Internet Impact Brief

Canada's Proposed Online Harms Legislation and the Internet

Author:
Mark Buell, Internet Society
Contributor:
Joel Templeman, CD, MPA, Bed, Executive Director, Internet Society Manitoba Chapter

Version 1.0 (8 November 2021)

Abstract

In 2020, the Government of Canada announced it would be introducing legislation to combat online harms. In July 2021 the Department of Canadian Heritage released two consultation documents related to its development: a Technical Paper[1] and a Discussion Guide[2] to address harmful content online. However a federal election was called in August, ending the parliamentary session before the online harms bill had been introduced. The Liberal Party was re-elected in September 2021 and has since announced it will introduce the online harms bill early in the upcoming session of Parliament.

This report uses the Internet Impact Assessment Toolkit[3] (IIAT) to assess how the online harms bill may affect the global Internet by impacting what the Internet needs to thrive as an open, globally-connected, secure, and trustworthy resource for all.

Methodology

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). This includes: an accessible Infrastructure with a common protocol, a layered architecture of interoperable building blocks, decentralized management and distributed routing, a common global identifier system, and a technology neutral, general-purpose network.
To assess whether the present proposal has an impact on the Internet, this report will examine its impact on the IWN foundation the Internet needs to exist, and what it needs to thrive as an open, globally-connected, secure and trustworthy resource.

Context

Canada's proposed Online Harms legislation follows similar initiatives in other countries including Australia, Germany, and the United Kingdom in recent years. The general intent of these bills is to address perceived harmful content posted to the Internet, including

[1] https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a2d
[2] https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/discussion-guide.html#a4a
[3] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/ The IIAT was developed by the Internet Society[3] to be used by anyone who wants to check if a particular policy, development, or trend affects the critical properties of the Internet Way of Networking (IWN).

hate speech, terrorist content, child sexual exploitation, and the non-consensual sharing of intimate images.

In its Technical Paper and Discussion Guide, the Government of Canada outlines its proposed approach to regulating social media and combating harmful content online in an effort to create a "safe, inclusive and open online environment." The Discussion Guide identifies the five areas of harmful content that will be subject to regulation under the Act:

1. Child sexual exploitation content.
2. Content that actively encourages terrorism.
3. Content that actively encourages or threatens violence.
4. Hate speech as defined under the amended Canadian Human Rights Act.[4]
5. Non-consensual sharing of intimate images.

According to the Technical Paper, the Act will cover "online communications service providers" (OCSP), defined in the Technical Paper as "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."[5] Facebook, YouTube, TikTok, Instagram, Twitter, and Pornhub are listed as examples of OCSPs in the Discussion Guide. Platforms of all sizes and potential reach are included; there are no exceptions for smaller OCSPs. Services such as fitness applications and travel review websites will be excluded, as will private communications.

The Act will require the regulated entities to take all "reasonable measures to make harmful content inaccessible in Canada," including the use of automated systems and algorithms to identify potentially harmful content. Once content is deemed harmful, the OCSP will be required to filter the offending content, making it inaccessible in Canada expeditiously. The Technical Paper defines "expeditiously" to mean "twenty-four (24) hours from the content being flagged, or such other period of time as may be prescribed by the Governor in Council through regulations."[6]

The role of Digital Safety Commissioner (DSC) will be created, charged with overseeing, administering, and enforcing the new regulations. It will have the authority to levy fines of up to $10 million or three per cent of an offending OCSP entity's gross global revenue, whichever is greater. The Act also empowers the DSC to apply to the Federal Court for an order to require Internet Service Providers (ISPs) to block access[7] to an OCSP in Canada if the platform has demonstrated persistent non-compliance with a content filtering order(s).

[4] https://laws-lois.justice.gc.ca/eng/acts/h-6/page-1.html
[5] https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a2d
[6] https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a2d
[7] It is important to note that the approaches taken by Germany and the European Union do not include provisions for blocking websites. In Australia, blocking is only to be used in very limited circumstances and for limited time.

The Government of Canada's attempts to apply national laws to the Internet, which is essentially a global resource, could potentially put the very foundation of the Internet at risk. Of particular concern are provisions in the legislation that call for automated systems to identify harmful content, the requirements for content filtering and content blocking, as well as the extremely short time frame between the identification of harmful content and the need to make it inaccessible online. As proposed, the bill also raises privacy-related concerns.

How the Proposed Online Harms Bill Affects the Internet

In order to understand how the online harms bill could affect the Internet itself we assess how it might impact the Critical Properties of the Internet as described by the Internet Society[8].

Common Global Identifiers that are unambiguous and universal

Common global identifiers, particularly the Internet Protocol (IP)[9] addressing system and the Domain Name System (DNS)[10], deliver a consistent experience for Internet users. When these systems are fractured – including by network-blocking systems – networks rely on sub-optimal gateways, translators, and mapping tables to maintain the broken connections. Fractured namespaces create additional costs, overhead, friction and delays within the network, and reduce the security and reliability of consistent, authoritative addressing. Furthermore, when the critical property of functioning and consistent global identifier systems is damaged, the Internet ceases to be a global network and becomes a set of imperfectly interconnected, sub-optimal networks.

