96 Mowat Avenue
Toronto, Ontario, Canada M6K 3M1

Tucows' response to the Government proposed approach to regulating social media and combating harmful content online

24 September, 2021

The ongoing Covid-19 pandemic has thrown into stark relief how important it is that Canadians have full and equitable access to the free and open Internet. With the sudden and urgent necessity to avoid in-person interaction, Canadians have turned to the Internet to do business, attend school, and socialize with other people in Canada and around the world. While addressing a true need, this broad turn towards online interactions has of course also led to an increase in exposure to harmful content online. **We need standards, we need to enable safe and secure access to information and to community, and we need to protect Canadian Internet users in a fair and balanced way.** We appreciate that the Government of Canada is working to address these needs.

Here at Tucows, **we believe in the free and open Internet**, allowing Canadians to share opinions and artwork, meet people from all around the world, and live our lives in the digital realm just as we do in the physical world. With that goal in mind, it is crucial to **find the right balance** between freedom of expression and access to ideas on the one hand and protection against illegal and harmful content on the other.

Surveillance and limitations on Canadians' expression on the Internet is unacceptable; we as Canadians must be safe to express ourselves without fear of either government censorship or being harmed by the types of content this legislation attempts to address.

As a domain name services provider and a proudly Canadian company, Tucows, both as a business and as a community of coworkers, is a crucial part of the same Internet ecosystem that we all use every day. We are pleased to be able to share our expertise in this response to the Government's proposed approach to address harmful content online.

Lawmakers must not fall into the trap of making quick decisions and implementing half-formed or ill-informed plans that will have long-term effects on the rights and freedoms of Canadian citizens. When developing broad new legislation such as this, it's crucial that the Government **consider the input of experts in the industry who have already spent years working on combatting online harms and moderating content on online platforms.** To that end, we will raise our concerns with the proposed new legislation. The Government should do everything possible to gather input from Canadians, especially Canadians already working in this space, and incorporate those insights into revisions of this draft legislation.

Applicability

The legislation would apply to “Online Communication Service Providers” (OCSPs); the limitation to services that enable communication with other users of the same service is a good start but still leaves gaps such as personal websites or blogs—does a Wordpress blog with a vibrant community of commenters fall under this definition? A personal website with a message board? **The exemption for private communications is crucial and must be clear enough to preclude any surveillance of personal expression or private communications.**

The five categories of harmful content being addressed here (hate speech, child sexual abuse material (CSAM), non-consensual sharing of intimate images, incitement to violence, and terrorist content) are appropriate categories, as each one poses **imminent risk of harm to a person**, and are already prohibited under the Criminal Code.

We also support the OCSP reporting requirements relating to harmful content and particularly note “how they monetize harmful content” as a valuable metric to track and disclose.

Privacy Concerns

It is crucial to ensure that **Canadian citizens’ privacy rights are not only respected but are a fundamental part of any new legislation**, especially relating to online services where personal data is essentially currency and people are highly vulnerable to the theft of their data, their money, even their identity.

How will improper and excessive surveillance and storage of personal data be prevented, especially in the case of false positives, considering the known limits and biases of algorithmic content flagging?

Relatedly, the oversight for accessing Basic Subscriber Information (BSI) through a Production Order is unclear or lacking; who authorizes these orders? Who makes sure that there are valid grounds to access personal data in relation to a suspected incident? Proper checks and balances must be put in place to protect Canadian citizens as well as people from around the world. We will want the rights of Canadians to be protected worldwide, which speaks to a need to participate as a country in international dialogue on this important legislative initiative, to ensure reciprocity in the protection of fundamental rights.

24-hour Responses

The requirement for OCSPs to take action within 24 hours of a user report or algorithm flag will absolutely lead to errors.

24 hours is not sufficient time to review reports, so OCSPs will either over-respond by taking down content that does not fall within the five categories of online harms, or they will

dismiss reports too quickly and miss actual harmful content in the frenzy. Which way it goes will depend on both the strength of the penalties for not taking down harmful content and the capacity of the individual OCSP to create a team dedicated to reviewing reports.

