CENTRE FOR LAW AND DEMOCRACY

Russia

Comments on Internet Content Restrictions

July 2013

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Introduction

In recent years, freedom of expression in Russia has come under severe threat. Independent broadcasters and journalists have come under attack, both figuratively and literally, and a raft of legislation has been adopted cracking down on the ability of opposition voices to make themselves heard. Although the Internet is famously resistant to censorship or control, there are troubling indications that Russia's government is seeking to limit one of the few spaces for debate that remains relatively free.

In July 2012, the Russian parliament passed "On amendments to the Federal Statute 'On the Protection of Minors against Information Detrimental to their Health and Development' and to other legal Acts of the Russian Federation" (the Amendments). The stated aim of the Amendments is to protect children from information harmful to their health and development, and it empowers Russia's federal executive to establish a database of domain names and network addresses of websites that contain information which is banned within the Russian Federation and to take steps to shut down or block these websites. However, the "blacklist" targets a broad and vaguely defined range of websites, including any which contain information about "non-traditional" sexual lifestyles. The list is also developed in a manner which is troubling for its lack of transparency and procedural protections, giving the government a wide ambit to abuse its new powers. The potential for abuse is even more serious given the fact that the agency tasked with implementing the new law, the Federal Service for Supervision in Telecommunications, Information Technology and Mass Communications (Roskomnadzor), lacks the independence which is required of a body that regulates speech.

There have also been disturbing signs that the government intends to enforce the law using the technique of deep-packet inspection (DPI), an extremely invasive method. Although it is difficult to confirm whether and to what extent this technique is indeed being used, the introduction of DPI would represent a significant threat to online privacy in Russia and freedom of expression on the Internet.

Shutting down or blocking websites are extreme measures, analogous to seizing and destroying copies of a printed publication. Vagueness, a lack of transparency and the absence of procedural protections are always problematic when dealing with laws which impact on freedom of expression. Viewed in the context of Russia's eroding human rights situation, and taking into account the extreme nature of the measures they authorise, the Amendments are a cause for very serious concern. This Analysis examines the Amendments in the context of international freedom of expression

standards, and offers substantive recommendations for how they should be amended to ensure respect for those standards.

1. Freedom of Expression

Freedom of expression is among the most fundamental and important human rights. It is guarantees in Article 19 of the *Universal Declaration of Human Rights* (UDHR),[1] as follows:

> Everyone has the right to freedom of opinion and expression; this right includes the right to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers.

Article 19 of the UDHR is broadly recognised as having crystallised into customary international law and it is thus applicable to all States. However, freedom of expression is also guaranteed in Article 19 of the *International Covenant on Civil and Political Rights* (ICCPR)[2], which Russia ratified in October 1973:

> 1. Everyone shall have the right to hold opinions without interference.
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Article 10 of the *European Convention on Human Rights* (ECHR),[3] which Russia ratified in May 1998, contains similar protections, although the list of legitimate aims is slightly longer, also including territorial integrity, information received in confidence, and the authority and impartiality of the judiciary.

According to both the ICCPR and the ECHR, freedom of expression can be limited in certain contexts, but only in accordance with the 'the three-part test' for assessing the legitimacy of any proposed restriction. According to this test, a restriction on freedom of expression is only legitimate if it:

---

[1] UN General Assembly Resolution 217A(III) of 10 December 1948.
[2] UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976.
[3] Adopted 4 November 1950, E.T.S. No. 5, entered into force 3 September 1953.

1. Is provided by law or imposed in conformity with the law.
2. Pursues one of the legitimate aims listed in Article 19 (3).
3. Is necessary to secure that aim.

In its most recent General Comment on Article 19 of the ICCPR, adopted in September 2011, the UN Human Rights Committee stated:

> Paragraph 3 lays down specific conditions and it is only subject to these conditions that restrictions may be imposed: the restrictions must be "provided by law"; they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3; and they must conform to the strict tests of necessity and proportionality. [references omitted][4]

The first part of the test not only requires restrictions to be based on a legal provision, but also to meet certain standards of clarity and accessibility. This is because uncertainty as to the scope of a restriction is likely to create a chilling effect on freedom of expression, whereby individuals avoid making any statement which could be deemed to be covered by the restriction. As the Human Rights Committee has stated:

> For the purposes of paragraph 3, a norm, to be characterized as a "law", must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution. Laws must provide sufficient guidance to those charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.[5]

The list of legitimate aims in Article 19(3) – namely the rights or reputations of others, national security and public order, public health or morality – which the second part of the test requires all restrictions to pursue, is exclusive. Both the wording of the article and statements by the UN Human Rights Committee make this clear:

> Restrictions are not allowed on grounds not specified in paragraph 3, even if such grounds would justify restrictions to other rights protected in the Covenant. Restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated. [references omitted][6]

---

[4] General Comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 22. See also *Mukong v. Cameroon*, 21 July 1994, Communication No.458/1991, para.9.7 (UN Human Rights Committee).
[5] General Comment No. 34, *ibid.*, para. 25.
[6] *Ibid.*, para. 22. See also *Mukong v. Cameroon*, note 4, para.9.7.

