The Canadian Government's proposed approach to address harmful content online

GLOBAL PARTNERS DIGITAL

Global Partners Digital submission
September 2021

About Global Partners Digital

Global Partners Digital is a social purpose company dedicated to fostering a digital environment underpinned by human rights.

Introduction

We welcome the opportunity to provide comments on the Canadian government's proposed approach to address harmful content online through a new Act of Parliament. GPD recognises the legitimate desire of the government to tackle harmful content online, and many of the proposals put forward in the discussion guide and technical paper are reasonable and sensible. Based on our analysis, however, we believe that particular aspects of the proposal, if taken forward in their current form, may pose risks to individuals' right to freedom of expression and privacy online and could be inconsistent with Canada's international human rights obligations.

In this response, we relay our concerns and make a series of recommendations on how the proposal could be revised to mitigate these risks. We believe these considerations and recommendations, if incorporated into the upcoming legislation, will help safeguard freedom of expression and privacy online.

Framework for analysis of the proposed approach

Our analysis of the government's proposed approach is based on international human rights law, specifically the International Covenant on Civil and Political Rights (ICCPR), ratified by Canada in 1976. Article 19 of the ICCPR guarantees the right to freedom of expression, including the right to receive and impart information and ideas of all kinds regardless of frontiers. Article 17 of the ICCPR guarantees the right to privacy and provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". Restrictions on the right to freedom of expression or privacy guaranteed under international human rights law are only permissible when they can be justified. In order to be justified, restrictions must meet a three-part test, namely that: (1) restrictions are provided by law; (2) restrictions pursue a legitimate aim; and (3) restrictions must be necessary and proportionate, which requires that the restriction be the least restrictive means required to achieve the purported aim.

It is important to remember that Canada's obligation to ensure that these rights are not unjustifiably restricted exists both in relation to restrictions which stem from the actions of the state itself as well as those caused by third parties, such as private companies. As such, it makes no difference from the perspective of the individual affected whether any restrictions are imposed and enforced directly by the state (e.g. through creating criminal offences which are enforced by the police and the courts) or through third parties, particularly when the third party is acting in order to comply with legal obligations.

Human rights analysis of the proposed approach

Scope of Entities

We are concerned about the scope of entities included under the proposed framework. The technical paper sets out that new rules and obligations would apply to all Online Communication Service Providers (OCSPs), and defines Online Communication Services (OCSs) as "a service that is accessible to persons in Canada, the primary purpose of which is to enable users of the service to communicate with other users of the service, over the internet". While this would exclude some online services, the proposal would still include a broad range of entities, of all sizes, without providing a clear list of determining or limiting factors. Notwithstanding the current definitions and exemptions, we recommend that the government be required to consider a range of criteria and use these to designate entities on this basis *before* they would become subject to any regulatory requirements.

This would ensure the scope of entities subject to the regulatory requirements would be more proportionate. Were all entities falling within the definition of OCSPs to be bound by those requirements, this would not constitute a narrowly tailored and proportionate response, and would place an unreasonable regulatory burden upon smaller entities. We are concerned that higher regulatory burdens will reduce competition in the market, and power may be further concentrated on a smaller group of large online platforms. This would lead to fewer places for individuals to express themselves online and ultimately affect freedom of expression in the aggregate.

We therefore recommend that the proposal include certain factors which the government would be required to consider when making determinations on entities within scope. This should include the varying size (based on the number of users and resources) and nature of services, and include only those where there is compelling evidence or rationale necessitating their inclusion. While the language in the proposal requiring the government to consider whether there is "a significant risk that harmful content is being communicated on a particular entity" (albeit only in relation to further inclusions or exclusions of services) meets this standard in part, we recommend that it be further developed in line with the above, and also to include explicit consideration of users' rights to freedom of expression and privacy.

This would bring the proposal in line with the approach taken by other states. For example, Ireland's Online Safety & Media Regulation Bill provides that online services within scope will be designated by a newly created Media Commission. The Bill Includes explicit exemptions for certain types of services, and requires the Commission to have regard to the nature and scale of services, and the fundamental rights of users and operators, among other factors, when making designations. It would also provide services with the ability to appeal designations in court. These provisions would serve as a substantive check against inappropriate designations and reflect a proportionate and clear risk-based approach.

