EUROPEAN INFORMATION SOCIETY INSTITUTE, O. Z.
Registration address: Štítová 1243/1 040 01 Košice, Slovakia
Postal address: Martin Husovec / EISi, TILT, P.O.Box 90153, 5000 LE Tilburg, The Netherlands
IČO: 42 227 950, www.eisionline.org, eisi@eisionline.org

10 July 2017

The Registrar
European Court of Human Rights
Council of Europe
F-67075 Strasbourg Cedex
France

Third Party Intervention Submission by
European Information Society Insitute (EISi)

In re *Kharitonov v Russia*, App. No. 10795/14

INTRODUCTION

- This third-party intervention is submitted on behalf of the European Information Society Institute (EISi), an independent non-profit organization based in Slovakia which focuses on the overlap between technology and law. EISi promotes human rights in a digital society by conducting impact litigation before the courts. It also serves as a research center for high technology law.
- EISi welcomes the opportunity to intervene as a third party in this case granted by the leave of the President of the Court on 21 June 2017 (ECHR-LE14.8bP3 NI/tsh) pursuant to Rule 44 (3) of the Rule of Court. This submission does not take a position on the merits of the applicant's case.
- In our submission, we address: (i) importance of the decision and task of the Court, (ii) the reasons why the states should be held accountable for collateral over-blocking of the websites by private parties, (iii) importance of specific legal basis as to the target and means of blocking, (iv) the need to observe the principle of proportionality in grant and implementation of website blocking and (v) available remedies against the abuse of website blocking.

TASK BEFORE THE COURT

(1) This case provides the Court with an opportunity to define the limits of permitted state interference in the online environment. Unhampered and reliable Internet access to information not only facilitates freedom of expression, but also promotes other values guaranteed by the European Convention on Human Rights (the "Convention")[1], such as by providing access to education and empowering minorities.[2]

(2) While this case will be of importance for all member states of the Council of Europe, it will also be crucial for Russia. The current Russian implementation of website blocking leads to collateral website blocking on a massive scale and lacks any adequate safeguards against the abuse. In accordance with the data provided by Roskomsvoboda, a Russian community project supporting freedom of information online, as of 28 June 2017, 6,522,629 Internet resources have been blocked in Russia. Of this number, 6,335,850 Internet resources were blocked collaterally, meaning that *97% of all blocked Internet content in Russia is blocked without an adequate legal justification*.[3] This is an unprecedented scale. At different times due to collateral blocking Russian users were not able to access widely-used Internet services such as: Google,[4] Vkontakte,[5] Wikipedia,[6] Wayback Machine (http://web.archive.org/),[7] GitHub,[8] Reddit,[9]

[1] Convention for the Protection of Human Rights and Fundamental Freedoms, 1953. Also known as the European Convention on Human Rights

[2] See generally: Human Rights Council, Thirty-second session, Agenda item 3, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A/HRC/32/L.20, dated 27 June 2016 <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf> accessed 04 July 2017

[3] Roskomsvoboda, Blocking distribution by governmental agencies <https://reestr.rublacklist.net/visual> accessed 04 July 2017

[4] 'Russia Blocks Google Temporarily in Tax Dispute', The Moscow Times (Moscow, 22 June 2017) <https://themoscowtimes.com/news/google-blocked-for-3-hours-in-russian-tax-dispute-58250> accessed 04 July 2017

[5] Sergei Karpukhin, 'Russia's leading social network banned by "mistake"', Reuters (Moscow, 24 May 2013) <http://www.reuters.com/article/net-us-russia-vkontakte-idUSBRE94N0BD20130524> accessed 04 July 2017

[6] Shaun Walker, 'Russia briefly bans Wikipedia over page relating to drug use', The Guardian (Moscow, 25 August 2015) <https://www.theguardian.com/world/2015/aug/25/russia-bans-wikipedia-drug-charas-https> accessed 04 July 2017

