Online Safety in Canada

The Canadian Internet Registration Authority | June 23rd, 2022

Executive Summary

1) The Canadian Internet Registration Authority (CIRA) commends the Government of Canada's commitment to address illegal content online and shares the view that the internet is a vital tool for participation in our democracy, society, and economy.

2) CIRA's submission reflects its role as the .CA country-code top-level domain registry operator, cyber security services provider, and experience in international internet governance fora, including the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Governance Forum (IGF) and the Internet & Jurisdiction Policy Network (I&JPN).

3) Having carefully followed the Online Safety Expert Panel's process, CIRA respectfully submits that Canada's online safety legislation must maintain a commitment to the open non-proprietary standards of the internet and consider the technical architecture of its infrastructure. Specifically:

   a) The current deliberations about online safety in Canada have excluded the domain name system (DNS) from the scope of proposed internet content regulation. This is the correct approach and is consistent with that of key allies.

   b) Actions at the upper layers of the technology stack are the most precise and effective for managing illegal content online. To the contrary, DNS-level action to manage illegal content online is a disproportionate response.

   c) Excluding the DNS from the framework will align Canada's approach with international best practices and maintain key internet principles, including openness and reliability.

   d) Canada's approach should ensure website blocking by ISPs is a tool of absolute last resort.

About CIRA

4) The Canadian Internet Registration Authority (CIRA) is a member-based, not-for-profit organization best known for managing the .CA country code top-level domain (TLD) on behalf of all Canadians. CIRA operates the .CA registry and associated .CA domain name system (DNS) network, with over 3.2 million domains under management.

5) Our mission is to build a trusted internet for Canadians. According to SpamHaus, .CA is one of the safest TLDs in the world, with an abuse rate of less than 0.1%.[1] CIRA also provides several cybersecurity services to keep Canadians safe online. These include:

   a) *DNS Firewall*: our enterprise-level DNS protection for small businesses, municipalities, education, and healthcare institutions that protects over 3.1 million people from malware, ransomware and other security threats.

[1] SpamHaus, "The World's Most Abused TLDs," *The SpamHaus Project*, Date Accessed June 08, 2022, https://www.spamhaus.org/statistics/tlds/

b) *Anycast DNS*: routing infrastructure that brings global content closer to end users and keeps users safe by minimizing the impact of security threats.

c) *Canadian Shield*: a free cybersecurity service for Canadian families and personal devices that protects from malware, phishing and scams. In 2021, Canadian Shield blocked over 30 million malicious domains from compromising Canadians' data, devices and networks.

6) CIRA partners with several institutions to keep these services up-to-date and Canadians safe online, including the Canadian Centre for Cyber Security, the Canadian Centre for Child Protection, and Scam Advisor.

Introduction

7) CIRA shares the Government of Canada's view that the internet is central to Canadian life and vital for the full participation in our economy, society, and democracy.

8) CIRA's mission is to build a trusted internet for Canadians. We centre our work around the following principles:

a) *Open*: the internet and its underlying protocols are built on open, non-proprietary standards, which allow services and devices to interoperate across distributed networks. The open internet enables innovation and offers a level playing field for new ideas, business models, platforms, and companies.

b) *Trusted*: Canadians expect privacy, safety, and security on the internet – without which there are severe implications for our culture, economy, and democracy.

c) *People-centred*: the internet can be a democratizing force for good by serving the public interest through transparency, accessibility, and education.

9) The internet is rife with opportunities for abuse and harm. CIRA applauds the Government of Canada's commitment to fostering a safe online environment for Canadians. We support the objective to combat illegal activity online while protecting Canadians' freedom of expression.

10) CIRA's recommendations are derived from the role CIRA plays in the operation of the domain name system for the .CA TLD, as a cyber security services provider, as well as CIRA's understanding of internet architecture and involvement in global fora for multistakeholder internet governance.

11) CIRA holds the multistakeholder model of internet governance in high regard and endorses the Government of Canada's longstanding support[2] for the bottom-up development of internet standards.

[2] Kathryn Brown, "Canada's unique opportunity to lead the future of the internet," *The Hill Times,* February 26, 2018, https://www.hilltimes.com/2018/02/26/canadas-unique-opportunity-lead-future-internet/135540

12) CIRA respectfully submits that any legislation to advance online safety in Canada must do so without threatening the open, non-proprietary standards on which the internet was built and without compromising the technical infrastructure on which it operates.

The current deliberations about online safety in Canada have excluded the DNS from the scope of proposed internet content regulation. This is the correct approach and is consistent with that of key allies.

13) CIRA submits that Canada's framework for online safety should exclude intermediaries who provide domain name services from the regulation of illegal content to avoid undermining the technical architecture of the internet.

