PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DÉFENSE DE L'INTÉRÊT PUBLIC

285 McLeod Street, Suite 200, Ottawa, ON K2P 1A1

24 September 2021

Digital Citizen Initiative
Department of Canadian Heritage
25 Eddy St, Gatineau QC K1A 0S5

BY EMAIL to: pch.icn-dci.pch@canada.ca

Re: ***The Government's proposed approach to address harmful content online*- Submission of the Public Interest Advocacy Centre**

Dear Consultation Secretariat Staff,

The Public Interest Advocacy Centre (PIAC) is pleased to provide the Government of Canada with our submission on the Government's proposed approach to address harmful content online, which is attached.

Sincerely,

John Lawford
Digitally signed by John Lawford
Date: 2021.09.24 19:43:39 -04'00'

John Lawford
Executive Director & General Counsel
613-562-4002
jlawford@piac.ca

Introduction

The Public Interest Advocacy Centre (PIAC) is providing the below comments on the Government of Canada's proposed approach to regulating social media and combatting harmful content online ("Proposal"). PIAC is a national non-for-profit organization and registered charity that provides legal and research services on behalf of consumer interests, and, in particular, vulnerable consumer interests, concerning the provision of important public services. We are commenting narrowly on the possible impact that the Proposal's site-blocking feature may have on telecommunications consumers, but reserve the right to comment on any aspect of the Proposal at a later stage.

The Proposal states that the new legislation would apply to "online communication service providers" (OCSPs) and would include specific exemptions for telecommunications service providers (TSPs). PIAC supports this distinction and recommends that the government continue to draw an explicit line between OCSPs and TSPs. TSPs should not be able to circumvent their telecommunications duties under the *Telecommunications Act* by arguing that they are governed by the new regime under this Proposal.[1] The government should ensure TSPs continue to fulfill their obligations to telecommunications users as required by the laws and regulations overseen by the Canadian Radio-television and Telecommunications Commission (CRTC).

The Proposal suggests establishing a Digital Safety Commissioner and giving it the authority to apply, once all enforcement measures have been exhausted, to the Federal Court for an order requiring relevant TSPs to block access – in whole or in part – to an OCSP repeatedly demonstrating persistent non-compliance with orders respecting the removal of child sexual exploitation content or terrorist content. The Proposal states that s.36 of the *Telecommunications Act* will not apply to Canadian carriers that comply with these blocking orders and does not plan to repeal or amend this section.

With the exception of child sexual exploitation content, which is already *de facto* censored by the Cybertip.ca Cleanfeed project, PIAC does not believe that site-blocking is an appropriate mechanism to address the online harms identified in the Proposal. If the Proposal is to create an avenue for site-blocking we suggest that the CRTC be the decision-maker, so as to ensure that site-blocking does not undermine Canada's telecommunications system nor impair Canadian's rights to telecommunications services. If the government decides to make the Federal Court the site-blocking adjudicator we suggest that it create explicit requirements that the court consider s. 36 and s. 27(2) rulings and jurisprudence and issue orders that apply narrowly to the conduct of

[1] As an example of attempted circumvention, in Broadcasting and Telecom Decision CRTC 2015-26, Bell Mobility and Videotron attempted avoid application of the *Telecommunications Act* by arguing they were broadcasting undertakings when offering mobile TV services rather than TSPs, despite the fact that subscribers needed to have a mobile wireless voice plan, data plan, or tablet plan in order to access mobile TV services. The CRTC rightfully concluded that the two companies were providing telecommunications services and thus subject to the *Telecommunications Act.*

the specific parties before them in order to safeguard Canada's telecommunications system and the CRTC's role in regulating it.

ISP site-blocking is not an appropriate mechanism to address online harms

PIAC submits that it is likely not appropriate to create a regime in which ISPs are required by court order to block user access to non-compliant OCSPs because mandatory site-blocking: 1) is incompatible with Canada's net neutrality framework rooted in ss. 36 and 27(2) of the *Telecommunications Act* as articulated by the CRTC; and 2) could result in excessive infringement of Canadians' rights to freedom of expression on the Internet.