[7] Roskomnadzor, 'Blocking of extremist video of the terroristic organization "ISIS" on the Internet' (24 October 2014) <https://rkn.gov.ru/news/rsoc/news27794.htm> accessed 04 July 2017; 'Roskomnadzor blocked Wayback Machine', CNews (24 October 2014) <http://www.cnews.ru/news/top/roskomnadzor_zablokiroval_mashinu_vremeni> accessed 04 July 2017

[8] Ingrid Lunden, 'Russia Blacklists, Blocks GitHub Over Pages That Refer To Suicide', Tech Crunch (03 December 2014 <https://techcrunch.com/2014/12/03/github-russia/> accessed 04 July 2017

[9] Andrew Griffin, 'Reddit Banned in Russia Because of One Thread', Independent (13 August 2015) <http://www.independent.co.uk/life-style/gadgets-and-tech/news/reddit-banned-in-russia-because-of-one-thread-10453063.html> accessed 04 July 2017

Disney, Discovery and Nickelodeon blogs,[10] VPN services,[11] websites hosted on Amazon Web Services,[12] and websites that use CDN services provided by CloudFlare.[13]

(3) In addition to the lack of safeguards, the website blocking system in Russia has vulnerabilities that facilitates over-blocking. Any owner of a blocked website can *unilaterally* change the IP address of the website to any other IP address (for example, the IP address associated with youtube.com). In such case Internet access providers that use IP blocking will be required, under the threat of a penalty, to block the IP address associated with youtube.com making it immediately unavailable for Russian users. This vulnerability in the Russian website blocking system has been known since 2012, including by Roskomandzor, the authority.[14] The magnitude of its wide exploitation for abuse is only rising.[15] Since its start, internet access was blocked to a number of popular websites, including Wikipedia and news websites.[16] It cannot be ruled out that this vulnerability is also responsible for a recent disruption in the banking system.[17]

(4) Over-blocking in Russia is thus very widespread. The case at hand is only one of the hundreds of thousands of websites that are being continuously collaterally blocked. This magnitude of collateral censorship merits strong intervention of the Court. In particular, many aspects of the state interference in this case are typical for modern interferences with internet architecture. They provide the Court with an excellent opportunity to improve conditions for the citizen's exercise of human rights online.

ACCOUNTABILITY OF THE STATE

(5) In circumstances of this case the state is heavily involved in the implementation of website blocking. The over-blocking is a foreseeable consequence of the government's actions, which means that the state should be held accountable for all its negative consequences and abuse, including by third parties.

(6) The Russian Federation does the following: (i) it passes legislation regulating website blocking, (ii) decides access to which online locations to be blocked, (iii) operates a centralised register of online locations to be subjected to blocking, (iv) coordinates efforts of Internet

---

[10] Nikolai Chumakov, 'Disney and Discovery blogs in Tumblr were partially inaccessible in the Russian Federation due to imperfection of blocking procedure', TJ (27 April 2017) <https://tjournal.ru/43720-blogi-disney-i-discovery-v-tumblr-okazalis-chastichno-nedostupni-v-rf-iz-za-nesovershenstva-blokirovok> accessed 04 July 2017

[11] 'Roskomnadzor blocked VPN-service Hideme.ru', RBC (12 January 2016) <http://www.rbc.ru/rbcfreenews/587784999a7947550ffb6bf7> accessed 04 July 2017

[12] 'Roskomnadzor blocked Amazon Cloud Service', RBC (22 June 2016) <http://www.rbc.ru/rbcfreenews/576aa5a29a79475930f4e977> accessed 04 July 2017; 'Russian Authorities Block, Then Unblock, Amazon's Cloud Service', combined reports by East-West Digital News, Meduza (24 June 2016) <http://www.ewdn.com/2016/06/24/russian-authorities-block-then-unblock-amazons-cloud-service/> accessed 04 July 2017

[13] Andy, '2,800 Cloudflare IP Addresses Blocked By Court Order', TorrentFreak (14 October 2015) <https://torrentfreak.com/2800-cloudflare-ip-addresses-blocked-by-court-order-151014/> accessed 04 July 2017

[14] The Federal Service for Supervision of Communications, Information Technology, and Mass Media, the governmental agency responsible for overseeing website blocking in Russia.