While we recognise - and welcome - the fact that the Digital Safety Commissioner would be authorised to tailor regulatory requirements to different categories of OCSPs, and that this would take into account different business models, sizes and resources, it is not clear how much discretion there will be tailor requirements given that many of those set out in the proposal are quite prescriptive. In addition to the Digital Safety Commission being able to tailor requirements, we believe that consideration of whether any regulatory requirements should be imposed at all is also necessary and that this should be undertaken when designating categories or OCSPs as bound by the legislation in the first place.

Recommendation 1: We recommend that the government be required to consider a range of criteria and to use these to designate entities on this basis *before* they would become subject to any regulatory requirements.

Recommendation 2: We recommend these criteria include consideration of the varying size of entities (based on the number of users and resources) and nature of services, and include only those where there is compelling evidence or rationale necessitating their inclusion. We further recommend that these criteria include a specific requirement to consider users' rights to freedom of expression and privacy.

The process for excluding or including new categories of services is also troubling as it provides the government with the ability to expand the scope of entities without sufficient parliamentary oversight. The proposal simply requires the Governor in Council to consult with the Digital Safety Commissioner and be "satisfied that there is a significant risk that harmful content is being communicated on the category of services or that specifying the category of services would further the objectives of this Act". We recommend that the proposal provide that the inclusion of new categories of services be subject to parliamentary approval, in the form of primary legislation.

Recommendation 3: The proposal should require that any changes to the types of entities within scope be done via primary legislation, as opposed to secondary legislation produced by the Governor in Council.

Private Communications Services

We are pleased that the proposal includes an exemption for services "that enable persons to engage only in private communications". However, we are concerned that this exception could ultimately include certain channels which should be considered private without additional clarification on what exactly constitutes "private communications". For example, it is not clear whether it covers large chat groups, forwarded or widely shared communications, or services with multiple functions including private communications.

The potential inclusion of private communications services is particularly concerning since many such channels use end-to-end encryption, limiting (although not eliminating) the ability of those who provide such services to filter or monitor content which is generated or shared using them. The application of any such requirements would be unfeasible unless those channels ceased to use end-to-end encryption, which would amount to an unjustifiable restriction on the right to privacy and freedom of expression.

We therefore suggest that the proposal includes additional references to individuals' right to communicate privately, including on encrypted services. Private communications services should continue to remain entirely outside the regulatory framework, and there should be additional clarification on what exactly constitutes "private communications".

Recommendation 4: The proposal should include additional references to individuals' right to communicate privately, including on encrypted services. Private communications services should continue to remain entirely outside the regulatory framework, and there should be additional clarification on what exactly constitutes "private communications".

New Rules and Obligations

We are concerned about the approach taken under the proposal, which would require that all OCSPs abide by a broad range of new rules and obligations with little clarity on how much discretion the Digital Safety Commissioner would have to tailor requirements for different categories of OCSPs. While we are pleased that some obligations, such as those on establishing appeals mechanisms and transparency requirements, would apply to all entities, compliance with some of the obligations included under the proposal would require even the most well-resourced entities to take actions which pose risks to human rights.

- **24 Hour Determinations**

We are particularly concerned that the proposal would require entities in scope to make a determination on the legality of content within 24 hours of the content being flagged, and to then remove the content if deemed to be illegal. While we recognise that entities within scope would have the ability to decide to keep the content up, it is important to remember the context in which this legislation is being adopted, namely a concern of the government that not enough harmful content is being removed. While the letter of the law may not pressure entities to remove more content, broader political and public pressure may do so, creating risks to individuals' right to freedom of expression due to the incentive for entities to err on the side of caution or "play it safe" and remove legal content in questionable situations.

Even entities that are making their best efforts to comply with this obligation and are able to withstand any external pressure may nonetheless, due to the strict time constraints, make decisions on a rushed basis without being informed by adequate expertise. This could lead to both over-removal and under-removal, with over-removal constituting an interference with the right to freedom of expression. Moreover, this type of obligation places a potentially large financial and logistical burden on entities who are responsible for making legal determinations without sufficient expertise, and we reiterate the concerns expressed above in relation to further concentration of the market.