Incompatibility with Canada's net neutrality framework

Net neutrality is the concept that all data traffic on a network should be treated indiscriminately and that internet service providers (ISPs) should be restricted from blocking, slowing down or speeding up the delivery of online content at their discretion. There are many iterations of net neutrality around the world and determining the scope of net neutrality requires looking specifically at the ways ISPs are regulated within the relevant jurisdiction. In Canada, the CRTC has stated that the following documents make up Canada's net neutrality framework: Telecom Regulatory Policy CRTC 2017-104 (*Differential pricing practices)*, Telecom Decision CRTC 2017-105 (*Videotron unlimited music*), Broadcasting and Telecom Decision CRTC 2015-26 (*Bell Mobile TV*), and Telecom Regulatory Policy CRTC 2009-657 (*Internet traffic management practices*).[2] Underlying this framework are the factors upon which public support for net neutrality is built: competition, innovation, consumer choice, access and affordability, and privacy.[3]

Canada's net neutrality framework is rooted in ss. 27(2) and 36 of the *Telecommunications Act,* which must be interpreted and applied to further the telecommunications policy objectives set out in section 7 of the *Telecommunications Act.*

Section 27(2) prohibits Canadian carriers from unjustly discriminating or giving undue or unreasonable preference or disadvantage to any person, including itself and competitors. The CRTC has set out four criteria for considering whether preference is undue or unreasonable in the context of differential price setting:

- the degree to which the treatment of data is agnostic (i.e. data is treated equally regardless of its source or nature);
- whether the offering is exclusive to certain customers or certain content providers;

[2] Telecom Regulatory Policy CRTC 2017-104*, Framework for assessing the differential pricing practices of Internet service providers*, 20 April 2017 [*Differential pricing practices*].
[3] *Ibid.* at para 32.

- the impact on Internet openness and innovation; and
- whether there is financial compensation involved.[4]

Using these criteria, the CRTC has previously held that zero-rating data charges associated with a category of content resulted in undue preference/disadvantage.[5] Since the impact of outright blocking is greater than differential price setting it follows that blocking would also unduly disadvantage website users and operators, who are unable to obtain or provide the content they wish to obtain or provide. The user is unduly disadvantaged relative to a user accessing other content, and the operator is unduly disadvantaged relative to operators who run other sites. Implementing a site-blocking regime may also potentially disadvantage smaller or newer ISPs, who may be less able to absorb the cost of updating their networks to enable blocking. The extent of these costs will depend on what blocking system is ordered and how the list of non-compliant OCSPs is maintained and updated. The government should be mindful of placing additional burden on ISPs, particularly smaller or newer ones, in order to ensure the public has access to adequate levels of choice and competition is sufficient to drive innovation. Lastly, while there are not, to our knowledge, vertically integrated ISPs and OCSPs such a possibility may present itself in future, at which point there will likely be additional concerns regarding impacts on competition and also freedom of expression, as ISPs will have financial incentive to suppress content on non-affiliate OCSPs.

Section 36 of the *Telecommunications Act* limits the ability of Canadian carriers to control the content or influence the meaning or purpose of telecommunications carried over their networks without prior CRTC authorization, but does not give the CRTC the power to require TSPs to block content. In the 2018 *FairPlay Decision,* the CRTC stated: "section [36] gives the Commission the explicit power to authorize an ISP to block a website, the proposed regime would go further and require such blocking pursuant to a Commission order. Because section 36 confers an authorizing power and not a mandatory power, the power to mandate blocking must be found elsewhere…"[6]

The CRTC then determined it is only able to approve ISP content blocking if doing so will further the telecommunications policy objectives in s. 7, under certain circumstances. In the context of Internet traffic management practices, the CRTC has stated:

