article 8 and 12 of the French Law No. 2014-1353 of 13 November 2014, reinforcing the provisions in the fight against terrorism.
[30] See Article 2 of Decree No. 2015-125 implementing Law No. 2014-1353 cited above. The Conseil d'Etat has ruled that this blocking method (DNS) was proportionate as the risks of overblocking were limited: see France, *Conseil d'État* [State Council], judgement of 15 February 2016, No. 389140, ECLI:FR:CESSR:2016:389140.20160215, para. 15.The Decree further establishes the administrative authority tasked with the blocking of online terrorist content and child abuse images (*Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication*' (OCLCTIC). In practice, this is a special section of the police.
[31] Compare Article 16 of the Spanish Law 34/2002, concerning Information Society Services and Electronic Commerce.
[32] See Law 21/2014 of 4 November 2013 and Royal Decree 2011/1889/2011 on the enforcement of intellectual property rights: https://www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/marco-juridico/via-administrativa.html
[33] *Ibid*.
[34] Article 510.6 of the Spanish Penal Code.
[35] See Article 8.3 of Italian Regulation No. 680/13/CONS (2013), concerning the administrative body *Autorità per le Garanzie nelle Comunicazioni* ('AGCOM'), which grants AGCOM the power to block websites. See here for a translation of the text.
[36] See CoE Report *supra* note 28, at page 291 (Greece Country Report).
[37] See Article 1 (gg) of Italian Regulation No. 680/13/CONS (2013), cited above, which grants to the AGCOM the power to order the blocking of websites both through IP-address and through DNS-blocking. Since the beginning of 2017, AGCOM has only ordered the use of DNS blocking in all its resolutions. Article 4 of the Decree of 29 January 2007 on the prevention of child pornography contemplates both DNS and IP-address blocking.
[38] See *supra* note 32.
[39] These blocking powers derive from the general powers of courts to issue injunctions. In the EU, this is also as a result of Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society ('Info Soc' Directive) and Directive 2004/48/EC on the enforcement of intellectual property rights.
[40] See United Kingdom, High Court of Justice of England and Wales, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors*, [2014] EWHC 3354 (Ch), judgment of 17 October 2014. These criteria were confirmed by the Court of Appeal [2016] EWCA Civ 658, judgment of 6 July 2016.
[41] See Germany, *Bundesgerichthof* [Federal Court of Justice], I ZR 174/2014, judgment of 26 November 2015, para 89.
[42] See *mutatis mutandis* High Court of Justice of England and Wales, Chancery Division, *Twentieth Century Fox Film Corp & Ors v. British Telecommunications Plc* [2011] EWHC 1981 (Ch), judgment of 28 July 2011, para. 186.

[43] See Denmark, *Copenhagen Handelsretten* [Maritime and Commercial Court in Copenhagen], No. A-38-14, judgement of 11 December 2014.
[44] See Belgium, *Hof van Beroep Antwerpen* [Antwerp Court of Appeal], 2010/AR/2541, judgment of 26 November 2011.
[45] See United Kingdom, High Court of Justice of England and Wales, *Dramatico Entertainment Limited & Ors v British Sky Broadcasting Ltd & Ors* [2012] EWHC 1152 (Ch), judgment of 2 May 2012, para. 13.
[46] See High Court of Justice of England and Wales, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch), judgment of 17 October 2014, para. 256.
[47] See *supra* note 38.
[48] See Germany, *Bundesgerichthof* [Federal Court of Justice], I ZR 3/2014, judgment of 26 November 2015.
[49] See *supra* note 43, at para. 88.
[50] See Sweden, *Patent- och marknadsdomstolen* [Patent and Market Court of Appeal], PMT 11706-15, judgement of 13 February 2017.
[51] See United Kingdom, High Court of Justice of England and Wales, Chancery Division, *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors*, [2014] EWHC 3765 (Ch), judgment of 13 November 2014, paras. 8.
[52] See Austria, *Oberster Gerichtshof* [Highest Court], 4 Ob 71/14s, judgement of 26 June 2014. These proceedings gave rise to the well-known *UPC Telekabel Wien* decision of the Court of Justice of the European Union, Judgment of 27 March 2014, UPC Telekabel Wien, C-314/12, ECLI:EU:C:2014:192.
[53] See e.g. in France, Cour Cass, Civ 1, 6 July 2017, *SFR and others v Association of cinema producers and others*, No 16-17.217, 16-18.298, 16-18.348, 16-18.595, ECLI:FR:CCASS:2017:C100909. In the same sense, burden-sharing is the object of the ongoing appeal against the 2016 Court of Appeal decision in the *Cartier & Ors. v BskyB & Ors.* case (Court of Appeal of England and Wales, [2016] EWCA Civ 658). See http://ipkitten.blogspot.co.uk/2017/02/the-next-round-of-cartier-uk-supreme.html.
[54] See Spain, *Audiencia Provincial de Madrid* [Provincial Court of Madrid], Decision No. 3012/2012, judgement of 29 November 2012.
[55] See *supra* note 53.
[56] See *Cartier & Ors. v BskyB & Ors*., *supra* note 42, at paragraph 262-263.
[57] See *supra* note 54.
[58] See French Decree 2015-125, of 5 February 2015, on blocking websites promoting terrorism, and of websites circulating pornographic images and representations of children. Article 3.*supra* note 32.
[59] See French Decree 2015-125, of 5 February 2015, on blocking websites promoting terrorism, and of websites circulating pornographic images and representations of children. Article 3.
[60] See *Cartier & Ors. v BskyB & Ors*. *supra* note 42, at paragraph 264.
[61] See Belgium, Criminal Instruction Code. Article 28sexies(1).
[62] See Spain, Law 29/1998, concerning the Contentious-Administrative Jurisdiction. Article 122bis.
[63] See, among many other authorities, *RTBF v. Belgium*, no. 50084/06, § 103, ECHR 2011
[64] See A/66/290, *op.cit,* para. 81.
[65] See e.g. ECtHR, *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, ECHR 2015
[66] See Recommendation CM/Rec(2008)6, *op.cit*. Section I. and Recommendation on the protection of human rights with regard to search engines, o*p.cit.* para 16.
[67] *Ibid., Recommendation* CM/Rec(2008)6, Section III (ii) and *Yildirim v Turkey*, *op.cit*, para. 64
[68] *Yildirim v Turkey*, *op.cit*, para. 66.
[69] *Op cit*. Concurring opinion.