Finally, the necessity element, or third part of the test, represents the high standard that States seeking to justify restrictions are expected to overcome. As stated by the European Court of Human Rights:

> Freedom of expression, as enshrined in Article 10, is subject to a number of exceptions which, however, must be narrowly interpreted and the necessity for any restrictions must be convincingly established.[7]

The three-part test is internationally accepted as the standard by which violations of freedom of expression should be evaluated and it has proven to be an effective measure of legitimacy. Restrictions on online expression, like all restrictions, are legitimate under international law only if they pass muster under all three parts of the test.

As the Internet has grown in popularity, a number of governments have put in place systems aimed at restricting content online. Online content control can be carried out for legitimate motives, such as restricting access to child pornography, as well as for illegitimate ones, such as silencing political opposition. Similarly, emerging international standards have come to recognise that some methods of enforcing content restrictions are legitimate, while others violate freedom of expression.[8] Clearly, both a legitimate purpose and a legitimate method of enforcement are required in order for a particular framework to pass the three-part test and hence to be considered to comply with international law.

The most definitive statement to date of international human rights standards regarding the Internet is the *Joint Declaration on Freedom of Expression and the Internet* which was adopted in 2011 by the four special international mandates on freedom of expression, the United Nations Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information. As regards systems for filtering and blocking, the Declaration states:

> 3. Filtering and Blocking
>
> a. Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure –

[7] See, for example, *Thorgeir Thorgeirson v. Iceland*, 25 June 1992, Application no. 13778/88, para. 63.
[8] For a more thorough discussion of the methods which have been used to control content on the Internet, see Ronald Deibert *et al.*, *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, United States: MIT Press, 2008).

> 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.
> b. Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.
> c. Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.[9]

A basic principle underlying this statement is that content restrictions should be imposed in as targeted a manner as possible, consistent with the "necessity" requirement in the three-part test. It is also noteworthy that the *Joint Declaration* emphasises the need for transparency regarding end-user filtering systems.[10]

The most targeted techniques involve issuing takedown orders which compel the removal of particular illegal content. If website owners are unwilling or unable to comply with such orders, authorities can also deregister a domain that is hosting restricted content, making the website inaccessible. This is clearly a far less targeted approach, which essentially engages the standards set out about regarding blocking. Furthermore, the efficacy of both of these methods depends on where the website is based. Russian authorities have no power to remove content from websites operating from other countries. In some cases, content removal requests may be voluntarily complied with, either for moral reasons, such as a shared opposition to the spread of child pornography, or commercial ones, such as the threatened revocation of a licence to operate within particular markets. However, to comprehensively restrict the availability of particular types of content will normally require the use of blocking or filtering, which can be carried out at the ISP level, on the Internet backbone at international gateways or both. As the statement by the special mandates makes clear, these sorts of measures are either illegitimate or face a significant hurdle to be justified.

The issuance of takedown orders and implementation of other measures can be done by either an independent administrative body or by the courts. However, given that these are restrictions on freedom of expression, and the paramount need to prevent political abuse of the system, it is an accepted principle that oversight of the system should be done by a body which is fully independent of government and other political forces. In their 2003 Joint Declaration, the special mandates stated, in respect of media regulation:

---

[9] Adopted 1 June 2011. Available at: http://www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.
[10] *Ibid.* See also clauses 5(b) and 6(f).

> All public authorities which exercise formal regulatory powers over the media should be protected against interference, particularly of a political or economic nature, including by an appointments process for members which is transparent, allows for public input and is not controlled by any particular political party.[11]

The same principle applies to regulation of the Internet, whether or not it is deemed to be a form of media. Procedural protections and, in particular, giving those targeted by these measures a full opportunity to contest them, is also required.

It is always important to assess the legitimacy of content restrictions, but this is particularly true when they are applied in an online context since the Internet's value as a medium largely flows from its free and open character. Systems for controlling online content must be assessed not only in terms of their impact on the specific speech that is being targeted, but also in terms of their potential to chill online speech more broadly. In this vein, online privacy has been recognised as being of significant importance to freedom of expression. The importance of protecting communications against undue surveillance has been recognised by the UN Special Rapporteur on Freedom of Opinion and Expression:

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy…. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.[12]

Governments should bear this in mind when considering regulatory systems which affect the Internet, and they should refrain from heavy-handed interventions that could undermine the free character of the Internet.