> 122. The Commission finds that where an ITMP would lead to blocking the delivery of content to an end-user, it cannot be implemented without prior Commission approval. Approval under section 36 would only be granted if it would further the telecommunications policy objectives set out in section 7 of the Act. Interpreted in light of these policy objectives, ITMPs that result in blocking

[4] *Ibid.* at para. 126.
[5] Telecom Decision CRTC 2017-105, *Complaints against Quebecor Media Inc., Videotron Ltd., and Videotron G.P. alleging undue and unreasonable preference and disadvantage regarding the Unlimited Music program,* 20 April 2017.
[6] Telecom Decision CRTC 2018-384, *Asian Television Network International Limited, on behalf of the FairPlay Coalition – Application to disable online access to piracy websites,* 2 October 2018, at para. 69 [*FairPlay Decision*].

> Internet traffic would only be approved in exceptional circumstances, as they involve denying access to telecommunications services.

Similarly, in Telecom Decision CRTC 2016-479 the CRTC affirmed, in the context of Quebec's attempt to block access to unauthorized gambling websites, that "blocking would only be approved where it would further the telecommunications policy objectives set out in section 7 of the Act."[7] The CRTC did not find that Quebec's actions would further these objectives but, rather, would impede them.

The Supreme Court of Canada has summarized the purpose of the *Telecommunications Act* in light of its policy objectives as being "to encourage and regulate the development of an orderly, reliable, affordable and efficient telecommunications infrastructure for Canada."[8] PIAC submits that blocking the delivery of almost any content to end-users is fundamentally at odds with the policy objectives set out in s. 7. A TSP that blocks content requested and transmitted over their network effectively is an unreliable service provider providing sub-standard service from a user point of view. The very point of an ISP, indeed, the reason a contract exists between the ISP and the user, and what the ISP accepts monetary compensation for, is to provide access to the Internet and to carry traffic over the ISPs' network to and from the wider Internet.

Section 7(i) of the *Telecommunications Act* requires telecommunications policy to "contribute to the protection of the privacy of persons". Further, the CRTC has stated that it

> "recognizes that [Virtual Private Networks] VPNs are a legitimate tool to protect sensitive information, as recommended by security firms. While the Commission does not find differential pricing practices to have a direct negative impact on privacy per se, it is concerned that their adoption could discourage the use of VPNs and thus compromise the privacy and/or security of consumers.[9]

The CRTC has consistently held that subs. 7(i) permits the Commission to create higher privacy obligations in relation to confidential customer information in telecommunications than is required in general Canadian privacy law.[10]

Upholding individuals' ability to protect their privacy through VPNs and other encryption methods may make site-blocking an ineffective tool for preventing access to non-compliant OCSPs and these tools may, under the CRTC's approach to privacy under subs. 7(i), be held to be an important aspect of telecommunications' users' privacy. There are a variety of ways users, even technically unsophisticated ones, may easily circumvent blocked access to websites. One method of blocking websites is to program the Domain Name System (DNS) server to refuse to translate the URL into an IP address. When a person looks up a website, they enter a URL

---

[7] Telecom Decision CRTC 2016-479, *Public Interest Advocacy Centre – Application for relief regarding section 12 of the Quebec Budget Act,* at para. 7 [Telecom Decision*, Quebec Budget Act*].
[8] *FairPlay Decision*, *supra* note 4 at para. 69, citing *Barrie Public Utilities v. Canadian Cable Television Assn.*, [2003] 1 SCR 476, at paragraph 38.
[9] *Differential pricing practices*, *supra* note 5 at para. 78.
[10] See: Telecom Decision 2003-33 and 2003-33-1, Confidentiality provisions of Canadian carriers. Online: https://crtc.gc.ca/eng/archive/2003/dt2003-33.htm

