How Bill S-210 Puts Canadians' Security and Privacy at Risk by Harming the Internet

22 May 2024

A submission by the Internet Society to the Standing Committee on Public Safety and National Security Re: Bill S-210—An Act to restrict young persons' online access to sexually explicit material.

Executive Summary

Although well-intentioned, S-210, *an Act to restrict young persons' online access to sexually explicit material*, includes requirements that could disrupt essential functions of the Internet and ultimately harm Canadians' security and privacy. The introduction of age verification requirements and increased liability for Internet intermediaries, not just providers of adult content, would create an untenable situation. Internet service providers, whose primary role is to facilitate online traffic, would be forced to make difficult decisions about allowing secure traffic and facing potential liability, or rejecting secure traffic and cutting off Canadian users from the benefits of the global Internet.

In order to ensure that the Internet continues to properly function in Canada and to protect the security and privacy of Canadians, the Internet Society[1] urges the Standing Committee on Public Safety and National Security not to return Bill S-210 to the House until, at a minimum, amending Bill S-210 to narrow the scope of covered entities to remove Internet infrastructure services.

How S-210 Would Hinder Internet Services Crucial to the Flow of Information Online

Bill S-210 would make the providers of Internet services responsible for validating an end user's age when they are accessing sexually explicit material through the providers' services. This includes network operators, content delivery networks, search engines, email services, and others anywhere on the path from the original server where the sexually explicit material originates to the end user.

- The Bill defines "Internet service provider" as "a person who provides Internet access, Internet content hosting or electronic mail." This definition includes every operator of any network that carries, even in passing, any part of the sexually explicit material that is the target of the Bill.

[1] Founded in 1992 by a number of the original architects of the Internet, the Internet Society is a global nonprofit organization dedicated to ensuring the open development, evolution, and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocates for policies that protect the Internet. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF). *See,* https://www.internetsociety.org/.

- The Bill's definition of "Internet service provider" is far broader than the vernacular meaning of such a provider (often called "ISP"), which normally means the provider of a link from some place (like your residence) to the wider Internet—what might also be called an "Internet access provider." However, the Bill would still be extremely problematic if its definition of "Internet service provider" were the more usual meaning, since it would place liability onto a service provider that generally has limited ability to know the content its customers are accessing. Due to technical developments related to privacy on the Internet, these limitations are increasing[2] (both to shield people from intrusive practices by ISPs, often related to the suppression of speech in some jurisdictions, and to protect against broader security and privacy threats).
- The Bill uses the Criminal Code's definition of "organization", which includes a wide range of intermediaries and individuals, both online and offline, that profit from facilitating the flow of information online, whether explicit material or not.
- The Bill does not exclude Internet infrastructure intermediaries that have no way to know what content would require age verification without having to develop invasive content monitoring capabilities, some of which may be extremely difficult technically if not impossible.

The current text of S-210 contains three ways for Internet service providers to avoid these liabilities:

- One is to make the material available for a "legitimate purpose related to science, medicine, education or the arts." The Bill does not define these legitimate purposes, but one might presume that (for instance) health education materials would be covered under such a provision. Of course, an organization would necessarily be taking a risk that the materials it makes available *would* be covered under this exception and might avoid taking such a risk anyway in an abundance of caution.
- The second way to avoid liability is to have "implemented a prescribed age-verification method to limit access to the sexually explicit material made available for commercial purposes to individuals who are at least 18 years of age." Most Internet service providers would be forced to implement this method to manage their liability, and some of them would be unable to do it because they could not tell whether a given portion of traffic (called a datagram") crossing their network had or had not been age-authorized.
- The third way to avoid the liability is to be in the middle of implementing whatever provisions the Bill's enforcement authority has set out, so long as that takes 20 days or less.

[2] See Roi Toirosh. *Keeping Up with TLS Technology Trends: Insights and Analysis*, May 10, 2023, available at https://www.radware.com/blog/applicationdelivery/2023/05/keeping-up-with-tls-technology-trends-insights-and-analysis/

Technical Challenge: Forcing Infrastructure Intermediaries to Perform Age Verification is Impractical and Dangerous.

Forcing Internet infrastructure intermediaries to perform age verification to avoid liability is technically infeasible and would put people at major risk of harm. The Internet was created as a general-purpose network. Infrastructure intermediaries, such as network operators, content delivery networks, and cloud storage services, facilitate the flow of information online as conduits for data passing through their networks and services. They are not typically aware of the specific content passing through their services, and due to widespread technical protections for information flows online, they are mostly unable to access this information.

Content travels across the Internet in "packets" (more formally, "datagrams"). Information flowing between machines on the Internet is broken into small chunks—datagrams—that can each take a different path to their destination.[3] The destination computer (e.g. the end user's computer) reassembles all the datagrams into the complete flow of information. It is technically impossible for a network operator to examine a single datagram passing through their network and determine whether it contains sexually explicit material, as they usually do not have all the other datagrams needed to reassemble the content. (Even if all the datagrams take the same path through the same network operator, the network operator cannot keep them all around to examine until the final datagram arrives for technical reasons of network efficiency.)