2. Use of DPI to Monitor Content

The Amendments are somewhat vague as to what specific techniques will be employed to enforce the content restrictions. However, there are some indications that the system will involve DPI. In August 2012, Russia's government began a series of consultations with representatives of Internet-related industries during which, according to reports, DPI was discussed as the most appropriate tool for

[11] Adopted 18 December 2003. Available at: http://www.osce.org/fom/66176.

[12] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, UN Doc. A/HRC/23/40, para. 79.

implementing the law in Russia's bigger cities.[13] In November 2012, Ilya Ponomarev, a member of the State Duma who had been involved in the process, told a journalist that the consultations concluded with a consensus that DPI technology would be employed.[14] It is difficult to ascertain with certainty the degree to which DPI technologies have been, or are being, rolled out. However, if DPI is being used widely, it could present a significant challenge to Internet freedom in Russia.

DPI involves installing automated systems which examine all Internet traffic in search of particular signatures, such as a keyword or a fragment of computer source code.[15] While there are legitimate uses of DPI, such as to screen out viruses or defend against distributed denial of service attacks, its use in order to control the content of communications over the Internet is troubling because the scope of traffic analysis inherent in DPI raises significant privacy concerns. Once a DPI program is in place, it can be adjusted to copy all of the traffic from a particular user to an external storage mechanism, thereby becoming an extremely intrusive surveillance mechanism. DPI technology can even be used to modify Internet traffic on the fly. A sophisticated DPI system is capable, for example, of deleting unfavourable references to a particular political leader on a website and replacing them with favourable ones, without ever notifying the owner of the website.

Whether or not Russian DPI systems are used in this manner, the very existence of such a powerful tool, and the potential that such a pervasive surveillance mechanism might be in place, could be expected to exert a powerful chilling effect on online discourse in Russia. The deployment of DPI technology is particularly problematic when viewed in the context of Russia's poor record in terms of respecting freedom of expression.[16]

Recommendation:

[13] See http://www.gazeta.ru/politics/2012/08/03_a_4709265.shtml [in Russian].
[14] Andrei Soldatov & Irina Borogan, " The Kremlin's New Internet Surveillance Plan Goes Live Today", Wired, 1 November 2012. Available at: http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/.
[15] Ben Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control'", Global Voices, 23 June 2009. Available at: http://advocacy.globalvoicesonline.org/wp-content/uploads/2009/06/deeppacketinspectionandinternet-censorship2.pdf.
[16] Freedom House, *Freedom of Press 2013*. Available at: http://www.freedomhouse.org/report/freedom-press/2013/russia.

- Russia should refrain from using deep-packet inspection technology to enforce the Amendments, and should instead focus on measures which are content-specific in nature.

3. Illegitimate Categories of Banned Content

According to Article 3(2) of the Amendments, material subject to blocking includes sites which contain child pornography, information about illegal drugs and information about suicide. However, on 29 June 2013, the rules were further amended to add material which "propagandises non-traditional sexual relations" to the list of banned content.

This last category is a significant and clear violation of international human rights law. Discrimination and violence based on gender and sexual orientation are recognised as major problems in Russia.[17] Although morality is included as a legitimate interest under Article 19(3) of the ICCPR, it has been unequivocally recognised that this clause should not be used to restrict open debate on matters of sexual orientation. According to the European Court of Human Rights:

> There is no scientific evidence or sociological data at the Court's disposal suggesting that the mere mention of homosexuality, or open public debate about sexual minorities' social status, would adversely affect children or "vulnerable adults". On the contrary, it is only through fair and public debate that society may address such complex issues as the one raised in the present case.[18]

The Venice Commission, an advisory body of legal experts of the Council of Europe, specifically examined the legitimacy of laws in Russia, Ukraine and Moldova targeting the "propagation of homosexuality" in 2013 and concluded:

> On the whole, it seems that the aim of these measures is not so much to advance and promote traditional values and attitudes towards family and sexuality but rather to curtail nontraditional ones by punishing their expression and promotion. As such, the measures in question appear to be incompatible with "the underlying values of the

[17] Human Rights Watch, "Russia: Investigate Attacks on Peaceful LGBT Demonstrators in St. Petersburg", 10 July 2013. Available at: http://www.hrw.org/news/2013/07/10/russia-investigate-attacks-peaceful-lgbt-demonstrators-st-petersburg. Amnesty International, "RUSSIA: ONGOING ATTACK ON THE RIGHTS OF LGBTI PEOPLE", 3 July 2013. Available at: http://www.amnesty.org/en/library/asset/EUR46/028/2013/en/d161580b-5a3a-4bbd-b158-41e000a4f058/eur460282013en.html.