including a domain name (ex. Google.ca). A DNS server translates domain names into an IP address which can be used to communicate directly with the websites. Most ISPs have their own DNS servers, which customers may, and most do use (although a technically sophisticated user can specify their preferred DNS server to be one other than that of their ISP). DNS-based blocking can be easily circumvented by entering the IP address directly, using a proxy, using another DNS server or following a link to the IP address. Another method is to block the IP address. This can be easily circumvented by users by using a VPN, which hides the destination of web traffic from the internet service provider. IP blocking is also easy for the site operator to circumvent by changing their IP addresses. A third method is to inspect the packets of data to determine their destination and block packets destined for the infringing website Deep-packet inspection can be easily circumvented by encrypting web-traffic. End users do not have to understand these circumvention measures to use them. Through software users can establish encrypted private network connection with a non-compliant OCSP which an internet service provider cannot block.

The Proposal's indication that ISPs may be required to block access to only a part of a non-compliant OCSP leads PIAC to presume that deep-packet inspection would be a necessary blocking method. Deep-packet inspection would require ISPs to examine aspects of packets which they would not otherwise examine and use that information to make a decision about whether the packet should be permitted to pass. These additional steps may impose undue burden on ISPs potentially impacting network performance and competition among telecommunications companies. Deep-packet inspections may also constitute an unreasonable search if they reveal private information about users, for example, their financial, medical, or personal information, which is at the heart of the "biographical core" protected by s.8 of the *Charter.*[11]

Finally, the CRTC has forbidden, on the basis of users' confidentiality interests, ISPs' use of deep packet inspection for any purpose except traffic management:

> 103. In light of the above, the Commission finds it appropriate to establish privacy provisions in order to protect personal information. The Commission therefore directs all primary ISPs, as a condition of providing retail Internet services, not to use for other purposes personal information collected for the purposes of traffic management and not to disclose such information. [12]

[11] Depending on the context, Canadians have a reasonable expectation of privacy in their identity as the internet subscriber associated with particular usage (R v Spencer 2014 SCC 43) and in their personal digital devices (R v Fearon 2014 SCC 77) and in electronic conversations (R. v. Marakah 2017 SCC 59; R. v. TELUS Communications Co. 2013 SCC 16), and personal computers (R. v. Morelli 2010 SCC 8) and work computers where personal use is permitted (R. v. Cole 2012 SCC 53).
[12] Telecom Regulatory Policy CRTC 2009-657, *Review of the Internet traffic management practices of Internet service providers* (21 October 2009), at para. 103.

It is not surprising, therefore, that given the scope of ss. 27(2) and 36 that the CRTC has yet to approve a site-blocking request, even in situations of alleged harm.[13] PIAC submits that nothing in the *Telecommunications Act* nor the net neutrality framework articulated by the CRTC provides an exception to allow site-blocking merely because content is criminal or, to use the language of the Proposal, harmful. As this section of our comments highlights, ss. 27(2) and 36 have been interpreted in such a way as to require ISPs to treated content agnostically and not prefer, restrict, slow, or block content unless the CRTC authorize them to do so, having determined that differential treatment or restricted access will further the objectives of telecommunication policy. Any argument that restricting access to a subset of non-compliant OCSPs has only an incidental interference with the provision of telecommunications service is untenable. The nature of Internet activity is that it is personal to the user. The government, CRTC, ISP, and OCSP do not know the extent to which users, those engaging in harmful content and those not, rely on the OCSP that is to be restricted. Restricting access could have the effect of seriously impeding service if a customer only or predominantly uses the Internet to access the blocked websites.

Potential Impact on Freedom of Expression

The CRTC has acknowledged the role of Internet access in safeguarding, enriching, and strengthening Canada's "social and economic fabric."[14] Free expression on the Internet is fundamental to this fabric and, according to a Joint Declaration by the UN Special Rapporteur for Freedom of Opinion and Expression and the IACHR-OAS Special Rapporteur on Freedom of Expression:

> [A]ll restrictions on freedom of expression, including those that affect speech on the Internet, should be clearly and precisely established by law, proportionate to the legitimate aims pursued, and based on a judicial determination in adversarial proceedings. In this regard, legislation regulating the Internet should not contain vague and sweeping definitions or disproportionately affect legitimate websites and services.