Regardless of the approach, **this short response timeframe burdens Canadian Internet users as well as those of us who are seeking to protect them**: either their content is taken down inappropriately and they must appeal the decision or their valid report is dismissed and the problematic content remains online, continuing to cause the very harm this legislation is attempting to prevent. Taking down content near-immediately upon complaint is not a thoughtful approach to this difficult dilemma, nor is it permissible under the Charter of Rights and Freedoms.

It also seems fairly arbitrary; **why 24 hours?** Where exactly did that number come from? Do our government and law enforcement agencies respond within 24 hours to similar types of reports, basing this on their real-life experience? No. When issues of this kind are reported, either by victims or by online service providers of all kinds, the RCMP takes days *at best* to respond, let alone prosecute the harms.

Scope of harms

The scope of content that falls into these broad categories is unclear and apparently not yet defined, as that will be included in the full legislation; this should be open to the Canadian public to comment on. **The Internet community has been working on the issue of online harms and abuse of the domain name system for years, and is still deep in the process of defining abuse; have the drafters of this legislation considered the work of those experts at all?** And, have the response timeframes in place in those industries been considered when setting this 24 hour response time?

Free expression

How will issues of freedom of expression be addressed? Facebook already takes down breastfeeding pictures and other acceptable content without oversight; this will expand to **people using the reporting system and fast takedown requirements to silence voices they disagree with**, including anti-choice people brigading health care forums. Imagine a woman posting a story of sexual assault to raise awareness and reclaim her story, only to find it taken down due to ill-meaning people reporting it as hate speech. The writer can submit an appeal, but it's adding insult to injury.

Use of Algorithms

Meaningful human review is crucial in this situation, as in other areas relating to content moderation and the response to online harms. Algorithms are imperfect, proven to perpetuate the biases of their creators and datasets, and false positives abound, resulting in the **uneven application of legal penalties to the communities this legislation purports specifically to protect.** Algorithmic content moderation, especially in relation to false positives in content moderation, is the topic of a great deal of research and many popular articles. To ignore this issue is to **willfully subject Canadian citizens to unequal treatment under the law**. Algorithms may be used to flag content for further human review but **must not be the sole arbitrator of what is permissible content on the Internet.**

Fragmentation of the Internet

Banning content in Canada that is still available in other countries will cause fragmentation of the Internet. Authoritarian governments have shown that controlling "their" internet and what their citizens can view only moves the content—users who still want to access "banned" content can easily use a VPN, for example, to appear to be in a different jurisdiction. This also means that **those harmed by the content**—the victim, for example, of non-consensually-shared intimate photos, **can no longer view (and report) the content while the harm to them continues unabated.**

The limits on the requirement for ISPs to block Canadian access to certain content must be strong and clear. The underlying concept here is appropriate; CSAM and terrorist content is illegal and those laws must be enforced. That said, the definition especially of "terrorist content" has not been shared, and leaves open significant concerns of government overreach. As a domain registrar we have been called on to remove allegedly terrorism-related content from our platform, and in some cases the website in question has in fact been a journalism site (rather than one supporting the terrorist content), while in other cases it has posed as true journalism in order to spread messages of hate. **The difficulty is in determining whether the content is in fact illegal and it's essential to this process that proper oversight exists.** We work with Tech Against Terrorism to verify reports of terrorism-related content; are OCSPs now left on their own to make these determinations?

We receive many complaints every day from lawyers and other Internet users asking for full websites to be taken down when the issue is a mention of an individual, a single photo, or a single page on a larger website. **How will the requirement to block Canadian access to content accommodate the fact that blocking by ISP may only occur at the IP or domain name level and cannot be as granular as free speech requires?** Any prospective legislation will have to be much more precise about how an OCSP can order a customer to excise the offensive content or face takedown, otherwise we are trying to hit a fly with a sledgehammer.