The Act will require Internet Service Providers (ISPs) to block access to OCSPs in certain circumstances. According to the Technical Paper, "The Act should provide the Digital Safety Commissioner with the authority to apply to the Federal Court for an order requiring relevant Telecommunications Service Providers, as defined in subsection 2(1) of the *Telecommunications Act*,[11] to block access in whole or in part to an offending OCS in Canada."[12] Blocking interferes with and damages the common distributed routing system the global Internet depends on, specifically by interfering with the operation of the IP addressing system and the DNS.

IP-based blocking works by inserting a device into the network to block IP addresses. DNS-blocking is done by funneling traffic to a modified and unauthoritative DNS server that blocks certain names. Both methods can lead to the situation where names and addresses do not resolve consistently, authoritatively, and dependably everywhere.

[8] https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/
[9] An IP address is the unique numerical identifier for a device on the Internet.
[10] The DNS is the system used to map alphabetic domain names, like internetsociety.org, to numeric Internet Protocol addresses.
[11] https://laws-lois.justice.gc.ca/eng/acts/t-3.4/FullText.html#h-459781
[12] https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a2d

Requiring ISPs to implement blocking regimes, will force them to impose additional requirements on routing policy and DNS management that conflict with the current goals of maximizing resilience, reducing costs, and optimizing traffic flows. This reduces their ability to optimize connectivity. Network-level blocking bans profoundly affect the ability of network operators to provide global reach and worldwide connectivity.

As proposed, the Online Harms bill has the potential to negatively impact the Internet's common global identifiers. The implementation of actions such as filtering and blocking signal a dangerous trend toward regulation that may have profound negative consequences for the Internet.

How Will the Proposed Online Harms Bill Affect the Realization of the Full Potential of the Internet?

The critical properties are what is needed to have the Internet, but they are not sufficient if we want the Internet to reach its full potential. To assess how this proposal might impact what we need for an Internet that is open, globally connected, secure, and trustworthy, we will look at it through the lens of the enablers of these goals.

Easy and Unrestricted Access

"It is easy to become part of the Internet, for networks and users alike. That means that for users the Internet is affordable and Internet services are accessible, and that networks can easily become part of the Internet, without unnecessary regulatory or commercial barriers for both groups."[13]

The Online Harms Act will require OCSPs to develop and use complex and costly tools such as automated systems to identify harmful content and content blockers. As noted above, the use of such tools is required for all OCSPs, regardless of their size or reach. By requiring the use of these tools, the Act essentially puts barriers in place for new entrants to the market.

Large OCSPs, like the ones identified in the Discussion Guide, have the resources to comply with the regulatory requirements, whereas new players, including innovative Canadian start-ups, may not. The Online Harms Act therefore places limitations on Internet access for new digital businesses, damaging the Internet's potential as an open resource and limiting the ability of innovative Canadian companies to compete in the market.

[13] https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

Unrestricted Reachability

"Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves. Once a resource has been made available in some way by its owner, there is no blocking of legitimate use and access to that resource by third parties."[14]

IP-based blocking places barriers in the network, such as firewalls, that block all traffic to a set of IP addresses. A variation on IP blocking is throttling, where a portion of traffic to an IP-number is blocked, making access slow and unreliable to discourage users. Blocking whole ranges of IP numbers over-blocks wide swathes of the Internet, prohibiting access to many more than the intended sites or services. Over-blocking using the DNS causes similar collateral damage when an entire website is blocked in order to cut access to specific pages or types of content on it.

These practices fragment the global identifier systems and damage the critical property that makes the Internet consistently accessible and authoritative. Internet users in Canada may find their content censored illegitimately, limiting their ability to communicate with others and diminishing the globally connected nature of the Internet.

While performing a DNS lookup, the DNS resolver also checks the requested name against a block list. If the requested name is on a block list, the resolver will return incorrect information (such as a page indicating that content has been blocked) or will declare that the name does not exist. Ultimately, the end user will be unable to reach the content they wish to access when using certain domain names. Essentially, content blocking profoundly impacts the ability of network operators to ensure global reach for the Internet, limiting the Internet's potential as a trustworthy resource.

Data Confidentiality of Information, Devices, and Applications

"Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. Allowing the transfer of sensitive information helps create a secure Internet. Data confidentiality also extends to data-at-rest in applications and on devices. (N.B., "confidentiality" also contributes to privacy, which is part of a trustworthy Internet)."[15]

Content blocking requires that Internet traffic be examined to determine its content. Even some encrypted traffic – that which is not end-to-end encrypted – can be examined using proxies, violating the ability of users to perform end-to-end encryption. Users encrypt sensitive information to protect their personal information, to safeguard financial information, and to protect themselves from attackers. By "baking in" surveillance by requiring backdoors such as proxies, users are put at risk, their messages are at risk of being modified by unwanted third parties, and trust in the Internet is eroded.