PIAC submits that government mandated website blocking necessarily engages s. 2(b) of the *Canadian Charter of Rights and Freedoms* and this right ought to be considered by the government in the context of the Proposal. We find support for this position in s. 41(1) of the *Telecommunications Act*, which requires the CRTC consider freedom of expression when

[13] As an example, in a Letter Decision from Diane Rheaume, Secretary General of the CRTC to J. Edward Antecol dated 24 August 2006 (file no. 8622-P49-200610510), the CRTC declined an application purportedly made under s. 36 to have the Commission proactively authorize ISPs to block certain websites alleged to constitute hate speech. The applicant provided expert evidence in support of his view that the two websites in question violated the *Criminal Code*. He also claimed that the websites, having posted his home address and made repeat and violent anti-Semitic statements, cause him to fear for his personal safety and the community at large. The CRTC reiterated that s.36 could not be used to require ISPs to block access to websites and denied the Application for procedural reasons.

[14] For example, Telecom Regulatory Policy CRTC 2016-496, *Modern telecommunications services – The path forward for Canada's digital economy,* 21 December 2016 at para. 21.

deciding to prohibit or regulate unsolicited telecommunications to prevent undue inconvenience or nuisance.

Canadians have a right to "freedom of […] expression, including freedom of the press and other media of communication." The fundamental values underlying the guarantee of freedom of expression were well articulated by McLachlan J's dissent (not on this point) in *R v Keegstra* [1990] 3 SCR 697. To paraphrase, the main justifications for freedom of expression are:

1. The free flow of ideas is essential to political democracy and the functioning of democratic institutions.
2. A marketplace of ideas leads to a more relevant, vibrant, and progressive society.
3. People have a fundamental right to their own beliefs and opinions, and to express them, and such expression contributes to the self-realization of both speaker and listener.

What constitutes protected expression under Supreme Court of Canada jurisprudence is quite broad and includes non-violent hate speech[15] and child pornography.[16] Both types of expression have been limited via *Criminal Code* prohibitions in ways that have been held demonstrably justifiable in a free and democratic society and PIAC is not arguing that it is impossible for the government to further restrict these forms of expression in justifiable ways. However, we want to raise our concerns about the potential issues with the Proposal's site-blocking regime in relation to freedom of expression.

Harm is often dependent on one's perception. PIAC took the position that net neutrality does not warrant special treatment for harmful or even criminal content in relation to disabling access to sites hosting content allegedly infringing copyright[17] and in relation to Bill 74 which purported to allow the Province of Québec to require ISPs to block access to 'unauthorized' gambling websites within 30 days of receipt of notice from Quebec.[18] In the former instance, copyright holders argued access to content allegedly infringing copyright was harmful, but some users, site operators, and ISPs disagreed. In the latter, the government of Quebec claimed unauthorized online gambling websites were harmful because they did not contain the same responsible gaming rules as sites run by the government. However, the province also embedded the site-blocking regime in a budgetary bill and made it clear that blocking access to unauthorized websites would generate significant revenue, thus demonstrating how the concept of harm can be used to mask other aims. Reasonable people can disagree about the value of various forms of expression and whether such expression ought to be suppressed to prevent harm.