Recent efforts at online platform regulation have tended to promote the privatisation of law enforcement, which, as noted above, pose heightened risks for freedom of expression when content is not clearly defined, or when removals are mandated under strict timelines. We therefore recommend that this obligation be amended, and that the proposal not require online platforms to make determinations on the legality of content, and certainly not within a strict 24 hour time period. Such decisions should instead be made by public authorities with sufficient safeguards and accountability.

The risks of this approach is clearly exemplified by Germany's Network Enforcement Act (NetzDG), which requires social media networks with over two million users to establish user complaint mechanisms and remove or block access to "manifestly illegal" content within 24 hours of receiving a complaint. All other illegal content must be taken down within seven days. This law has been criticised for outsourcing legal adjudications to private entities and the over removal of permissible content.[1] Even the world's largest online platforms, such as Facebook, struggle to comply with this law. Facebook's July 2021 NetzDG Transparency Report demonstrates that, of all the reports in the first half of 2021 that led to a block or deletion, the company was unable to make a decision within 24 hours for several thousand cases, despite the fact that Facebook

[1] Human Rights Watch, "Germany: Flawed Social Media Law - NetzDG is Wrong Response to Online Abuse", (2018), available at: https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law

employs 129 individuals to process NetzDG reports.[2] As the government's proposal currently sets out an even more restrictive time period (24 hours for all five types of content) it is unlikely that even the largest online platforms will be able to comply with this obligation in a way which does not present heightened risks for freedom of expression. Other proposals, such as the UK's Draft Online Safety Bill, take a tiered approach to imposing obligations, and do not provide a specific time period for the removal of illegal content.

Ideally, there would be no requirement to make determinations and take action within the proposed 24 hour time period. However, if entities are still required to make such determinations, we recommend that the proposal be amended to provide both large and small entities with a more flexible time frame when they are unable to comply with the 24 hour requirement. They should also be able to seek assistance from the government if they are unable to develop the necessary internal structures to be able to comply without posing risks to individuals' right to freedom of expression online.

Recommendation 5: The proposal should be amended to remove the requirement that entities make determinations within 24 hours and remove content identified as illegal. If the proposal is to include these obligations, it should, at minimum, provide entities with a more flexible time period to make determinations, and enable entities to seek assistance from the government if they are unable to develop the necessary internal structures to be able to comply without posing risks to individuals' right to freedom of expression online.

The proposal should also explore means of balancing the risks of over removal associated with time-sensitive takedowns. For example, a study exploring the optimisation of takedown and appeals processes related to content governance decisions recommends the introduction of an "Alternative Dispute Resolution Panel", in which a platform must compensate the user and cover the costs of the appeals process in the case of wrongful takedown and thus is incentivised to reduce the prevalence of over-blocking.[3] The proposal should also take into account the existence of additional and pre-emptive means of addressing the proliferation of harmful content online as well as removal; for example, Moonshot's research on potential interventions for 'incel' content in Canada indicates that re-directing offending users to helplines and support services, safeguarding algorithm designs to ensure that harmful content is not promoted in the feeds of vulnerable or impressionable users, and adequate prevention funding can reduce the incidence of incel-related hate speech and incitement to violence online.[4] These pre-emptive approaches avoid forcing offending users to migrate to smaller, less well-regulated platforms to spread the same content after it is removed or they are de-platformed elsewhere. Rather than focus solely on content removal, the proposal should include a broader range of provisions for the de-prioritisation and prevention of harmful content beyond simply removing it *ex post*,[5] encouraging OCSPs to develop systems and processes which will tackle the issue in a more nuanced and rights-respecting manner.

---

[2] Facebook, NetzDG Transparency Report (July 2021), available at: https://about.fb.com/de/wp-content/uploads/sites/10/2021/07/Facebook-NetzDG-Transparency-Report-July-2021.pdf

[3] Lenka Fiala and Martin Husovec, "Using Experimental Evidence to Design Optimal Notice and Takedown Process", (2018) Connecticut Law Review 50(2), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3218286

[4] Moonshot, Understanding and Preventing Incel Violence in Canada, (2021) available at: https://moonshotteam.com/preventing-incel-violence-in-canada/

[5] Evelyn Douek, "Facebook's Oversight Board; Move Fast with Stable Infrastructure and Humility", (2019) North Carolina Journal of law & Technology 21(2), pp. 42-43, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3365358

Recommendation 6: We recommend that the proposal include alternative means of addressing the proliferation and removal of harmful content online without resorting to the private adjudication of law enforcement and mandating that online platforms make determinations on the legality of content. Alternative approaches should emphasise the role of de-prioritisation and intervention as effective means of addressing the spread of illegal content online in a more proportionate fashion.