[15] Nikita Likhachev, 'Crisis of the Register of the forbidden websites, or why some people may not access TJ', TJournal (08 June 2017) <https://tjournal.ru/45147-krizis-reestra-zapreshyonnih-saitov-ili-pochemu-ne-u-vseh-otkrivaetsya-tj> accessed 04 July 2017

[16] Evgeny Berg, 'Activists used the security vulnerability of Roskomnadzor's activity and now they block websites. How does it work?', Meduza (Riga, 08 June 2017) <https://meduza.io/feature/2017/06/08/aktivisty-vospolzovalis-uyazvimostyu-v-rabote-roskomnadzora-i-teper-blokiruyut-chuzhie-sayty-kak-eto-ustroeno> accessed 04 July 2017

[17] Andrey Frolov, 'Is «Sberbank's» crash connected to the security vulnerability of Roskomnadzor's blocking system', VC.RU (09 June 2017) <https://vc.ru/p/sber-crash-rkn> accessed 04 July 2017

access providers in implementing website blocking, (v) monitors compliance with website blocking obligations and (vi) fines Internet access providers that fail to comply. In such circumstances the state should also be accountable for the actions of private parties, such as Internet access providers, taken to implement the framework laid down by the state.

(7) After a state authority supplies an IP address of the target online location, it asks Internet access providers to comply with website blocking regulations by blocking the IP address. The collateral blocking is then a predictable result given that one IP address is often shared by multiple, often hundreds of websites.[18]

(8) It is thus reasonably foreseeable and, by this point also widely established, that profit-maximizing Internet access providers use *technological implementation* of the blocking that magnifies collateral blocking. The IP address blocking technique is one of the least expensive ways of restricting access to information.[19] Internet access providers frequently choose it over other possible ways. In fact, Internet access providers may not even have the necessary equipment to employ a more granular method of website blocking. For example, Roskomnadzor, the authority,[20] has recently reported that 50-55% of all Russian Internet access providers do not have equipment that allows to analyse Internet traffic and have to rely on IP address blocking.[21] Providers that have no choice, but to engage in over-blocking since a failure to comply with the website blocking regulations will lead to fines and also possible suspension of the license required to provide their services. Moreover, in Russia, the courts do not consider unavailability of equipment that allows granular website blocking as a valid excuse for failure to block access only to targeted websites.[22] To illustrate the real conditions consider that even Rostelecom, the largest Russian Internet access provider (38% market share of broadband market), in which the state is a majority shareholder, acknowledged that it is unable to use more granular website blocking techniques.[23]

(9) In circumstances when private individuals, such as Internet access providers, who are tasked with the implementation of the government blocking, are primarily motivated by economic considerations, which then results in significant collateral censorship, the state should be required to affirmatively protect online freedom of expression and, for these purposes, be held accountable also for all the foreseeable market-intermediated failures

---

[18] Lukas Feiler, 'Website Blocking Injunctions under EU and U.S. Copyright Law—Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law?' (TTLF Working Papers No. 13, 2012) <https://law.stanford.edu/wp-content/uploads/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf> accessed 04 July 2017: "A single IP address is often used to host multiple websites, and indeed often hundreds of them". A report published by UK Ofcom in 2012 found out that "[f]or the COM, NET and ORG top-level domains, 97% of websites reside on IP addresses shared with other websites, compared to 87% in 2002" (see CSMG Final Report for Ofcom, 'Study into Websites Sharing Internet Protocol Addresses' (26 April 2012) <https://www.ofcom.org.uk/__data/assets/pdf_file/0022/15817/websites-sharing.pdf> accessed 04 July 2017)

[19] The costs of IP blocking are equally low as with DNS blocking (see Ibid. <https://law.stanford.edu/wp-content/uploads/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf>); A report published by Ofcom in 2010 defined IP address blocking as "low cost"

[20] The Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications

[21] Roskomnadzor, 'Statement of Roskomnadzor's Head, Alexander Zharov' (15 June 2017) <https://rkn.gov.ru/news/rsoc/news46550.htm> accessed 04 July 2017