For example, the Proposal suggests that users may be blocked from accessing OCSPs that are repeatedly non-compliant in blocking access to "terrorist content" and that the definition of this harm will be based on the *Criminal Code.* The *Criminal Code* contains a definition of "terrorist

[15] *R v Keegstra* [1990] 3 SCR 697.
[16] *R. v. Sharpe*, 2001 SCC 2, [2001] 1 S.C.R. 45; R. v. Barabash, 2015 SCC 29, [2015] 2 S.C.R. 522.
[17] *FairPlay Decision*, *supra* note 4 at para. 67
[18] Telecom Decision, *Quebec Budget Act*, *supra* note 10.

activity" which, to paraphrase, requires: 1) an act or omission; 2) committed, at least in part, for a political, religious, or ideological purpose; 3) with some intention to intimidate the public with regard to its security, including economic security, or with some intention to compel a person, government, or organization to do or refrain from doing any act; and 4) that intentionally a) causes death or serious bodily harm through violence, b) endangers a person's life, c) causes a serious risk to the health or safety of the public, d) causes substantial property damage, whether to public or private property, or e) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to cause death or bodily harm or endanger a person's life. PIAC is concerned that there may be instances where it is difficult to distinguish between legitimate forms of expression and terrorist content. For example, protest and work stoppages are excluded from the above definition, but it is not clear if they would be captured under "terrorist content" if, for example, the content depicted people seriously disrupting an essential service with the intention of compelling a government or organization to respond to protest or labour demands, both of which are made for an ideological purpose. PIAC recommends that the government provide more information, after consultation with civil liberties societies and minorities' rights groups, on how it intends to ensure that the scope of content to be blocked under the category of "terrorist content" does not capture otherwise legitimate forms of expression, including advocacy, protest, dissent, and work stoppages, which may, depending on one's political perspective, resemble terrorist activity. PIAC also recommends that the government consider safeguards to ensure that governments, corporate interests, and majority groups are not able to use the proposed site-blocking regime to suppress expression that threatens their power by, for example, repeatedly complaining about OCSP non-compliance and having these complaints entertained by the Digital Safety Commissioner, whose level of independence is not clear from the Proposal. As former CRTC National Commissioner Timothy Denton, as he then was, wrote: "History shows that schemes of regulation – and censorship – have a tendency to expand […]."[19] PIAC is concerned that over time more and more content may be restricted, under the guise of harm, to suit the desires of the state.

Content that sexually exploits children is nearly universally accepted as harmful and PIAC is not against blocking access to child pornography. However, PIAC wonders why they government has not acknowledged that Canada's major ISPs already voluntarily block customer access to non-Canadian websites that are hosting child pornography using Cleanfeed Canada, an undertaking of the Canadian Coalition Against Internet Child Exploitation (CCAICE).[20] ISPs currently perform this blocking without, to our knowledge, legislated authority.[21] PIAC suggests the government consider regulating this existing practice and determining what needs to be

[19] Broadcasting Regulatory Policy CRTC 2009-329, *Review of broadcasting in new media*, 4 June 2009, Concurring opinion of Commissioner Timothy Denton (Revised as of 8 July 2009).
[20] Cybertip.ca, "Cleanfeed Canada" online: <https://www.cybertip.ca/app/en/projects-cleanfeed>.
[21] Cybertip.ca states: "ISPs do not consider themselves qualified to determine the legality of content. The Criminal Code allows a judge to make such legal determinations for child pornography content on the Internet, and to issue take-down orders if such content is hosted in Canada. ISPs follow this legislation and rely on the courts for direction. There is no such legislation for child pornography content hosted outside of Canada, so filtering access based on the Cybertip.ca list is an effective way to deal with such foreign content."

done in order to use this system to further reduce Canadian's exposure to child abuse images and create a disincentive for those who access and distribute child pornography in a way that is effective, proportional, and results in minimal impairment to expression that does not constitute child exploitation.

Since justifying infringement of a *Charter* right requires an assessment of whether the measures selected are rationally connected to the aim of the legislation, which in this instance is reducing public exposure to terrorist content and child exploitation content, PIAC's comments regarding the potential ineffectiveness of site-blocking mentioned in the previous section are also relevant to the discussion of freedom of expression.

Recommendations if the government is to move forward with a mandatory site-blocking regime

PIAC does not believe it is appropriate to create a site-blocking regime that will require ISPs to block access to non-compliant OCSPs. However, if the government is to create an avenue for site-blocking, PIAC suggests that the CRTC be the decision-maker so as to ensure that Canadians' right to telecommunications services and right to freedom of expression, as discussed above, are not unduly restricted.