Enforcement capability is also in question, as users can bypass an ISP's blocklists by using a VPN or DNS-over-HTTPS functionality, masking their traffic. How will the legislation address this gap, without overreach? What exactly are Canadian Internet businesses being asked to do?

Commissioner powers and funding

It is both unfortunate and well known that the Canadian Office of the Privacy Commissioner lacks the power to levy fines or even effectively require organizations to change their behaviour; last year, Facebook ignored the findings of the OPC's investigation. How will the creation of this new Digital Safety Commissioner of Canada avoid the same problems? **Why do the legislators expect that the new Commissioner's fines or other findings will be respected, when the existing ones are not?**

We question the expectation that the operating budgets for the Commissioner and Recourse Council will be funded by OCSP "regulatory charges"; this is essentially **a tax on some (but not all) online service providers. Costs will of course be passed on to Canadian Internet users,** either in the form of payment for services or increased advertising on the platforms. On top of these costs for oversight bodies, we will already have incurred substantial costs dealing with all of the issues described above, including an expected increase in volume.

What is the expectation for OCSPs that decline to pay these costs? Currently, administrative penalties recommended by the OPC are often ignored and with no clear consequences.

Engaging LEA and CSIS

Regarding the requirement for OCSPs to notify law enforcement and the Canadian Security Intelligence Service in some circumstances, **we would support the 'imminent risk of human harm' limitation** (the first of the two options presented), requiring those entities to notify law enforcement only when imminent harm is suspected.

Extending this risk of serious harm to property (instead of only to people) is a *huge* concern. There needs to be further consultation with Canadians in this area (as with much of the rest of this proposed legislation), because people are not property and harm to property or to property rights should never receive the same high level of protection as imminent harm to people must.

We are also **concerned about privacy rights and surveillance in relation to this notification requirement**, as discussed earlier.

Recourse and appeals

Access to recourse is unequal; a Canadian (or anyone living in Canada? It's unclear!) whose content is removed under this new law can appeal to the platform itself and then to the Digital Recourse Council, but users from the rest of the world appear to have no such recourse. What happens if *their* content is removed due to a false positive flag or report? Under this proposed legislation, the platform could refuse to consider any appeal. The Digital Recourse Council may require a platform to return the Canadian user's content, but users from elsewhere would effectively be silenced from participation in Canadian online discourse, **limiting the perspectives available to Canadians. As discussed above, there is a need for international reciprocity; consultation and international agreements will be required.**

Timeframes for appeals must be clearly laid out so all parties—users, ISPs, and OCSPs alike—understand their options and requirements. Timeframes should be long enough to ensure that users have plenty of time to address content removals. **The Recourse Council will need to be prepared for a significant volume of appeals and must be held to the same response time that OCSPs are held to**—currently 24 hours**.**

Recommendations

With the above comments in mind, we offer the following recommendations. We look forward to reviewing future versions of this framework before it is passed into law, and are happy to assist by providing expertise and insights at every stage of the process.

The Government should:

1. **Launch a detailed consultation**, ensuring that those working on combatting online harms play a key part in assisting to modify this draft legislation
2. **Work with the Privacy Commissioner of Canada and the Provincial and Territorial Commissioners** to make the privacy rights of Canadian citizens a foundational element of this new legislation
3. **Balance the prevention of these five categories of harm against the Charter rights of Canadian citizens,** protecting our privacy and freedom of expression while preventing surveillance, limitations on free expression, and the use of algorithms to silence Canadian voices
4. **Address questions around funding** for this new Government department
5. **Prepare the Digital Recourse Council** for a significant volume of appeals and ensure they are able to respond within the same timeframe to which OCSPs are held

---

This comment was prepared by Sarah Wyld, with thanks to Jacinta Sandiford, Reg Levy, Graeme Bunton, and Stephanie Perrin for their input.