[22] For example, see: The decision of the Oktyabrsky District Court of Samara № 2-3527/13 of 29 May 2013 <http://sudact.ru/regular/doc/luIj9LaYWTHO/>, the decision Frunzensky District Court of Saratov № 2-2411/2015 2-2411/2015~M-2311/2015 M-2311/2015 of 18 August 2015 in the case № 2-2411/2015. <http://sudact.ru/regular/doc/BjUwOmNyfjr1/> accessed 10 July 2017

[23] Rostelecom, 'Regarding the matter of website blocking by the Internet access provider' (27 June 2013) <http://www.rostelecom.ru/press/news/d304702> accessed 04 July 2017

resulting from its framework, which acted as a trigger.[24] As was recently suggested by a study commissioned by the Council of Europe, the states that continuously encourage voluntary blocking without any legal basis may be eventually responsible for "infringements of freedom of expression by private companies".[25]

IMPORTANCE OF PROTECTION OF FREEDOM OF EXPRESSION ONLINE

(10) Freedom of expression, as laid down in Article 10 of the Convention, is essential to any democracy and is directly linked to the ability of citizens to live and participate in modern society. As a medium designed to enhance public access to news and facilitating the dissemination of information in general,[26] the Internet depends on this very fundamental right.[27] The right thus must be duly respected, guaranteed and protected by the state and relevant public institutions. However, in an era of decentralization of communications where new opportunities to impart and receive ideas arise, the risks are compounded by the frustratingly persistent issue of extraterritoriality. Moreover, technical measures restricting access to online content have become prevalent through authoritarian and democratic countries alike[28] in an attempt to regain control for reasons such as copyright infringement, "extremist" web-pages or otherwise harmful content. Whilst national authorities have a margin of appreciation, it is not unlimited[29] and is particularly narrow with regards to comments of the general interest or political issues.[30]

(11) Regular websites are a primary way how citizens experience the internet. Livehoods of individuals, groups and societies are relying on stability of the infrastructure that underpins them. The websites thus form an integral part of how citizens exercise their rights, including freedom of expression. Interfering with this infrastructure thus has very serious impact.

(12) Recognizing that freedom of expression is not an absolute right, Article 10(2) of the Convention provides the three-part test which sets out conditions for any such restriction to be lawful. Any interference must be: (1) prescribed for by law; (2) pursue a legitimate aim; (3) and must be necessary in a democratic society.

PRESCRIBED BY THE LAW

(13) When a website owner finds access to his website blocked merely because of sharing an IP address with another unaffiliated website owner that is actively involved in disseminating unlawful content, such restriction cannot be said to be prescribed by law. No legal basis is present in such circumstances and the applicant is not afforded the opportunity to regulate his conduct.[31] Such collateral censorship where the only connection can be incidentally found at the infrastructure level is similar to the blocking of an entire website in a situation when blocking of only few of its sub-pages would be justifiable, as was the case in Yildirim v Turkey.[32]

---

[24] Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated Internet platforms and Internet access providers (Adopted by the Committee of Ministers on 7 December 2011 at the 1129th meeting of the Ministers' Deputies)
[25] Swiss Institute of Comparative Law, Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content Excerpt, pp. 773-800 (Part 2 Comparative Considerations) Avis 14-067 (Lausanne, 20 December 2015) <https://rm.coe.int/16806575b4> accessed 04 July 2017
[26] Times Newspapers Ltd v the United Kingdom (1979) App nos. 3002/03 and 23676/03, para 27
[27] Delfi AS v Estonia (2015) App no. 64569/09., para 131
[28] Reporters Without Borders, 'Enemies of the Internet', <http://12mars.rsf.org/2014-en/#slide2> accessed 6 July 2017
[29] Aleksey Ovchinnikov v Russia (2010) App no. 24061/04para 51
[30] Axel Springer AG v Germany (2012) App no. 39954/08, para 90
[31] The Sunday Times v the United Kingdom (1979) App no. 6538/74, para 49
[32] Ahmet Yildirim v Turkey (2012) App no. 3111/10

(14) Unless the law and implementing legal orders aren't specific enough about *the target and means* used to achieve blocking, so that any collateral blocking is only an incidental occurrence, the interference cannot be said to be based on a proper legal basis.