In its 2018 *FairPlay* Decision, the CRTC stated that s. 36 "gives the Commission the explicit power to authorize an ISP to block a website, [but that] the proposed regime would go further and require such blocking pursuant to a Commission order. Because section 36 confers an authorizing power and not a mandatory power, the power to mandate blocking must be found elsewhere…"[22] The government would, therefore, need to amend the *Telecommunications Act* to provide the CRTC with the ability to issue site-blocking orders on application from not only Canadian carriers, but other interested parties, including, presumably, the Digital Safety Commissioner. This amendment would provide the CRTC with the authority to consider and, in very limited instances, issue mandatory site-blocking orders in ways that are congruent with telecommunications law and policy.

PIAC cautions that creating a court ordered site-blocking regime may produce results inconsistent with the CRTC's existing, approval-based site-blocking regime if, for example, an ISP seeking to block content via CRTC approval is denied, but the Digital Safety Commissioner is subsequently granted a Federal Court site-blocking order requiring the ISP to block content. Since the CRTC's decisions are based on telecommunications policy considerations such an inconsistence may undermine Canada's telecommunications system. That said, if the government intends to make a court ordered site-blocking regime, we suggest that it include explicit requirements that the court consider s. 36 and s. 27(2) rulings and jurisprudence and

[22] Telecom Decision CRTC 2018-384, *Asian Television Network International Limited, on behalf of the FairPlay Coalition – Application to disable online access to piracy websites,* 2 October 2018, at para. 69 [*FairPlay Decision*].

issue orders that apply narrowly to the conduct of the specific parties before them in order to safeguard Canada's telecommunications system and the CRTC's role in regulating it.

PIAC notes that the Federal Court of Appeal (FCA) recently affirmed the availability of mandatory interlocutory injunctions as a means of blocking online access to content allegedly infringing copyrighted materials in Canada.[23] In the absence of parliamentary intervention, site-blocking orders will likely be issued based on the factors identified by Mr. Justice Gleeson in *Bell Media Inc. v. GoldTV.Biz*, 2019 FC 1432 not only in the context of online 'piracy', but online harms as well.

PIAC is not commenting on the general appropriateness of these factors,[24] but submits that they may be insufficient to safeguard Canada's net neutrality framework and Canadians' right to freedom of expression, noted above, especially given Mr. Justice Gleeson's consideration of these issues – upheld by the FCA – was as follows:

> "I am not prepared to conclude, as the Plaintiffs have suggested, that the principle of net neutrality is of no application where a site-blocking order is sought. However, I am satisfied, in the face of a strong *prima facie* case of ongoing infringement and a draft order that seeks to limit blocking to unlawful sites and incorporates processes to address inadvertent over-blocking that neither net neutrality nor freedom of expression concerns tip the balance against granting the relief sought. As has been previously noted by the Supreme Court of Canada, albeit in a different context, the jurisprudence has not, to date, accepted that freedom of expression requires the facilitation of unlawful conduct (*Equustek* at para 48). Similarly I am not convinced that the principle of net neutrality, or the common carrier doctrine, is to be applied in a manner that requires ISPs to facilitate unlawful conduct."[25]

PIAC also notes that court ordered site-blocking can be impractical and burdensome. Mr. Justice Gleeson's site-blocking order has been updated several times to expand the list of domains to be blocked and remove domains no longer being used to provide access to the allegedly copyright-infringing content.[26] PIAC is not surprised by this outcome because, as we have described above, site operators and users can easily circumvent domain and IP address blocking. Also noted above is our understanding that smaller ISPs may be disproportionately impacted by the costs associated with ongoing and rapidly change blocking requirements. The