[18] *Alekseyev v. Russia*, 21 October 2010, Applications nos. 4916/07, 25924/08 and 14599/09.

> ECHR", in addition to their failure to meet the requirements for restrictions prescribed by Articles 10, 11 and 14 of the [ECHR].[19]

In short, the addition of material which "propagandises non-traditional sexual relations" to Russia's blacklist represents the latest in a series of discriminatory measures adopted by Russia's government targeting the LGBT community, and is an unjustifiable infringement of the right to freedom of expression, among other core human rights.

The prohibitions on information about illegal drugs and information about suicide are also problematic, due to their vague and broad nature. Material relating to drug use, for example, might include anything from Bob Marley records to websites advocating the legalisation of marijuana.

A cardinal principle of freedom of expression is that restrictions must be constructed as narrowly as possible, in line with the "necessity" requirement of the three-part test. This means that the categories of prohibited content should be precisely defined. If a law could be open to a range of different interpretations, the effect is that speech is potentially restricted to the broadest extent of those interpretations. Vague definitions can also lead to a chilling effect, as the uncertainty forces speakers to steer well clear of the possible outer limits of the restriction. The prospect of having a website blacklisted is serious enough to influence decisions about what to publish on it. This is particularly true given that the law places obligations on third parties, such as Internet service providers (ISPs) or web hosts, neither of which can be expected to take risks to defend third party content. Although the Amendments do not specifically impose liability on ISPs or web hosts, these bodies are required to enforce deletion orders, and ISPs risk losing their licence if they fail to comply promptly with their responsibilities.

Having been in force for less than a year, there are already indications that the restrictions are being enforced in an overly broad manner. Among the sites which have been banned are a YouTube video on applying Halloween makeup to simulate wounds, which was found to promote self-harm,[20] and several Russian-language Wikipedia pages, including the entries for "suicide", "self-immolation" and several types of illegal drugs.[21] The blocking of these sites, which are clearly informative or

---

[19] Opinion 707/2012, adopted 14-15 June 2013. Available at: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2013)022-e.
Alekseyev v. Russia, 21 October 2010, Applications nos. 4916/07, 25924/08 and 14599/09, .

[20] Kevin Collier, "Google Loses Appeal in Russian YouTube Censorship Battle", Daily Dot, 7 May 2013. Available at: http://www.dailydot.com/news/google-russia-censorship-appeal-youtube-makeup-vid/.

[21] See http://wikimedia.ru/blog/2013/04/08/15blacklisted/ [in Russian].

for purely entertainment value, extends far beyond what might be considered necessary in order to combat suicide or illegal drug use, and cannot be justified according to the three-part test. Their blocking is symptomatic of the over breadth of the categories enumerated in the Amendments.

Recommendations:

- The prohibition on material which ""propagandises non-traditional sexual relations" should be removed.
- The Amendments should limit prohibited content to child pornography, and material which explicitly incites others to commit suicide or use illegal drugs.

4. Lack of Procedural Protections

Due to the gravity of the freedom of expression restrictions inherent in blocking or prohibiting content, it is imperative that the systems by which restrictions are applied involve robust procedural protections to guard against potential abuses.

A fundamental ingredient of procedural fairness is that the oversight body should be independent from government, in order to ensure that restrictions on freedom of expression are exercised in an apolitical manner. Unfortunately, the Roskomnadzor signally fails to meet this vital condition. According to Article 8 of the "Regulations on Federal Service for Supervision in Telecommunications, Information Technology and Mass Communications",[22] the Roskomnadzor operates under the jurisdiction of the Minister of Telecommunications and Mass Communications, who has the power to both appoint and dismiss its head.

In addition to the absence of institutional independence within the oversight body, the law's mechanism for enforcement operates far too rapidly to allow for adequate procedural protections. If the Roskomnadzor decides that a particular website contains prohibited content, the web host is informed of the problem and instructed to pass the order on to the website's owner. However, the website's owner is given only 24 hours to respond to this notice by removing the content. If, after 24 hours, the material has not been taken down, the web host is itself then required to delete the website, within a further 24 hours. 48 hours after the original notice, if the material

[22] Adopted 16 March 2009.

remains online, the Roskomnadzor has a mandate to add the IP address of the website to the blacklist, with a requirement for all Internet service providers within Russia to block access to the content or risk losing their license to operate.