(15) An interference involving the blocking of access must be justified by a "pressing social need" relating to and pursuing one or more of the legitimate aims.[33] For example, in Russia the interference is aimed at preventing the dissemination of harmful information. While a state executive body may pursue a legitimate aim when issuing a blocking order to restrict access to a target website that makes illegal content available, the same cannot be said for lawful content hosted on untargeted websites.

NECESSITY IN A DEMOCRATIC SOCIETY

(16) As stated in the previous section, restriction of freedom of expression is possible under the three-part test set out in Article 10(2) of the Convention, the last requirement resting on the *necessity* of the restriction in a democratic society. Although "necessity" lacks a clear definition, falling somewhere between "indispensable" and "reasonable",[34] it means that must not merely be expedient. "Necessity" implies the principle of proportionality, which lies at the heart of the Court's investigation into the reasonableness of the restriction and serves to ensure that the rights laid down in the Convention are not interfered with unnecessarily.[35] The difficulty in addressing proportionality resides in its multilayer nature, which has to be considered in the effort to provide fair and reasonable judicial outcomes. The importance of its gauging has been debated numerous times, perceived as "a very important guiding principle when assessing restrictions on fundamental rights".[36]

(17) Under the principle of proportionality, the Court examines, in particular, if a fair balance has been struck between the various interests at stake and whether a particular result could be achieved with less restrictive means, taking also into account the nature and severity of the sanctions imposed.[37] Generally, the Court has held that when national authorities restrict fundamental rights, they are required "to choose the means that cause the least possible prejudice to the rights in question".[38]

(18) Website blocking measures must comply with the principle of proportionality, in a way that facilitates the aforementioned balancing. This, partially, means that the measures imposed should be as narrow as the goal requires. The cost of their implementation should be also considered.[39] Regarding, in particular, the proportionality of internet access blocking measures, the Court has stated in Yildirim v Turkey[40] that the blocking of access to an IP address just because it hosts a website that contains illegal content, while knowingly and simultaneously blocking access to legitimate content, does not constitute a necessary measure; especially, since it is *technically possible to achieve the same result*, namely blocking access to the offending website, by more targeted measures. Judge Pinto De Albuquerque in his concurring opinion on

---

[33] Observer and Guardian v the United Kingdom (1979) App no. 6538/74, para 71

[34] The Sunday Times v the United Kingdom, para 59

[35] Council of Europe, "The margin of appreciation", <https://www.coe.int/t/dghl/cooperation/lisbonnetwork/themis/echr/paper2_en.asp#P140_13356> accessed 2 July 2017

[36] Lievens, E., Demeyer, K., & Dumortier, J. (2012). Removing and blocking illegal online content: about controversy, censorship and proportionality. In ECREA 2012 Pre-Conference: Imposing Freedoms: The role of copyright, privacy and censorship governance in the re/definition of rights in digital media, p. 5

[37] Morice v France [GC], para 127; Cumpănă and Mazăre v Romania [GC], no. 33348/96, para 111, ECHR 2004-XI

[38] Mouvement raëlien Suisse v Switzerland, [GC], para 75

[39] Savola, P. (2014). Proportionality of website blocking: Internet access providers as copyright enforcers, p. 122; Martin Husovec, 'Injunctions against Innocent Third Parties: The case of Website Blocking' 4 JIPITEC, 2, para 116 et seq.