[23] *Teksavvy Solutions Inc. v. Bell Media Inc*., 2021 FCA 100.
[24] Mr. Justice Gleeson used factors cited in United Kingdom jurisprudence and codified by the United Kingdom parliament in *Copyright, Designs and Patents Act 1988.* At the irreparable harm stage, Gleeson J. considered whether the injunction was necessary to protect the plaintiff's rights and the availability of alternative and less onerous measures. In weighing the balance of convenience he considered: effectiveness; dissuasiveness; complexity and cost' barriers to legitimate use or trade; fairness, including a brief note on freedom of expression and net neutrality; substitution; and safeguards.
[25] *Bell Media Inc. v. GoldTV.Biz*, 2019 FC 1432 at para. 97.
[26] The Wire Report, "Site-blocking in GoldTV case expanded again" (Sept 2021), online: <https://www.thewirereport.ca/2021/09/15/site-blocking-in-goldtv-case-expanded-again/>.

issues of practicality and burden have broader implications on telecommunications law and policy and, therefore, would be more properly addressed by the CRTC.

PIAC notes that Bell, Rogers, and Quebecor are requesting the Federal Court establish Canada's first-ever "dynamic" site-blocking order, which would require third-party ISPs to block a rolling list of IP addresses in real-time, as they are identified by the broadcasters as broadcasting 'pirated' National Hockey League games while those games are being broadcast throughout the NHL season.[27] If granted this order would require proactive content blocking, which is problematic for reasons discussed in our comment. This request demonstrates the growing need for the government, if it is to have court ordered site-blocking, to set parameters to minimize the impact of such decision on Canada's telecommunications system.

PIAC notes that Teksavvy is appealing the FCA decision to the Supreme Court of Canada arguing, in part, that judicial site-blocking "risks displacing and overtaking Parliament's carefully-crafted statutory regime…" and is "incompatible with the statutorily mandated neutrality of ISPs as common carriers..."[28] PIAC awaits the result of this appeal as should the government, before moving forward with legislation requiring ISPs to block content.

Conclusion

PIAC reiterates that site-blocking we believe it is inappropriate to use site-blocking to address the online harms identified in the Proposal, except in so far as to legislate and expand upon the existing practice of ISP's blocking access to non-Canadian websites that are hosting child pornography using Cleanfeed Canada.

If the Proposal is to create an avenue for site-blocking we suggest that the CRTC be the decision-maker so as to ensure that site-blocking does not undermine Canada's telecommunications system nor impair Canadian's rights to freedom of expression.

If the government makes the Federal Court the site-blocking adjudicator we suggest that it provide explicit requirements that the court consider s. 36 and s. 27(2) rulings and jurisprudence and issue narrow orders that apply only to the conduct of the specific parties before them in order to safeguard the role of the CRTC and Canada's telecommunications system.
As stated in the introduction, PIAC may voice our additional concerns about the Proposal at a later stage, particularly our concerns about: mandatory OCSP reporting to law enforcement and CSIS; extended data retention periods; expansion of the *Mandatory Reporting Act* to require

[27] The Wire Report, "Bell, Rogers, and Quebecor seek first-ever 'dynamic' site-blocking order"(July 2021), online: <https://www.thewirereport.ca/2021/07/08/bell-rogers-and-quebecor-seek-first-ever-dynamic-site-blocking-order/>.
[28] Chris Cooke, "Canadian ISP takes web-blocking debate to the country's Supreme Court" (Aug 2021), online: <https://completemusicupdate.com/article/canadian-isp-takes-web-blocking-debate-to-the-countrys-supreme-court/>.

ISPs to provide basic subscriber information to law enforcement; and the proposed administrative structure.

For now, we have limited our comments to the possible impact of the Proposal's site-blocking regime on telecommunications consumers. We ask that in considering whether and how to implement such a regime that the government consider the broader implications on Canada's net neutrality framework, including the effects on competition, innovation, consumer choice, access and affordability, privacy, and Canadians' right to freedom of expression.

*** End of Document ***