14) CIRA supports the panel's presumptive view to exclude the DNS and other core infrastructure from any resulting legislation meant to curb harms online.

15) DNS service providers have no influence over the content of websites. DNS service providers do not transmit, nor do they store the content of websites. As depicted in *Appendix A*, domain registries and other DNS service providers operate at the network and transport layers, which exist in the lower layers of the technology stack. The DNS is foundational to the internet, serving as its "phonebook." The DNS sends internet users in the direction they want to go online.[3] See *Appendix 2* for details about how the DNS works.

16) DNS-level actors, operating at a very low and foundational level of the technology stack are not well suited for identifying or removing harmful content, or determining whether content is likely to have harmful effects.

Actions at the upper layers of the tech stack are the most precise and effective for managing illegal content online. To the contrary, DNS-level action to manage illegal content online is disproportionate.

17) DNS-level action to mitigate and remove the content of websites is a disproportionate response. DNS service providers, as core internet infrastructure operators, exist below the application layer. The only tool available to DNS operators is to remove or prevent an entire domain name from being resolved.

18) There are other intermediaries, which operate nearer to the content and have a closer relationship to the person responsible for posting content, including social media platforms and web hosting companies. These intermediaries are better suited to intervene in the content of a website, and able to remove specific content with precision rather than preventing entire domains from being resolved. These intermediaries are also capable of facilitating communication with the person(s) responsible for the content of a website.

19) DNS-level actors – such as registries, registrars, and internet service providers (ISPs) – are farthest away from the content that is posted on these platforms. If Jane Doe posts illegal terrorist content on Facebook, there is no scenario in which a DNS-level actor would be able to take

[3] Jay Hoffman, "What Happens When You Enter a URL In Your Browser of Choice?" *The History of the Web,* April 15, 2019, https://thehistoryoftheweb.com/history-of-the-url/

action to make the content inaccessible to Canadians without disrupting access to all of Facebook.

20) Social media platforms like Facebook, Instagram and Twitter operate at the application layer. If Jane Doe posts hate speech or terrorist content, only Jane Doe or Facebook's internal content moderators can remove the content from the platform. This is the most precise and accurate way to render illegal content inaccessible to Canadians. DNS-level action to remove content is therefore unnecessary.

21) The internet's openness rests on the equal treatment of content through "the pipes." This is, in part, why DNS service providers and ISPs are not responsible for monitoring the content of websites. DNS-level action, through a registry, registrar, or ISP, would upend the current system in which content is treated equally by these intermediaries.

22) Therefore, CIRA supports the exclusion of the DNS from internet content regulation. Internet content, especially that which is posted on social media platforms, is outside of the ambit of action which could be reasonably taken by DNS service providers and ISPs. Excluding the DNS from the online safety legislation is the right approach.

Excluding the DNS from the framework will align Canada's approach with international best practices and maintain key internet principles, including openness and reliability

23) There are several lessons from other jurisdictions' internet content and services regulation that the Government of Canada can draw from. These include the European Union's (EU) *Digital Services Act* (*DSA*) and the United Kingdom's *Online Safety Bill*.

24) The EU *DSA* specifies categories of intermediaries, as well as different obligations for different types of service providers. Their obligations are "proportionate to size, impact and risk."[4] CIRA submits that the EU *DSA* assignment of obligations proportionate to a service's size, impact, and risk is the right approach.

25) The *DSA* regulates very large online platforms and very large online search engines that reach over 45 million users in the EU.[5] They have the most responsibility for curbing illegal content as they pose the most risks in the dissemination of illegal content.

26) CIRA also submits that the United Kingdom's decision to target user-to-user and search services in the *Online Safety Bill* is correct, and the UK's exclusion of intermediaries who provide core infrastructure should be emulated in Canada's approach.

Canada's approach should ensure website blocking by ISPs is a tool of absolute last resort.

[4] European Commission, "Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment," *European Commission,* April 23, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545

[5] European Commission, "The Digital Services Act: ensuring a safe and accountable online environment," European Commission, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en#new-obligations

27) In the 2021 Technical Paper for the Government's previous proposal to manage harmful content online, the proposed Digital Safety Commissioner would have the authority to apply to the Federal Court for an order for telecommunications service providers to block access, "in whole or in part" to an "online communications service" if the online communications service provider repeatedly did not comply with orders to remove child sexual exploitation content or terrorist content.[6]

28) While the Online Safety Expert panel workshops have not yet contemplated website-blocking, CIRA cautions that an expanded scope of regulated entities could open the door for over-use of this mechanism.