[40] Ahmet Yildirim v Turkey (2012) App no. 3111/10

the same case noted that, among the minimum criteria for Convention- compatible legislation on internet blocking measures is the observance of the criterion of proportionality, which provides for a fair balancing of the freedom of expression and other competing interests, and ensures that freedom of expression is respected.[41]

(19) The Court of Justice of the European Union (CJEU) arrived at a similar conclusion in its UPC Telekabel v Constantin decision,[42] stating that the measures taken by Internet access providers must not affect internet users who are using the services to lawfully access information. Failure to observe this principle would constitute an interference with the users' freedom of information, not justified by the objective pursued. Moreover, in Cartier and others v British Sky Broadcasting Limited and others, the UK High Court of Justice noted that "it ought to be possible to target the blocking so that lawful users are not adversely affected by it".[43]

(20) The principle of proportionality can be observed by balancing competing rights when implementing website blocking, that is the interests served by the website blocking (for example, protection of health and safety) and rights facilitated by retaining access to the information, including collaterally blocked websites. Instead of broadly preventing any type of blocking, this balancing exercise should be conducted in each case taking into account its particular circumstances. This approach was used at different times by CJEU when the CJEU had to reconcile competing human rights. For example, in Digital Rights Ireland Ltd the CJEU decided that data retention cannot be justified by simply pointing to the need of prevention of serious crime referred to "in a general manner".[44] On the contrary, in order to be justified data retention "must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences".[45]

(21) Applying this approach to website blocking, national legislation should contain precise guidance allowing balancing of competing rights when implementing website blocking. Courts or other competent authorities should use this guidance to assess positive and negative effects of issuing a website blocking order in each particular case. This balancing exercise should take into account, among other factors, harmfulness of illegal information, practical effectiveness of the measures and side effects of website blocking, including subsequent abuse by third parties.

(22) First and foremost, it should be recognized that primary enforcement strategy should be directed at the root cause of the intervention, i.e. persons who publish illegal information. As was explained above, website blocking is an extreme measure which significantly interferes with freedom of expression. Restriction of citizen's access to illegal information can be also achieved by less intrusive means. For example, website blocking will not be necessary if the person responsible for publishing the illegal information removes it from the website. Illegal information can also be removed by the website owner. Both of these results can be achieved by an enforcement action against the person who published illegal information or the website that disseminates illegal information. This reasoning was recently used by the German Federal Court of Justice in cases where a right holder requested an Internet access provider to block access to the website which was used to infringe right holder's copyright. The German Court decided that website blocking is the *ultima ratio* measure and before website blocking can be

[41] Ibid.
[42] C 314/12, UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and others, 27 March 2014, para 56
[43] Cartier and others v British Sky Broadcasting Limited and others, England and Wales High Court of Justice, 17 October 2014, para 257
[44] Joined Cases C-293/12 and C-594/12 dated 08 April 2014 Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, the Attorney General, para 62 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=121733> accessed 10 July 2017
[45] Ibid. para 63

implemented right holders should attempt to take an action against the website owner. Only if the enforcement fails or lacks any prospects of success website blocking can be implemented.[46]

(23) Second, the case-law of many Member States recognizes that proportionality of website blocking can be assessed if the law and implementing legal orders are specific as to target and means.[47] Otherwise, at the point of the grant of such a blocking, the court or an authority would skip the assessment of whether there is at least one permissible implementation of the order. This was recently pointed out by Advocate General of the CJEU Szpunar who argued: "The possibility of choosing which measures are most appropriate can, in certain situations, be compatible with the interests of the addressee of an injunction, but it is not so where that choice is the source of legal uncertainty. In such circumstances, leaving it entirely to the addressee to choose the most appropriate measures would upset the balance between the rights and interests involved."[48]

(24) The choice of the method of implementation of website blocking is crucial to the balancing exercise. Different methods of website blocking can have different effectiveness, consequences in terms of costs and side effects.