- **Automated Processes**

We are concerned that the proposal would require entities within scope to monitor for the five categories of harmful content on their services, including through the use of automated systems based on algorithms. Given the scale of content which is generated and shared online, entities will increasingly turn to automated processes, including AI, to meet their obligations. Larger platforms tend to develop their own bespoke tools with state of the art AI research, whereas smaller platforms may have to purchase or license generic tools for adaptation to their platform. However, the risk of encouraging or mandating the use of AI is that automated processes will detect and remove content that is not actually unlawful or harmful in a particular context.

Automated processes have had some success in relation to content moderation with types of images, including the ability to scan for copies of images that have already been identified by humans as constituting child sexual abuse and exploitation. But automated processing has been less effective at interpreting speech or less specific forms of unlawful or harmful content. For example, hate speech, incitement to violence and terrorist content may be a mixture of audio, visual and text content, and may be shared for a variety of reasons (including for journalistic or research purposes). Automated processes for their detection thus rely on a combination of natural language processing, image recognition and contextual knowledge-mapping for detection, technologies which, at present, are somewhat limited; for example, most natural language processing applications have about 80% accuracy even in their trained domain where relevant contextual knowledge is built in.[6] These automated technologies struggle with novel content and novel domains and with inferring users' intentions through context; for example, blacklisting particular words associated with hate speech results in the erroneous removal of commentary, testimony and satire. There is, therefore, a substantial risk that relying upon automated processes for all five forms of content will result in the removal of content which is entirely permissible due to algorithmic error.

We are also concerned that this obligation will result in discriminatory implementation, posing risks to individuals' right to non-discrimination. The proposal does provide that entities in scope must take measures to ensure that "the implementation and operation of the procedures, practices, rules and systems, including any automated decision making ... do not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act and in accordance with regulations".

However, algorithmic bias is well documented, due either to the availability of particular types of data for training the algorithm, the types of value judgements used to tag that data for training, or the biases and blind spots of those developing and testing the tool. Using automated tools inevitably results in over-censorship and/or unequal protection against online abuse of particular communities; for example, hate speech classifiers trained on widely used datasets of

[6] See, for example, Center for Democracy & Technology, "Mixed Messages? The Limits of Automated Social Media Content Analysis", (November 2017), available at: https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/

hate speech were shown to be up to two times more likely to label tweets by African-American as offensive compared to other users.[7]

We therefore recommend that the proposal exclude any obligations which require or encourage entities to use automated processes to proactively monitor and remove content. The proposal should specify that, if the OCSP implements automated decision-making to meet obligations, it must ensure the use of open source tools, transparency around standards, and appropriate appeals mechanisms. Beyond these, we believe the proposal might be strengthened by reference to the sorts of safeguards that entities must implement if they choose to build or use automated tools for content flagging, such as the building in of human moderator oversight, the transparent publication of the accuracy metrics of the tools employed, and the careful evaluation of accuracy scores against the human rights risks of particular errors through expert consultation and testing prior to roll out. The proposal could be further improved by requiring robust impact assessments of AI tools - specifically with regard to bias - to assess whether entities' use of automated processes results in, or could result in, differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act or under Article 26 of the International Covenant on Civil and Political Rights.

Recommendation 7: The proposal should include explicit recognition of Canada's obligation to uphold the right to non-discrimination under international human rights law, in addition to further guarantees of this right under the domestic legal framework.

Recommendation 8: The proposal should not compel or incentivise the use of automated processes to proactively monitor and remove harmful content, which has been proven to result in the removal of lawful and legitimate content online. If automated processes, such as those used for content flagging, are undertaken by entities to comply with obligations, these automated tools must be rigorously tested prior to roll-out through expert consultation and trials, must be accompanied by human oversight and adequate appeals mechanisms, and be regularly assessed for their impacts on users' human rights.