29) Site-blocking can be done by ISPs through DNS-blocking, IP-blocking, or other protocol-based methods. DNS-level action includes redirecting a domain name to a lander page as opposed to the original website associated with the domain. IP-blocking blocks certain IP addresses from resolving on a given network. Both DNS and IP-blocking can be disproportionate in their impact, resulting in the over-removal of legitimate content, harming freedom of expression. Site blocking is also easily circumvented with readily available tools such as virtual private networks (VPNs.)

30) CIRA submits that the Government's approach should ensure that court-ordered website-blocking by ISPs is a tool of absolute last resort for addressing illegal or harmful content online when there are more proportionate responses and intermediaries available to remove the content with precision.

Conclusion

31) CIRA submits that Canada's online safety legislation must maintain the open, non-proprietary standards of the internet and respect the technical architecture of its infrastructure.

32) The current deliberations about online safety in Canada have excluded the DNS from the scope of proposed internet content regulation. This is the correct approach and is consistent with that of key allies.

33) Actions at the upper layers of the tech stack are the most precise and effective for managing illegal content online. To the contrary, DNS-level action to manage illegal content online is a disproportionate response.

34) Canada's approach should ensure website blocking by ISPs is a tool of absolute last resort.

35) CIRA appreciates the opportunity to participate in the creation of a safer online Canada.

[6] Canada, "Technical Paper," Canadian Heritage, 2021, paragraph 120, https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content/technical-paper.html#a1

Appendices

Appendix 1: The Technology Stack

The DNS is a network layer protocol and is therefore far away from the application layer on which illegal content is accessed by users. The open systems interconnection (OSI) model explains the different layers at which protocols communicate across networks.[7]

Image 1: The Technology Stack

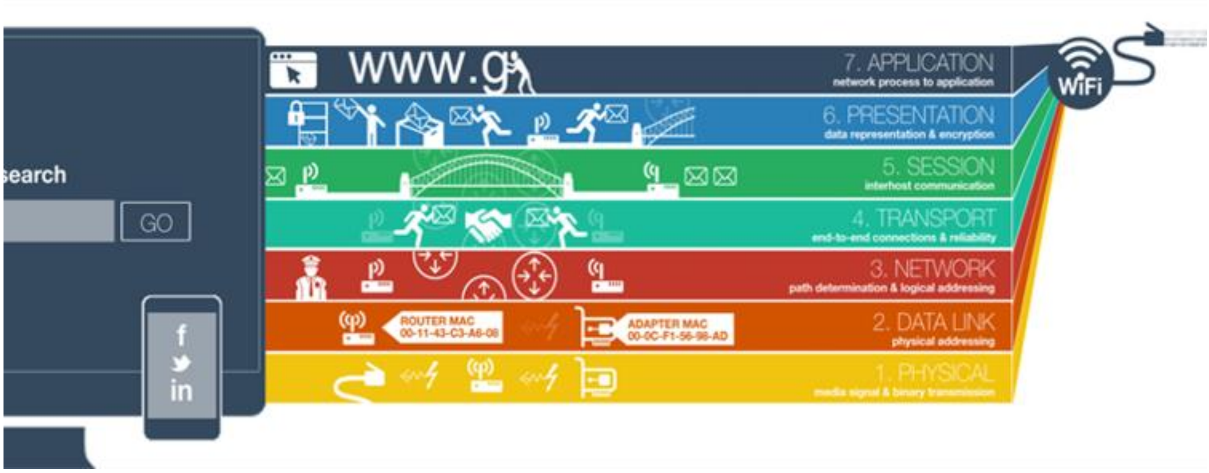

www.g
search
GO
f
in
ROUTER MAC 00-11-43-C3-A6-08
ADAPTER MAC 00-0C-F1-56-98-AD
7. APPLICATION
network process to application
6. PRESENTATION
data representation & encryption
5. SESSION
interhost communication
4. TRANSPORT
end-to-end connections & reliability
3. NETWORK
path determination & logical addressing
2. DATA LINK
physical addressing
1. PHYSICAL
media signal & binary transmission
WiFi

Table 1: Actors in the Technology Stack

OSI Model Layer	Actors
Application Layer	• Platforms + apps – Google, Facebook, Instagram, Twitter, Reddit, Discord, Youtube, eBay, Amazon, GoFundMe • Web Browsers – Google Chrome, Apple Safari, Microsoft Edge, Mozilla Firefox • Email – Microsoft Outlook, Google Gmail • App stores – Apple, Google, Amazon
Presentation Layer	
Session Layer	• CDNs (Akamai, Cloudflare, Amazon Cloudfront) • ICANN, RIRs (ARIN, RipeNCC, LACNIC, AFRINIC, APNIC) • Registries (CIRA, Nominet, DNS Belgium, Verisign, etc.), Registrars (Tucows, GoDaddy, etc.), • ISPs (Bell, Rogers, TekSavvy, Northwestel, etc.),
Transport Layer	
Network Layer (IP, DNS)	
Datalink Layer	• Apple, Samsung, Google, Microsoft, Dell, Acer, Huawei, Cisco,
Physical Layer	• Bell, Rogers, SaskTel, TekSavvy, Videotron, Northwestel, TorIX, OGIX, AT&T