(25) In case of the DNS blocking, the Internet access provider merely black-lists certain domain names from its DNS records. This technique can be easily circumvented by both users and targeted website operators. Users need only to use a different provider as a source of DNS records, which is a trivial setting in the Internet browser, or by simply using search engines instead of direct URL entry. The second method is IP address blocking, where an Internet access provider black-lists certain IP addresses used by the server where the targeted website is stored. This technique is relatively more difficult for users to circumvent. They would need to use a special proxy service or VPN to go around this block. The website operator can change his IP address. The last technique is called Deep Packet Inspection (DPI), which, unlike the previous two techniques, enables blocking certain URLs in addition to entire webpages. This method should be in particular used when the targeted service shares an IP address with other services, or if the specific part of the website is to be blocked. The most significant disadvantage to Deep Packet Inspection is that it may be easily subverted if the packets are encrypted, e.g. using the 'https' protocol and that it entails monitoring of user's access to internet.[49]

(26) Generally, more sophisticated blocking systems implemented by Internet access providers, allow to block a website hosted on a shared IP address without blocking other websites hosted on the same IP address, avoiding over-blocking.[50] As can be seen, IP address blocking is particularly prone to collateral blocking, since it blocks access to all website hosted on a single IP address. When the state allows Internet access providers to choose the method of implementation of website blocking, the state should consider what option the Internet access providers are more likely to choose (for example, whether Internet access providers have access to the equipment which allows to implement granular website blocking without collateral blocking). If it is predictable that Internet access providers will use less sophisticated methods, such as IP address blocking, this should be a factor against implementing website blocking in a particular case; but it can also mean that the state bears higher burden to first create conditions which will result in human rights complaint website blocking on the market.

---

[46] Martin Husovec and Lisa Van Dongen, 'Website Blocking, Injunctions and Beyond: View on the Harmonization from the Netherlands' (2017) GRUR Int. issue 7/2017; JIPLP 2017 Issue 9; TILEC Discussion Paper No. 2017-024. Available at SSRN: https://ssrn.com/abstract=2967318

[47] *Ibid*, see Part 4

[48] Opinion in Tobias Mc Fadden v Sony Music, C-484/14, ECLI:EU:C:2016:170, para 123

[49] Martin Husovec, 'Injunctions against Innocent Third Parties: The case of Website Blocking' 4 JIPITEC, 2, para 116

[50] Cartier and others v British Sky Broadcasting Limited and others, England and Wales High Court of Justice, 17 October 2014, para 39 and 42

(27) To summarise, we ask the Court to recognise that in order to comply with the "necessity in a democratic society" test when implementing website blocking the state must adopt legislation allowing balancing of competing rights when implementing website blocking. This is only possible if blocking is clearly defined in terms of target and means. The balancing exercise should be conducted in each case in order to properly access positive and negative effects website blocking in a particular set of circumstances. The absence of an obligation to conduct this balancing exercise can lead to severe collateral blocking and interference in freedom of expression.

REMEDIES

(28) Even when website blocking is proportionate in its design following the balancing exercise described in the previous section, freedom of expression in website blocking cases should also be facilitated by implementing certain ex ante and ex post remedies to over-blocking. They prevent abuse.

(29) Ex ante remedy accounts for the measures provided by the state prior to, or simultaneously with an action of blocking, which is expected to cause negative effects. When website blocking is implemented ex ante remedies may include: (i) prior notification of the owners of collaterally blocked websites and (ii) availability of appeal against website blocking before it is implemented.

(30) *Prior notification of the owners of collaterally blocked websites.* When website blocking is implemented it is usually possible to identify websites which are likely to be subjected to collateral blocking. For example, when collateral blocking is caused by restricting access to an IP address which is used to host several websites, such websites can be first identified by performing reverse IP address lookup.[51] If the state provides a notification to the owners of such websites before implementing website blocking, the owners may be able to deploy additional domain names or implement other techniques to ensure access to their websites,[52] warn their users about impending website blocking, attempt to persuade the owner of the target website to remove illegal information preventing website blocking (if affiliated) or use other self-help measures. Interestingly, in Russia, Roskomnadzor has to provide a prior notification to the target website,[53] but not to the owners of the websites that are likely to be subjected to collateral blocking. This puts the owners of collaterally blocked website in a worse position than that of the target website that contain illegal information. It is also important to note that sending prior notifications does not entail spending significant resources and is unlikely to impose any disproportionate burden on the state. Such pre-notification should not be seen, however, as the only solution, as it shifts the burden to operators of legitimate websites.