Recommendation 9: We recommend the proposal require robust impact assessments of AI tools - specifically with regard to bias - to assess whether entities use of automated processes does not result in differential treatment of any group based on a prohibited ground of discrimination within the meaning of the Canadian Human Rights Act or under Article 26 of the International Covenant on Civil and Political Rights.

- **Reporting and Preservation Obligations**

We are especially concerned that the proposal would require entities in scope to either: (1) notify the Royal Canadian Mounted Police (RCMP) in circumstances where the OCSP has reasonable grounds to suspect that content falling within the five categories of regulated harmful content reflects an imminent risk of serious harm to any person or to property; or (2) report prescribed information in respect of prescribed criminal offences falling within the five categories of regulated harmful content to prescribed law enforcement officers or agencies. In addition, we are concerned that regulated entities would be required to preserve prescribed information that could support an investigation when sought by lawful means.

[7] Maarten Sap & Al, "The Risk of Racial Bias in Hate Speech Detection" Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics (2019), available at: https://homes.cs.washington.edu/~msap/pdfs/sap2019risk.pdf

This is because these requirements pose a significant risk to individuals' right to privacy and could have a chilling effect on freedom of expression, particularly for marginalised groups which are already subject to the discriminatory impacts of mass surveillance and policing.[8] The proposal would expand the legal and technical surveillance capabilities of the state using safety as a rhetoric, but fails to establish the necessity of such obligations for all forms of content and does not devise them in a proportionate manner. We understand the government's desire to include mechanisms for engaging law enforcement and the Canadian Security Intelligence Service (CSIS), but the approach of the proposal should ultimately be to hold platforms accountable in a way that mitigates risks to privacy and freedom of expression.

We therefore recommend that these reporting and preservation obligations be removed from the proposal unless the government is able to substantiate the necessity of these obligations for each type of content. If these obligations are still included for certain forms of content, such as for child sexual exploitation content or terrorist content, then the exact circumstances for the triggering of such activity must be clearly provided for in the proposal, and must ensure that content which is flagged as illegal by an automatic tool is reviewed by a human moderator before such a process takes place, given the potential for AI error. It must further provide limitations on the types of information required and clear safeguards should be put in place around the deletion of user data if the content in question is later deemed not to be illegal.

These concerns are supported by Google and its subsidiary Youtube's challenge to new obligations under Germany's NetzDG. New obligations under will require companies to proactively and automatically pass on user data to the Federal Criminal Police Office (BKA) if platforms assume a violation of certain criminal offenses. But Google maintains that these obligations constitute a massive interference with users privacy as only 60% of the content that would be mandatorily passed on to law enforcement would contain any criminal content, resulting in the data of innocent users being permanently stored in police databases.[9]

Recommendation 10: The proposal should exclude reporting and preservation requirements unless they are able to establish the necessity of such obligations for all forms of content and devise them in a proportionate manner.

Recommendation 11: If reporting and preservations obligations are still included for certain forms of content, then the exact circumstances for the triggering of such activity must be clearly provided for in the proposal. It must further provide limitations on the types of information required and clear safeguards for the deletion of user data when content in question is later deemed not to be illegal.

Establishment of New Regulators

We are pleased that the proposal envisions the establishment of new regulators whose functions relate, in part, to the protection of human rights. For example, the technical paper notes that the Digital Safety Commissioner would oversee and improve online content moderation through engagement and by considering "the needs of and barriers faced by groups disproportionately affected by harmful online content such as women and girls, Indigenous Peoples, members of

[8] Cynthia Khoo, "Deplatforming Misogyny: Report on Platform Liability for Technology-Facilitated Gender-Based Violence" LEAF (2021), pp. 206-208, available at: https://www.leaf.ca/wp-content/uploads/2021/04/Full-Report-Deplatforming-Misogyny.pdf

[9] Sabine Frank, "On the Extended Network Enforcement Law in Germany - Comments from Youtube", YouTube Official Blog (July 2021), available at: https://blog.youtube/intl/de-de/news-and-events/zum-erweiterten-netzwerkdurchsetzungsgesetz-deutschland/

racialized communities and religious minorities and of LGBTQ2 and gender-diverse communities and persons with disabilities". It also states that the Digital Safety Commission, Digital Safety Commissioner, and Digital Recourse Council would all be subject to the Access to Information Act and the Privacy Act.