[7] Cloudflare, "What is the OSI Model?", *Cloudflare,* Date Accessed June 07, 2022, https://www.cloudflare.com/en-ca/learning/ddos/glossary/open-systems-interconnection-model-osi/

Appendix 2: How the DNS works

The DNS is the 'phonebook' of the internet. It is a hierarchical system of databases that correlates human-readable domain names, like 'canada.ca' or 'cira.ca' to their corresponding IP addresses. CIRA, as a registry, operates name servers for the '.CA' zone. CIRA is delegated the .CA zone by the Internet Corporation for Assigned Names and Numbers, the international not-for-profit organization at the top of the DNS hierarchy, who operates the root zone and is responsible for governance of the DNS.

Image 2: DNS Query Resolution

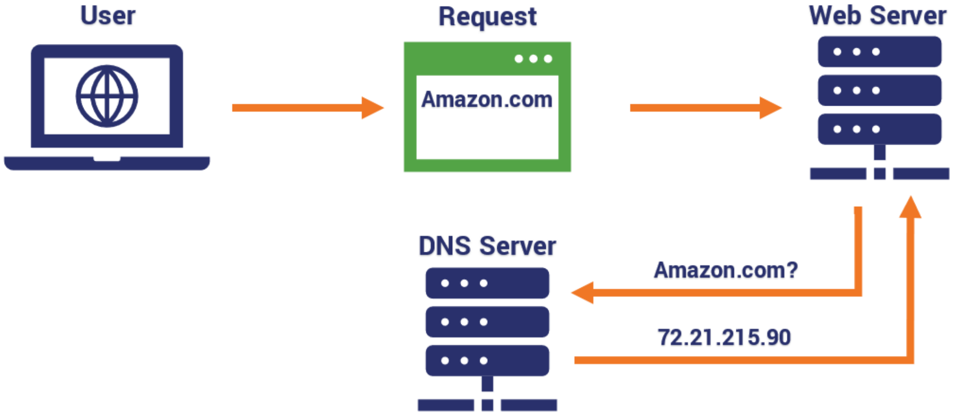
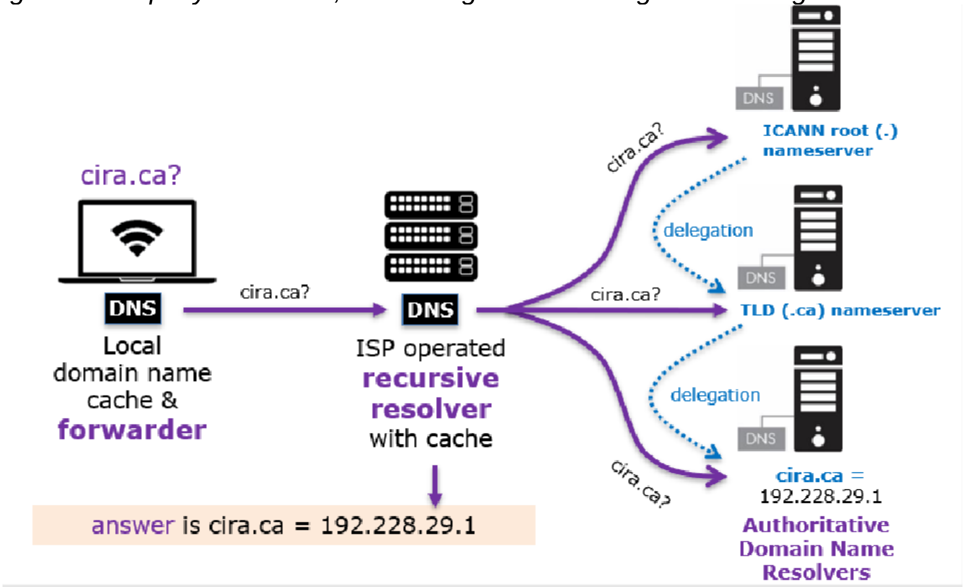


Image 3: DNS query resolution, accounting for zone delegations through DNS resolvers


cira.ca?
DNS
Local
domain name
cache &
forwarder
cira.ca?
DNS
ISP operated
recursive
resolver
with cache
answer is cira.ca = 192.228.29.1
cira.ca?
DNS
ICANN root (.)
nameserver
delegation
DNS
cira.ca?
TLD (.ca) nameserver
delegation
DNS
cira.ca?
cira.ca =
192.228.29.1
Authoritative
Domain Name
Resolvers