(31) *Availability of appeal against website blocking before it is implemented*. Creating a possibility to challenge website blocking before it is implemented may ensure that the balancing exercise described in the previous section is implemented correctly. It also contributes to a right to fair trial since the website owner is affected only after it had (i) access to the court because it was notified of the measures and (ii) equality of arms has been assured before the decision is taken.[54]

---

[51] For example, there are publicly available reverse IP lookup services are available such as http://reverseip.domaintools.com/

[52] For the technical aspects of the issue, see: Dornseif, M. (2004). Government mandated blocking of foreign web content. arXiv preprint cs/0404005(2004). pp. 14-17

[53] Article 15.1(7) of the Federal Law of the Russian Federation "On Information, Information Technologies and the Protection of Information" dated 27.07.2006 N 149-FZ

[54] See more: Martin Husovec and Miquel Peguera, 'Much Ado about Little – Privately Litigated Internet Disconnection Injunctions' (IIC 2015, 10)

(32) Ex post remedies may facilitate exercise of freedom of expression after website blocking is implemented and may include (i) availability of appeal against website blocking after it is implemented, (ii) limiting duration of website blocking orders and (iii) post-grant supervision.

(33) *Availability of appeal against website blocking after it is implemented*. Although less effective than appealing website blocking before it is implemented, appeal after access to the website that was collaterally blocked can still be an essential means of redress for website owners. This right can be facilitated when users trying to access a blocked website are informed about why the website is unavailable and how the website blocking can be appealed. Such appeal or challenge can be available both to users and website operators.[55] This practice is implemented by the courts in the UK.[56]

(34) *Limiting duration of website blocking orders*. Arnold J in Cartier and others v British Sky Broadcasting Limited[57] expressed his concerns about the number of websites that can be subjected to blocking and in order provide for this concern limited duration of the blocking orders. For example, in Russia, unlimited duration of website blocking orders led to a practical problem. After blocking is implemented owners of blocked websites often do not pay for the domain name and as the time goes on, the domain name becomes vacant. After that any person can purchase the domain name of a blocked website and by changing the IP address associated with this website cause blocking of all websites hosted on this IP address.[58]

(35) *Post-grant supervision.* In order to uncover and document instances of over-blocking caused by website blocking, the state should monitor such instances and act upon them. It is the state's responsibility to prevent abuse by third parties.

(36) The remedies suggested above are only examples of safeguards, which can be implemented to prevent abuse of website blocking and mitigate its negative impact on freedom of expression and other human rights. Many of these measures are easy to implement and their implementation should in our view supplement use of proportionate website blocking.

CONCLUSIONS

The European Information Society Institute (EISi) suggests that the Court:

- **recognises that the states can be held accountable for collateral over-blocking in circumstances where it is a foreseeable consequence of its actions and**

- **strengthens online freedom of expression by requiring that the state which mandates and delegates website blocking to private actors by default mitigates any risks of collateral censorship by taking proactive steps, such as case-by-case assessment of proportionality, guiding the choice of technological implementation and employing effective ex-ante and ex-post remedies.**

---

[55] See generally: Martin Husovec and Lisa Van Dongen, 'Website Blocking, Injunctions and Beyond: View on the Harmonization from the Netherlands' (2017)

[56] See, for example, http://www.ukispcourtorders.co.uk/ and para 264 of Cartier International AG and others v British Sky Broadcasting Ltd and others, [2014] EWHC 3354 (Ch), [2015] BUS LR 298

[57] Cartier and others v British Sky Broadcasting Limited and others, England and Wales High Court of Justice, 17 October 2014, para 265

[58] Evgeny Berg, 'Activists used the security vulnerability of Roskomnadzor's activity and now they block websites. How does it work?', Meduza (Riga, 08 June 2017) <https://meduza.io/feature/2017/06/08/aktivisty-vospolzovalis-uyazvimostyu-v-rabote-roskomnadzora-i-teper-blokiruyut-chuzhie-sayty-kak-eto-ustroeno> accessed 04 July 2017