The speed at which this process moves is highly problematic, as it does not provide website owners with enough time to mount a defence of their content. It is also unclear whether website owners, if they are able to respond in time, are even given an opportunity to argue their case. Oversight of the process is managed entirely by the Roskomnadzor, with no judicial role in approving deletion orders. The only recourse website owners have is to file a lawsuit challenging the Roskomnadzor's decision. In addition to being expensive, judicial challenges move slowly, and the impugned content must remain blocked until a judicial order to the contrary is obtained. Observers have expressed concern that this process could easily be manipulated by pro-government groups, who might plant banned material on opposition websites or forums as a means of getting them blocked.[23]

Recommendations:

- Oversight over the law's implementation should be vested in a body which is independent from the Russian government.
- The notice period for website owners to respond to complaints should be significantly extended and an effective right of appeal should be provided for so that website owners can challenge complaints before an independent body before their material is taken down. Website hosts should also be granted more time to delete the content before they are added to the blacklist. If deemed necessary, a more rapid process, but still involving a right of appeal, could be put in place for the rare cases where it is necessary to remove content rapidly due to its exceptionally harmful nature.
- Website owners should have the right to appeal any takedown notice to the courts.

5. Lack of Transparency

Transparency is a critical component of a legitimate system of online content control. At the front end, this requires complete openness about how regulatory measures are

[23] Alex Johnston, "Russian Censorship Law Goes Online", The Epoch Times, 1 November 2013. Available at: http://www.theepochtimes.com/n2/world/russian-censorship-law-goes-online-310388.html.

targeted and implemented. Besides fulfilling a basic requirement for government accountability, this openness allows mistakes to be rectified. If an authority maintains a blacklist of banned websites, it is only natural that some innocent sites will find themselves wrongly blocked. In 2009, Wikileaks released what they claimed was a copy of the secret blacklist compiled by the Australian Communications Media Authority (ACMA).[24] Ostensibly targeted only at sexual abuse, sexual violence and detailed instructions on committing crimes, the leaked list also included entries from Wikipedia and YouTube, as well as various religious sites, music sites, a tour operator and a Queensland dentist.[25] An alleged blacklist from Thailand, also released by Wikileaks, contained a similarly eclectic mixture of innocuous content, including websites hosting Charlie Chaplin videos and campaign ads from United States politician Hilary Clinton.[26]

Since the Amendments came into effect in November 2012, there are indications that Russia's blacklist has been plagued by similar mistakes. IP addresses for the homepages of both Google and YouTube have been mistakenly blocked due to what Roskomnadzor called "technical glitches".[27] In December 2012, a report by the Russian Pirate Party, an opposition group that promotes digital freedom, claimed that among the blocked sites were kindergartens, bedroom furniture makers and vegetarian cookbooks.[28]

Although Roskomnadzor has set up a website which allows users to check whether a particular website is blocked,[29] the full database of blocked sites is only available to webhosts and ISPs.[30] Keeping the blacklist secret prevents proper oversight by journalists or civil society. It also makes it difficult to determine whether significant numbers of innocuous sites are being caught up in the mechanism, or whether the law is being used to unfairly target particular individuals or groups. Secrecy also

---

[24] See http://wikileaks.org/wiki/Australian_government_secret_ACMA_internet_censorship_blacklist,_6_Aug_2008.

[25] It should be noted that there is some question as to the list's authenticity. The Australian government initially denied that it was accurate, before admitting that it "seemed to be close" to the real list. See http://www.news.com.au/news/blacklist-looks-like-acmas-conroy/story-fna7dq6e-1225699544375.

[26] See http://wikileaks.org/wiki/1,203_new_websites_censored_by_Thailand.

[27] "Second Google Blacklisting was a 'Glitch' – Media Watchdog", RIA Novosti, 26 November 2012. Available at: http://en.rian.ru/russia/20121126/177739712.html.

[28] "Russian Internet Blacklist 96% Illegal – Pirates", RIA Novosti, 17 December 2012. Available at: http://en.rian.ru/russia/20121217/178221958.html.

[29] The tool is available (in Russian) at: http://zapret-info.gov.ru/.

[30] Andrei Soldatov & Irina Borogan, " The Kremlin's New Internet Surveillance Plan Goes Live Today", Wired, 1 November 2012. Available at: http://www.wired.com/dangerroom/2012/11/russia-surveillance/all/.

increases uncertainty as to how the standards are being applied, and where the line is drawn as to what material is deemed unacceptable. Consequently, this practice fails to fulfil the requirement for clarity in the first branch of the three-part test.

Recommendation:

- A full list of which websites are being blocked should be published online and regularly updated.