Additionally, the vast majority of traffic on the Internet today is encrypted—scrambled in a way that only the sender and recipient can unscramble—such that it is not technically possible for a network operator to observe the underlying content that passes through their network even if they have all the datagrams necessary.[4] Bill S-210 would force Internet intermediaries to find ways to access the encrypted content going through their services. As implementing encryption is done by the endpoints of a given communication flow and not by, e.g., network operators passing the traffic through the Internet, many of these Internet intermediaries will find compliance impossible. Some Canadian Internet intermediaries could refuse to carry encrypted traffic altogether to protect against liability under S-210. However, this would result in large portions of the global Internet becoming inaccessible to Canadian users, or else expose Canadians to the use of unencrypted communications for banking and health care information, putting all Canadians at risk.

[3] Cloudflare. *What is a Packet,* available at: https://www.cloudflare.com/learning/network-layer/what-is-a-packet/

[4] Internet Society. *What is Encryption,* available at: https://www.internetsociety.org/issues/encryption/what-is/

How S-210's Age Verification Mandate Would Jeopardize User Safety, Security, and Privacy Online

The Bill's age verification obligations will significantly hinder key elements of what the Internet needs to exist and thrive as an open, globally connected, secure, and trustworthy resource. Forcing Internet infrastructure intermediaries to impose age verification contributes to Internet fragmentation by disrupting the seamless, interoperable nature of the Internet. It will also significantly jeopardize user security and privacy by forcing more services to scan traffic and collect/store personal data.

To understand why this can be problematic, consider the following analogy from the physical world. If Bill S-210 was similarly expressly targeted the offline world:

- If a company delivers packages containing parts that, when assembled, create sexually explicit material to people under 18, they could be held liable. This could also apply to service providers of the package delivery company, including an airline delivery company that transports the package, as well as the airport and air traffic controllers who enable the airplane to land and be offloaded at its facilities.
- The package would need to be opened at every step of the delivery chain. The contents would be checked against the age of the recipient, and a determination would be made as to whether the part in the package was a component of sexually explicit material. Then, it would need to be sent to the next entity for the process to be repeated.
- Not only would this be incredibly inefficient, but at each step there would be increased chances for theft, destruction of property, and the loss of privacy. Both businesses and individuals would have less trust in the Canadian shipping industry, damaging the economy and preventing Canadians from being able to easily receive and send packages.
- If any packaged materials were lost or stolen in transit as the package was repeatedly re-opened and closed, the total package would eventually need to be re-shipped, making package shipment slower and clogging the shipping infrastructure with extra packages that were needed only due to inefficiencies that came from that same shipping infrastructure.

Forcing Internet intermediaries to adopt age verification could prevent people from using security tools crucial to safety online.

Imposing age verification on Internet intermediaries would require them to access the content flowing through their services to avoid overblocking legitimate content or missing illegitimate content. However, most Internet traffic is protected by encryption, which prevents criminals from accessing a user's content as it travels across the Internet. This same encryption also prevents Internet intermediaries from viewing user content.

Encryption is a critical security technology that enables the use of the Internet for commerce, banking, medicine, and private conversations, some of which undoubtedly protect young people.

If Internet traffic were left unencrypted to allow access to content by Internet intermediaries, this unencrypted data would be susceptible to a wide range of threats. Criminals could access the information being sent across the network for use in scams or theft. For instance, foreign adversaries could access sensitive communications, putting Canadian government officials and national security professionals at risk.

Broad age verification requirements create massive privacy challenges that threaten security online.

Implementing age verification while protecting the privacy and security of users is always a difficult challenge. However, where age verification is implemented on the Internet and by whom can potentially compound these challenges. By requiring age verification by Internet intermediaries, Bill S-210 introduces significant new concerns to ensuring the security and privacy of Canadian users while performing age verification. Because of the exceptionally broad definition of "Internet service providers" in the Bill, it appears that virtually every organization involved in communicating on the Internet in Canada would need to implement such age verification, even if the organization has no direct relationship with the user in question. Under the Bill if enacted, every Internet intermediary would be required to implement such verification.

How data will be collected and shared with Internet intermediaries to determine the age of the user without potentially revealing user information is also a difficult problem. This is particularly challenging as most Internet intermediaries will have no direct relationship with a user and many Intermediaries would need to be provided with that information, but without any standard way to communicate it.

There are also significant challenges around age verification and access to the Internet. Depending on the age verification technique, some users may be prevented from access. For age verification techniques that require a valid government ID or bank account from users, the thousands of Canadians living[5] without a form of valid government ID or Canadians who are unbanked would be further marginalized. For other techniques that require the use of a camera, Canadians with devices without built in cameras or with older devices with poorer quality cameras can be left out. This is to say nothing of the privacy implications that arise from every camera on every Internet-connected device potentially radiating identity information about everyone who uses that device to every company involved in transmitting every datagram sent from that device across the Internet. It seems plain that that is not the intent of the Bill, but that appears to be its technical implication anyway.

[5] See Megan Marelli, *What it means to be a Canadian living without ID,* March 31, 2017, available at https://this.org/2017/03/31/what-it-means-to-be-a-canadian-living-without-id/

Conclusion

Bill S-210 aims at a very positive goal, protecting children from exposure to sexually explicit material online. However, the broad scope of Bill S-210 threatens not only the security and privacy of Canadian Internet users, but the core functions of the Internet itself. In its current form, Bill S-210 threatens to break the ability of Canadian Internet intermediaries to connect Canadian users with the rest of the global Internet. In order to ensure that the Internet continues to properly function in Canada and to protect the security and privacy of Canadians, the Standing Committee on Public Safety and National Security must not return Bill S-210 to the House until, at a minimum, amending Bill S-210 to narrow the scope of covered entities to remove Internet infrastructure services.