[14] Ibid.
[15] Ibid.

Integrity of Information, Applications, and Services

"The integrity of data sent over the Internet, and stored in applications, is not compromised. That is, information sent over the Internet shouldn't be modified in transit, unless directed by the communicating parties (e.g., a captioning bot may be useful to turn spoken words into text). Critical underlying Internet services, such as DNS and the routing system, cannot be manipulated or compromised by malicious actors. Data stored in applications cannot be manipulated or compromised by third parties."[16]

DNS-blocking carried out by ISPs to prevent access to certain OCSPs could also compromise security as it is effectively incompatible with DNS Security Extensions (DNSSEC)[17]. DNSSEC is a set of standards that have been developed to prevent malicious acts like DNS hijacking and domain name spoofing. It is designed to prevent DNS responses from being altered.

When service providers interfere with the functions of the DNS by redirecting the request or returning incorrect information about the site's existence, it essentially legitimizes the acts (that is, tampering with a DNS response) that DNSSEC was created to address. A DNSSEC-enabled browser or application cannot distinguish between a site that has been blocked or redirected because of a court order from one that truly presents a security threat. To succeed with the approach, DNSSEC must be effectively disabled which negatively affects the integrity of the naming system and may have adverse effects on the uptake of DNSSEC worldwide. The result will be a less secure Internet.

Accountability

"Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions."[18]

The definition of "harmful" is subjective. Who decides what is harmful and what is not harmful matters and may have implications for freedom of expression in Canada. Once harmful is defined, the use of automated systems to identify it online will be problematic. Automated systems cannot determine the difference between educational, satirical, and journalistic content from content that is in fact illegal and/or harmful. The incredibly short window for OCSPs to identify and block content once it is determined to be 'harmful' or otherwise face stiff monetary penalties coupled with the use of such automated systems greatly increase the likelihood of "false positives" resulting in legal and legitimate content being made inaccessible in Canada.

[16] Ibid.
[17] For more information about DNSSEC, see: https://www.internetsociety.org/deploy360/dnssec/
[18] https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

Privacy

"Privacy on the Internet is the ability of individuals and groups to be able to understand and control what information about them is being collected and how, and to control how this is used and shared. Privacy often includes aspects of anonymity, removing linkages between data, devices, and communications sessions and the identities of the people to which they pertain."[19]

As proposed, the Online Harms Act will require OCSPs to report information about people who have content that has been flagged as illegal to law enforcement agencies. OCSPs will also be required to "preserve data and information in their possession or control pertinent to (1) reports provided to law enforcement or notifications provided to the RCMP under part [E] and (2) potentially illegal content falling within the five (5) categories of regulated harmful content."[20] As discussed above, the Act may result in content being falsely identified as harmful, increasing the potential for innocent people to have their private information shared with authorities.

Summary

The Online Harms Act may have implications for several of the characteristics that enable the open, globally-connected, secure, and trustworthy Internet to thrive. Content blocking will restrict access to content and services online, and by interfering with the operations of the DNS, end user safety and security will be put at risk. Automated systems to identify illegal content will result in false positives. The privacy of end users will be jeopardized.

Summary & Conclusions

This report is limited in scope to the development and operations of the Internet as a global resource. However, numerous organizations and individuals, including the Internet Society Canada Chapter, CitizenLab, OpenMedia, Professor Michael Geist, and many others have expressed serious concerns related to the bill. Their concerns range from the inadequate public consultation on the proposed Act to legitimate concerns related to freedom of speech.

Furthermore, the bill could essentially result in the application of domestic Canadian law to the Internet, a global resource. The Internet Society Canada Chapter state in their submission to the consultation:

> "In short, the Proposal would have Canadian law apply to entities that have no connection to Canada, to speech that has no connection to Canada, and impose remedies for harmful speech for which there is no evidence of harm in Canada. No consideration appears in the Proposal to conflicts between Canadian and foreign domestic law, or what the

[19] Ibid.
[20] https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a2d

> implications to Canadians might be if foreign governments were to adopt regimes that assumed a similar universal jurisdiction approach."[21]

It is important to note that the types of harmful content that will be subject to regulation under the Act are already crimes in Canada with due processes associated. That these laws are limited or ineffective is not the fault of the medium, in this case the Internet. Instead of targeting the Internet, the Government of Canada should focus their efforts on strengthening the enforcement of these laws and prosecuting convicted offenders of these acts within existing legal and constitutional mechanisms, regardless of if it occurs online or in real life.

The potential benefits of extreme measure like those included in the Act must be weighed against their very real negative effects. In the case of the Online Harms Bill, those benefits will not result in a net good for Canadians, the Canadian economy, nor the Internet as a whole.

[21] https://internetsociety.ca/wp-content/uploads/2021/09/ISCC-Response-Online-Harms-Final-21-9-21-1.pdf