However, we are concerned that the proposal lacks a clear human rights mandate for its regulators. The technical paper fails to directly reference the right to freedom of expression under both domestic and international human rights law. We believe the inclusion of these protections and explicit acknowledgement of Canada's obligations under international human rights law to be critical here given the potential negative impacts on freedom of expression and privacy posed by the proposal. We recommend that the proposal be amended to explicitly reference Canada's obligation to uphold the right to freedom of expression and privacy as enshrined under Articles 19 and 17 of the International Covenant on Civil and Political Rights, which would ensure that protecting and respecting the rights to freedom of expression and privacy is one of the regulator's statutory duties.

Recommendation 12: We recommend that the proposal be amended to explicitly reference Canada's obligation to uphold the right to freedom of expression and privacy under Articles 19 and 17 of the International Covenant on Civil and Political Rights, which would ensure that protecting and respecting the rights to freedom of expression and privacy is one of the regulator's statutory duties.

It is equally important that the new regulators have a dedicated staff with sufficient knowledge and human rights expertise to effectively meet the proposed functions. The Digital Recourse Council will need to make informed decisions that could potentially encroach or infringe upon freedom of expression, particularly when issuing orders to OCSPs to make content inaccessible in Canada. We recommend that these decisions, as with those made by the Digital Safety Commissioner, be made according to clear criteria that require a consideration of freedom of expression.

Recommendation 13: We recommend that the proposal include a requirement for the new regulators to have a dedicated staff with sufficient knowledge and human rights expertise to meet the proposed functions, and to seek external advice when necessary to carry out their respective functions. We further recommend that the proposal require the Digital Safety Commissioner and Digital Recourse Council to make decisions according to clear criteria which includes the consideration of the impacts on freedom of expression.

Regulatory Powers & Enforcement

We are particularly concerned about the sweeping regulatory and enforcement powers that would be provided to the new regulators under the proposal. For example, the technical paper states that the Digital Safety Commissioner may, by order, require an OCSP to do any act or thing, or refrain from doing anything necessary to ensure compliance with any obligations imposed on the OCSP. The technical paper includes further investigatory powers for the Digital Safety Commissioner to conduct inspections of OCSPs at any time. The Commissioner would also be able to apply to Federal Court for an order requiring Telecommunications Service Providers to block access to services which consistently fail to apply to removal orders for child sexual exploitation content or terrorist content.

Given the broad powers envisioned under the proposal, we stress the need for effective oversight, transparency and readily accessible appeals mechanisms for services to challenge decisions of the new regulators. We understand that the new regulators must have sufficient inspection and

enforcement powers to effectively carry out its functions, but are nonetheless concerned that there are limited safeguards for the exercise of these powers. We welcome those elements of the technical paper which do provide for some degree of oversight, such as the fact that compliance orders may be appealed to the Personal Information and Data Protection Tribunal, but believe that these safeguards should go further.

We recommend the inspection powers of the Digital Safety Commissioner be limited in scope and subject to procedural safeguards, enabling entities to challenge the use of these inspection powers when undertaken for illegitimate purposes or when utilised in a disproportionate manner. We further recommend that any regulations concerning the Commissioner's ability to seek orders for the blocking of services list specific criteria and thresholds for the Commissioner to consider, including a requirement that the Commissioner consider the risks to freedom of expression before applying to the Federal Court. We welcome that the technical paper would require the Commissioner to consider the level of non-compliance and potential effects of the order, such as excessive blocking, when seeking an order. However, we believe that a more specific consideration of the human rights impacts would be preferable and ensure a more proportionate approach and limit risks to freedom of expression.

Recommendation 14: We recommend that the inspection powers of the Digital Safety Commissioner be limited in scope and subject to procedural safeguards, enabling entities to challenge the use of inspection powers.

Recommendation 15: We recommend that any regulations concerning the Commissioner's ability to seek orders for the blocking of services list specific criteria or thresholds for the Commissioner to consider before applying to the Federal Court for a blocking order. This should include a clear requirement of the Commissioner to consider the risks to freedom of expression.